Inside the Federal Government's Latest Guidance on IoT Security

Companies need to be mindful of November guidance from DHS and NIST.

Hanley Chew, Fenwick & West, Law Technology News

January 19, 2017

On Oct. 21, 2016, a massive distributed denial of service (DDoS) attack occurred against the domain name system (DNS) provider Dyn, causing widespread disruption of internet activity against the United States. A DNS is the part of the internet infrastructure that is responsible for translating domain names into numeric IP addresses, which ensures that information requests are routed to the proper server. The DDoS attack was accomplished when the attackers hacked a large number of unsecured internet-connected digital devices, such as CCTV videocameras and digital video recorders (i.e., the "Internet of Things" (IoT)), and directed the devices to transmit huge amounts of traffic to Dyn's servers. The hack of the IoT devices was made possible because the owners of these devices continued to use default user names and passwords and the utilization of the Mirai bot, which scans the internet for IoT devices that use those usernames and passwords.

The DDoS raised public awareness and concern about the lack of adequate security in IoT devices. Approximately three weeks later, two federal agencies—the Department of Homeland Security (DHS) and the National Institute of Standards and Technology (NIST), an agency in the Department of Commerce—released their guidance concerning security for IoT devices.

The DHS Guidance

On Nov. 15, 2016, DHS released its guidance on "Strategic Principles for Securing the Internet of Things," which set forth six nonbinding principles for addressing the security of IoT devices. The guidance was targeted toward stakeholders who "develop, manufacture, implement, or use network-connected devices."

Incorporate Security at the Design Phase: The guidance recommends that developers should build in security at the earliest phases of design and development. Some suggested practices include adopting unique, hard to crack default usernames and passwords; building the device using the most recent operating system; using hardware that already incorporates security features; and

designing the device with system and operational disruptions in mind.

Promote Security Updates and Vulnerability Management: Even when security is included at the design stage, vulnerabilities in devices may still be discovered after they are employed. The guidance suggests that these vulnerabilities can be mitigated through patching, security updates and vulnerability management. Some suggested practices include securing devices over network connections or through automated means; coordinating software updates among third-party vendors; developing automated mechanisms for addressing vulnerabilities; developing a policy concerning the coordinated disclosure of vulnerabilities; and developing an end-of-life strategy for IoT devices.

Build on Recognized Security Practices: The guidance recommends applying many of the tested practices in traditional IT and network security to IoT devices. In particular, the guidance refers to the NIST Cybersecurity Risk Management Framework as a starting point for assessing risk and best practices. Referring to relevant sector-specific guidance, where it exists; employing a holistic approach to security; and participating in information sharing platforms are suggested practices.

Prioritize Security Measures According to Potential Impact: The guidance recommends focusing on the potential consequences of disruption, breach or malicious activity across the consumer spectrum to determine where security efforts should be directed. It suggests knowing a device's intended use and environment, performing a "red-team" exercise where developers attempt to bypass the device's security measures at different levels (i.e., application, network, data or physical); and identifying and authenticating the devices connected to the network.

Promote Transparency Across the IoT: The guidance recommends that developers and manufacturers need to know any vulnerabilities associated with the software and hardware components provided by their vendors outside their organization. Increased awareness could help manufacturers and industrial consumers know where and how to apply security measures or build in redundancies. Some suggested practices include inclusion of vendors and suppliers in the risk assessment process; creating a publicly-disclosed mechanism for using vulnerability reports, such as a Bug bounty program; and developing and employing a list of known hardware and software components in the device package.

Connect Carefully and Deliberately: The guidance notes that IoT consumers should consider whether continuous connectivity is necessary, given the use of the IoT device and risks associated with its disruption. It suggests that consumers be advised of the intended purpose of any network connection, and controls should be built into IoT devices to enable manufacturers, service providers and consumers to disable network connections or specific ports when it is desired to enable selective connectivity.

NIST's Guidance

On the same day as DHS released its principles for securing IoT devices, NIST released its own guidance in NIST Special Publication 800-160, Systems Security Engineering Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems (NIST SP 800-160). NIST stated in NIST SP 800-160 that its objective to "address security issues" and "to use

established engineering processes to ensure that needs, concerns, and requirements, are addressed with appropriate fidelity and vigor, early and in a sustainable manner."

NIST SP 800-160 recognizes that identifying all potential risks and/or preventing all breaches, disruptions or attacks are not realistic goals and, therefore, focuses on incorporating system security engineering (SSE) at all stages of the device's lifecycle (i.e., design, development, deployment, and maintenance) so as to make IoT devices less inherently vulnerable and more resilient and to limit the damage from the inevitable breaches, disruptions, and attacks. It starts with and builds upon a well-established international standards published by the International Organization for Standardization (ISO), the International Electrotechnical Commission (ICO) and the Institute of Electric and Electronic Engineering (IEEE). NIST SP 800-160 defines 30 different processes from initial business and mission analysis through the design and architecture stages, and outlines specific SSE activities and tasks for each process.

NIST SP 800-160 also outlines design principles for security spanning three areas: security architecture and design (i.e., organization, structure, interconnections and interfaces); security capability and intrinsic behaviors (i.e., what the protections are and how they are provided); and life cycle security (i.e., security process definition, conduct, and management). It further provides an overview of engineering and security fundamentals, covering subjects such as protection needs; security requirements and policy; distinguishing requirements, policy, and mechanisms; system security architecture, views and viewpoints; security relevance; security function protection criticality; trustworthiness and assurance; and cost, performance, and effectiveness.

Although the guidance released by DHS and NIST is nonbinding, companies should be mindful of it. Because this guidance has been approved and released by the federal government, there will likely be regulators and/or plaintiffs who refer to the guidance when attempting to impose liability on IoT developers and manufacturers following a breach or disruption. Failure to follow the guidance may be argued to be evidence of inadequate security and negligence. In addition, insurers may also refer to the guidance during the underwriting process for obtaining cyberinsurance to ensure that IoT developers and manufacturers have an appropriate level of security. In effect, the guidance released by DHS and NIST may become a de facto standard of care. At a minimum, this guidance should be part of the conversation for the security of IoT devices.

Hanley Chew is of counsel with Fenwick & West, where he focuses his practice on privacy and data security litigation, counseling and investigations, as well as intellectual property and commercial disputes affecting high technology and data-driven companies.
