SECURITY

Here are the biggest IoT security threats facing the enterprise in 2017

The coming year will bring a large-scale IoT security breach, with fleet management, retail, manufacturing, and government at the biggest risk, according to experts.

By Teena Maddox | December 21, 2016, 8:06 AM PST

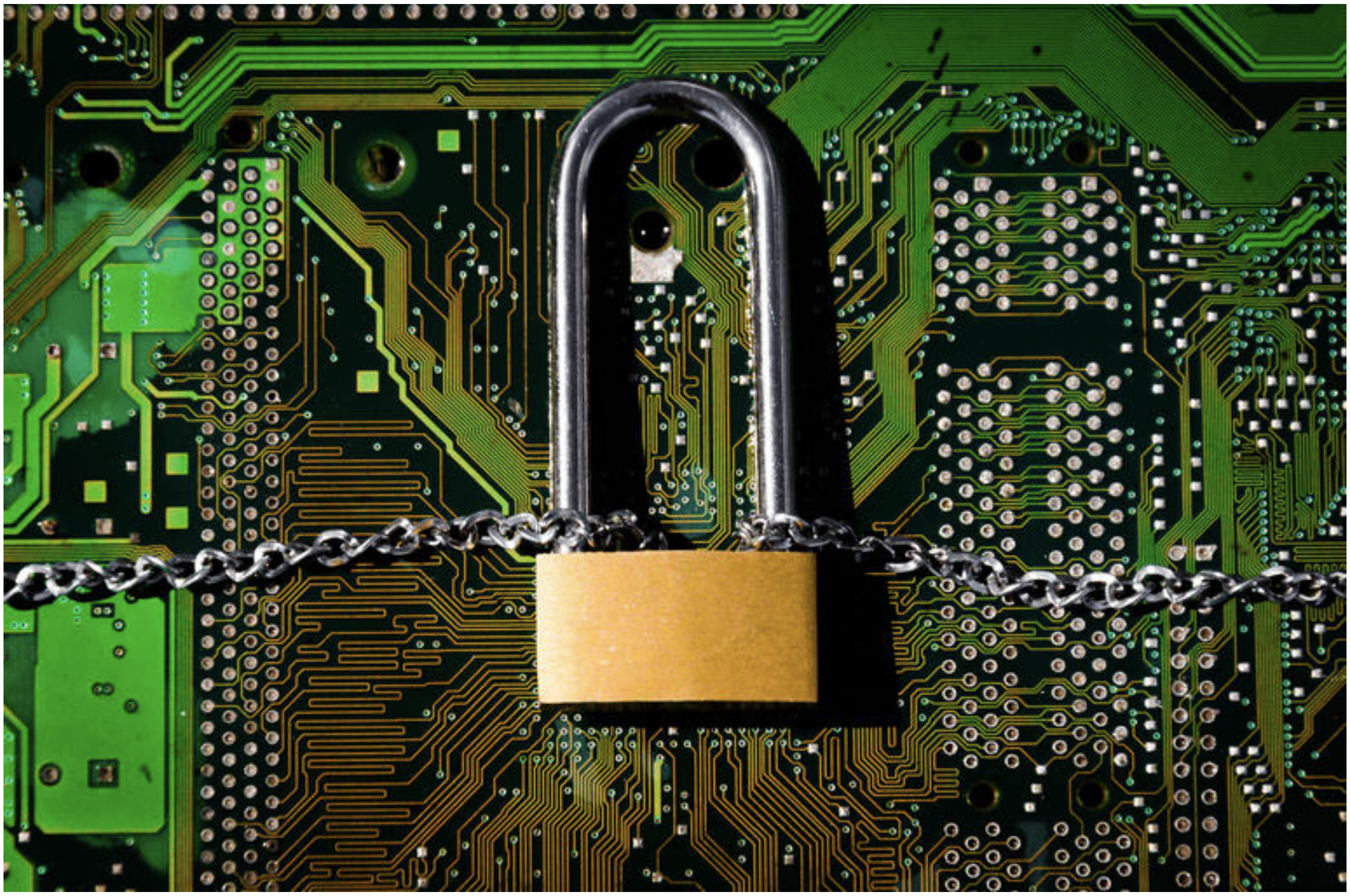

Image: iStock/Kirill_Savenko

In the past year, IoT security has quickly escalated as a hot-button issue with multiple threats against the enterprise such as the Mirai botnet that took down Twitter, Amazon, and Netflix. What's most alarming, though, is that it's likely only the beginning as more companies deploy IoT sensors and devices across their networks.

According to Gartner (http://www.gartner.com/newsroom/id/3185623), more than half of major new business processes and systems will include an IoT component by 2020.

Predicting the future is never easy, but TechRepublic talked to IoT security experts to find out what to expect in 2017. Participants were Frank Gillett, Forrester analyst; Sanjay Beri, CEO of Netskope; Adnan Amjad, partner, Deloitte Cyber Risk Services; Simon Moffatt, senior product manager, ForgeRock; Eve Maler, vice president of innovation and emerging technology, ForgeRock; Javvad Malik, security advocate at AlienVault; Jason Collins, vice president of IoT marketing at Nokia; David Campbell, chief security officer, SendGrid; Kirstin Simonson, second vice president at Travelers Global Technology; Chip Witt, senior product manager, threat intelligence, HPE Security Research, Hewlett Packard Enterprise; Kurt Collins, director of technology evangelism and partnerships at Built.io; and Tom Kellermann, CEO of Strategic Cyber Ventures.

SEE: Progress in ransomware battle remains murky despite industry efforts (https://www.techrepublic.com/article/progress-in-ransomware-battle-remains-murky-despite-industry-efforts/)(TechRepublic)

More about cybersecurity

Cybersecurity no. 1 challenge for CXOs, but only 39% have a defense strategy (https://www.techrepublic.com/article/cybersecurity-no-1-challenge-for-cxos-but-only-39-have-a-defense-strategy/)

Why deepfakes are a real threat to elections and society (https://www.techrepublic.com/article/why-deepfakes-are-a-real-threat-to-elections-and-society/)

10 signs you may not be cut out for a cybersecurity job (https://www.techrepublic.com/article/10-signs-you-arent-cut-out-to-be-a-cybersecurity-specialist/)

Dark Web: A cheat sheet for business professionals (https://www.techrepublic.com/article/dark-web-the-smart-persons-guide/)

TechRepublic: How serious is the IoT cybersecurity threat for the enterprise in

2017?

Frank Gillett: Forrester predicts a large-scale IoT security breach will occur in 2017. The biggest targets are fleet management in transportation, security and surveillance applications in government, inventory and warehouse management applications in retail, and industrial asset management in primary manufacturing.

Javvad Malik: In 2017, the IoT device security debate will escalate, putting pressure on manufacturers to architect fundamental security principles into the designs of internet-connected products. We may even see governments around the world take an active role in IoT safety legislation. Everyday appliances (e.g., the iron, washing machine and dryer) are subjected to rigorous testing, both by the manufacturer as well as independent testing labs, but a similar approach is not being taken with respect to cybersecurity for IoT devices. As a result, most are unsecure by design, and many vendors choose convenience (e.g., using default credentials in their appliances) over implementing proper security measures—a flagrant violation of best practices in product development.

Tom Kellermann: In 2017, I predict we'll see at least two polymorphic worms targeting IoT will spread in the wild and be leveraged for widespread DDoS attacks. One of these will be developed by North Korea and it will be used to punish the West via internet outages.

Jason Collins: There will be more and more IoT security breaches that will impact service acceptance. A growing realization is that the network has a large role to play in security for IoT because devices will not be able to handle the threat.

Adnan Amjad: In 2017, the continued rise in popularity of connected products results in an increase in the number of back doors open to an adversary, and IoT devices will become a target for ransomware. For manufacturers, building security in from the ground up and making it an integral component of the product—as opposed to adding in security at the final stages of manufacturing—can help prevent security issues later on in the product lifecycle. For businesses, develop your cybersecurity plan under the assumption that you will be breached. Prioritize the things that you need to keep safe and embed security elements into everything, beginning at the earliest stage of development.

Simon Moffatt: DDoS attacks, internet shutdowns powered by cheap, insecure IoT devices will become more common but become less lethal as backbone providers harden their defenses and device manufacturers adopt identity-based security to close vulnerabilities. However, the sheer number of cheap and insecure IoT devices deployed globally will ensure DDoS attacks continue sporadically through 2017. Catastrophic DDoS attacks might dominate tech media coverage, but the failure of IoT devices, service, and infrastructure to adopt and scale robust security and privacy tactics will play out in several ways also through 2017.

Chip Witt: The security industry has been talking about the security challenges IoT devices present for a few years, but 2017 will see attacks truly proliferate with the exponential adoption of connected devices and their associated (lack of) security. IoT sensors, with their limited computing power are only as secure as the firmware running on them, which means that their security posture depends on the readiness of device manufacturers to quickly react to attacks when they happen. Successful attacks on IoT sensors are difficult to detect because of the limited access to the device's system state, insufficient computing power for endpoint protection software to be installed on them, and lack of security compliance standards for IoT security best practices.

TR: Do you see more security intervention happening in the enterprise in 2017?

Sanjay Beri: 2017 is the year of the security intervention. The recent Dyn DDoS attack plus IoT plus cloud will force board-level meetings on cybersecurity at most Fortune 500 companies. This will force a doubling down on hiring and spending to quickly deal with enterprise blindspots.

David Campbell: DDoS mitigation will be center stage for internet-based companies in 2017. After the widespread DDoS attack of hosting company OVH in 2016, in which 150,000 Internet-connected devices were leveraged for a 1 Tbps attack, companies are going to have to start getting on the defensive side of DDoS mitigation. The Internet of Things is not going away, and without a way to regulate the resiliency of the firmware that operates these devices, the best way companies can protect themselves is with a clear DDoS mitigation strategy. It's not a matter of if anymore, but when, so having a mitigation strategy and having a relationship with a DDoS mitigation provider is table stakes for doing business on the internet in 2017.

Kurt Collins: In the next year we'll start to see more security-oriented measures put in place for IoT, and blockchain will play an integral role in that. One of the foundational premises of blockchain is to make sure that certain records and requests are accurate, just like an accounting ledger. When it comes to IoT, that is perfect because devices are widely distributed, sometimes calling back to the server and sometimes not. However, if they don't call back to the server, you want to make sure that the call any IoT device makes is actually the call it is supposed to make. By using blockchain on top of IoT, companies can implement a ledger methodology to any request that needs to be made to, or from, an IoT device and verify it is doing the right thing. Blockchain is critical in this because it is very difficult to fool blockchain and it creates a method of transaction verification.

TR: What impact do you think the General Data Protection Regulation (GDPR) to strengthen and unify data protection in the European Union will have on security?

Beri: With the GDPR deadline fast approaching, we'll see an increase in governance over unsanctioned apps where risky activities are blocked. Since the GDPR was adopted in 2016, we are now within the two-year countdown for compliance which will provoke a sense of urgency for organizations in 2017. Compliance is going to play a bigger role in the cloud as organizations become savvier to the apps people are using and increasingly realize how much sensitive data they have in their environments. 2017 will be ransomware's biggest year yet because organizations aren't inspecting for malware in the most commonly used apps. Malware is hiding in plain sight as SSL traffic passes through uninspected (which is a huge issue in general for enterprises).

Eve Maler: The most mature part of the IoT security and privacy technology stack comes from its web API heritage, with protocols such as OAuth and OpenID Connect playing a key role. With the FCC tightening privacy rules for broadband providers in the US, and the GDPR looming in the EU, the adoption of the OAuth-based consent and delegation standard User- Managed Access (UMA) protocol is likely to accelerate.

TR: What might happen in 2017 so that IoT device makers can provide additional security before rolling out devices to a broader audience?

Gillett: New certifications will be born. Major vendors like Cisco, Microsoft, IBM, and others will invest heavily in the form of low or no-cost training and certifications. Meanwhile, Forrester expects that 10 industrial vendors will jointly certify their IoT-enabled products with enterprise vendors, as Rockwell Automation has done with Cisco.

Kirstin Simonson: Security standards are still evolving to accommodate the plethora of devices coming to market without the necessary internal security features in place. For makers and manufacturers of these connected devices, it is extremely important that consideration for the digital security of each device is incorporated into the development protocols or methodology behind their production. In other words, security should not be an afterthought of product development. As a reference point, the National Institute of Standards and Technology (NIST) provides a comprehensive framework for businesses who design or develop numerous types of devices, which provides information that is very relevant to this topic. There are also other organizations that provide useful information for building security into the development methodology of electronic devices.

Witt: While it is likely that more security features will be built into IoT devices in 2017, making IoT inherently more secure, a large number of existing insecure devices will be used as the platform to launch targeted breaches and DDoS attacks. The trend will likely lead many companies to rethink the approach of protecting their internet-facing services against the DDoS attacks. Organizations will need to ensure they are implementing proper application security testing of connected devices and taking a data-centric approach that protects the sensitive information throughout its lifecycle with proven encryption and tokenization techniques.

Jason Collins: Governments will start exploring moves to regulate the IoT. Security and privacy concerns around IoT will create a situation where governments will push to regulate in a patchwork fashion. They will move to push the regulations into the network where there are more reasonable controls than controlling the end-user devices.

TechRepublic: What impact do you think a new president will have on IoT security?

Beri: With the increase in high profile data breaches in 2016 such as the Yahoo data breach and DNC hacks, the incoming administration will make cybersecurity a key focus. Particularly, the newly-appointed federal CISO will make cloud security and safe cloud enablement a priority, as it's expected to be the biggest threat vector for the government. Cloud adoption is only going to rise from here, and the federal CISO needs to be aware of the threat shadow IT poses to the government.

Also see:

- The smart city security nightmare: How cities can stay awake (https://www.techrepublic.com/article/the-smart-city-security-nightmare-how-cities-can-stay-awake/)

(TechRepublic)

- How risk analytics can help your organization plug security holes (http://www.techproresearch.com/article/how-risk-analytics-can-help-your-organization-plug-security-holes/) (Tech Pro Research)
- Experts predict 2017's biggest cybersecurity threats (https://www.techrepublic.com/article/experts-predict-2017s-biggest-cybersecurity-threats/) (TechRepublic)
- Cybersecurity ebook: The ransomware battle (http://www.techproresearch.com/downloads/cybersecurity-spotlight-the-ransomware-battle/) (Tech Pro Research)
- Interview with a hacker: Gh0s7, leader of Shad0wS3c (https://www.techrepublic.com/article/interview-with-a-hacker-gh0s7-leader-of-shad0ws3c/) (TechRepublic)
- Gallery: The 10 biggest business hacks of 2016 (https://www.techrepublic.com/pictures/gallery-the-10-biggest-business-hacks-of-2016/) (TechRepublic)
- Internet of Things: The Security Challenge (http://www.zdnet.com/topic/internet-of-things-the-security-challenge/) (ZDNet Special Report)

RELATED TOPICS: SECURITY INTERNET OF THINGS SOFTWARE CXO HARDWARE MOBILITY DATA CENTERS

About Teena Maddox

Teena Maddox is a Senior Writer at TechRepublic, covering hardware devices, IoT, smart cities and wearables. She ties together the style and substance of tech. Teena has spent 20-plus years writing business and features for publications including Peo...