CSO
FROM IDG

IoT security basics

SURVIVAL GUIDE

The Internet of Things: Why it is vulnerable | *Building an IoT security action plan* | **Enterprise structural changes, employee awareness can bolster IoT security** | Five best practices for building IoT offerings

A guide to IoT security basics

The Internet of Things – the connecting of billions of everyday and industrial devices using tiny sensors that transmit data and share information in the cloud – is revolutionizing the way we live and do business.

IoT platforms are expected to save organizations money, improve decision-making, increase staff productivity, provide better visibility into the organization and improve the customer experience. Six in ten U.S. companies now have some type of IoT initiative underway – either formal or experimental, according to IT trade association CompTIA.

All this potential comes with some big security risks – mainly with the unsecured devices themselves, but also with their ability to join forces to bring down systems. This can leave corporate networks vulnerable.

CSO's Basic Guide to IoT Security, gathered from CSO's popular interviews with IoT experts, provides a complete look at techniques used to prevent and defend against IoT-related attacks, as well as advice for IoT planning.

CONTENTS

The Internet of Things: Why it is vulnerable

These four key security risks are trade-offs to the benefits of IoT

BY STACY COLLETT

The Internet of Things – that vague yet expansive term – describes the connecting of billions of everyday and industrial devices using tiny sensors that transmit and share data and information in the cloud.

IoT devices can be used in nearly every industry to capture valuable data. For example, healthcare providers are looking at technologies to improve patient care, and retailers are looking to the IoT for opportunities to find new customers and improve the shopping experience.

Six in 10 U.S. companies now have some type of IoT initiative underway – either formal or experimental, according to IT trade association CompTIA.

IoT platforms are expected to save organizations money, improve decision-making via access to new data sources, increase staff productivity, provide better visibility into the organization and improve the customer experience. The McKinsey Global Institute predicts the IoT ecosystem will have a total economic impact of up to $11 trillion by 2025.

But this relatively new sector has significant security concerns. The October 2016 distributed denial-of-service attack on domain name service provider Dyn came as a shocking reminder of the IoT's security holes. The attack used malware called Mirai, which enslaved more than 380,000 IoT devices found in businesses and homes, its creator claims, to disrupt service at Netflix, Twitter, Spotify and other popular sites. It exploited a security flaw in inexpensive, connected DVRs, Webcams and surveillance cameras.

Security professionals say the service disruption was just the tip of the iceberg compared to the potential damage that can be unleashed by billions of unsecure IoT devices.

"You can grade the threat intensity as the IoT devices become more autonomous," such as self-driving cars, airplanes, house appliances and industrial systems connected to the internet. "That's where the real threat is," says Nicholas Evans, vice president and general manager within the Office of the CTO at Unisys, where he leads its worldwide applied innovation program.

Some 20.8 billion things could be connected to the internet by 2020, according to research firm Gartner. That's about 5.5 million devices added every day, fueled by more affordable and ubiquitous sensors, processing power and bandwidth. Also by 2020, more than half of major new business processes and systems will incorporate some element of the IoT, according to Gartner.

While the benefits of IoT are undeniable, the reality is that security is not keeping up with the pace of innovation.

The IoT ecosystem introduces risks that include malicious actors manipulating the flow of information to and from network-connected devices or tampering with devices themselves. This can lead to the theft of sensitive data and loss of consumer privacy, interruption of business operations, slowdown of the internet and potential disruptions to critical infrastructure and finally impacting the economy.

Four security vulnerabilities to consider

The more IoT devices that are in use, the more the security vulnerabilities, given that there are typically multiple security holes per device, and the broader the attack surface, says Roberto Tamassia, Ph.D., executive master in cybersecurity at Brown University.

"Factors that contribute to IoT device vulnerabilities include device manufacturers who don't have extensive cyber security experience, computing power and storage constraints that limit the available security mechanisms, cumbersome software update procedures, and the lack of user awareness of the security threats posed by these devices," explains Tamassia.

It should come as no surprise that IoT devices are a very attractive and powerful form of ubiquitous, low-hanging fruit for attackers who take advantage of several enterprise weak points.

1. The mobile workforce: Mobile workers who use home networks shared by their IoT devices can lead to enterprise network vulnerabilities. Take the popular NEST thermostat, for example. In 2015, upon accessing, NEST's mini USB port, TrapX Security engineers used an ARP spoofing app to spoof the ARP address for the network gateway as part of a man-in-the-middle (MITM) attack, says Moshe Ben-Simon, co-founder of TrapX Security. An MITM attack allows a person to intercept another person's internet connection and gather all of the information being transmitted across that network. Hackers use MITM attacks to gain increasing control of systems on either or both ends of the communication, including enterprise networks.

Even if you find the NEST thermostat in the home and not on enterprise property, close to company networks, the massive remote and mobile workforce ensures that criminal hackers' control of home computer systems ultimately leads to attacks on the corporate systems that employees connect to from home.

2. Unsecured office devices – webcams and access devices: IoT makes it possible for hackers to create and use botnets on such a large scale that taking down many kinds of infrastructure at once using DDoS attacks becomes relatively routine. An enterprise device could be hijacked for use in an attack, or the company's network could become the unwitting victim of a massive DDoS attack.

3. Consumer data: IoT is key to unlocking mountains of private consumer data, adding to hackers' targets and attack vectors and enabling them to easily guess common passwords used by key business, government, military, political and cultural targets, according to Ryan Manship, security practice director at RedTeam Security.

IoT collects consumer data to aid companies with targeted marketing by building a digital representation of each consumer's preferences and features, says Manship. Attackers steal and combine the different data to reveal consumer interests and habits, which they use to guess user passwords and answers to security questions so they can log into the enterprise where employees have reused the same passcodes, explains Manship, a contributor to the SANS Securing the Human training program.

4. Ransomware vulnerabilities: Today's ransomware attacks involve encrypting a victim's data and holding it hostage until they pay you. "Tomorrow, IoT offers a range of new ransomware attacks. Script kiddies might annoy people by locking them out of their house or their cars," says Jason Hong, head of the research group at Carnegie Mellon's Computer Human Interaction: Mobile Privacy Security Lab at the School of Computer Science. Anonymous might fiddle with a company's HVAC or lighting, raising electrical bills or irritating occupants, he says, and attackers might seek to break into multiple autonomous vehicles or medical devices, holding people virtually hostage, he says. ■

Building an IoT security action plan

Consider these tasks and technologies when implementing an IoT security strategy

BY STACY COLLETT

While many IoT devices aren't built with security in mind, their risk is primarily in providing additional points of entry for an attacker to gain access to your network. "Which, if you think about it, is no different than where we stand today, with the only difference being the volume of attackable devices we may have on our networks," says Nathan Wenzler, chief security strategist at AsTech, an information security consulting firm.

The problem isn't new, but it does add an increased scope that many may not be prepared to handle, Wenzler says. Aside from endpoint protection software, Wenzler recommends using the same security protocols companies are leveraging today will help protect critical assets against an IoT device becoming compromising. Consider these actions:

- **Take inventory:** Organizations first need to assess what internet-connected device they currently have, their vulnerabilities, and how they will address them. Gartner classifies IoT devices into four categories.
  1. Passive, identifiable things like RFID tags have a low threat risk.
  2. Sensors that communicate information about themselves, like pressure sensors, have a moderate threat risk.
  3. Devices that can be remotely controlled and manipulated, such as HVAC systems, have an above average threat risk.
  4. Smart autonomous things with many sensors and functions, like self-driving cars, hold the highest risk for sensitive data loss, malware and sabotage.
- **Segregate your network:** Internal firewalls and access control lists (ACL) will help isolate your critical areas from those which are not as critical. If you're implementing IoT devices, isolate those networks from being able to reach your data servers or other mission critical infrastructure.
- **Protect administrator accounts:** Hackers commonly break into workstations and other endpoints as a staging ground to launch more attacks. Usually, they're after administrator credentials which can net them access to other systems. IoT devices can be used to stage some of these attacks, so be sure to change the passwords of any administrator credentials on a regular basis, limit the number of those accounts in use, and limit where these credentials can be used from.
- **Patch everything:** Patching systems and applications limits the number of exploits and vulnerabilities that an attacker can use to break into other areas of your network from a compromised IoT device. It's a long-established best practice, but many organizations are still not patching comprehensively. Doing so will minimize your attack surface from any asset, including IoT devices.

- **Monitor your network:** SIEM tools and other behavioral analysis programs are becoming increasingly advanced and can monitor for a wide range of anomalous use. Most organizations already have these systems in place, and it should be trivial to add rules or monitoring criteria to alert if an IoT device does anything other than communicate to its appropriate central control point. This doesn't require special plug-ins or IoT-specific tools, as these devices still use standard network protocols to do their job.
- **Follow DHS recommendations:** The Department of Homeland Security wants enterprises to participate in information sharing platforms to report vulnerabilities and receive timely and critical information about current cyber threats and vulnerabilities from public and private partners. Information sharing is a critical tool in ensuring stakeholders are aware of threats as they arise3. The DHS National Cybersecurity and Communications Integration Center (NCCIC), as well as multistate and sector-specific information sharing and analysis centers (ISACs) and information sharing and analysis organizations (ISAOs), are examples.

Technologies that bolster IoT security

In corporate IT, there's a strong emphasis on endpoint security—or putting security software on laptops, desktops and smartphones, Hong says. "This only works for the top-tier of devices, but not for the billions of devices that will make up the middle and bottom tier," he says. "There will need to be major advances in network security to protect these kinds of devices."

Organizations will also need significant innovations in artificial intelligence and big data techniques to detect unusual behaviors, Hong adds. "We can barely manage the security of our desktops, laptops and cloud servers today, and adding thousands or tens of thousands of devices to a home or corporate network will mean that we will need new and automated ways of quickly detecting and responding to attacks."

Overall, no single, homogeneous security technology can protect all IT assets including IoT edge processing, IoT platform middleware, back-end systems and data, says Ruggero Contu, research director at Gartner. "A multifaceted security approach is required to address expanded digital and physical risks," he says.

At the endpoint, different approaches can be used, from embedding security features within chip architecture to deploying software agents to perform different security controls, Contu says. Gateways will provide valuable help in a complex architecture such as IoT ecosystems that are difficult to secure due to heterogeneous devices and identity profiles.

"Gateways will be deployed to align and handle specific IoT domains, managing a specific set of devices with similar trust requirements, and therefore the domains can be shaped using principles of a common trust model," Contu says. "Federation of trust models allow interoperability between different domains and the devices that use different trust models." ■

Enterprise structural changes, employee awareness can bolster IoT security

You may have to change the way you procure and approve IoT devices and related items to ensure a secure environment.

BY STACY COLLETT

From an enterprise's perspective, there are three sides to the IoT threat:

1. Being attacked by an IoT army from around the world

2. Allowing enterprise-owned IoT devices to participate in such an attack against others

3. Allowing your IoT devices to attack your own company.

Making structural changes to your business will do nothing to help you defend against the first scenario, but it could make a profound difference in blocking attack scenarios two and three.

The structural IoT problem is that many of these devices are being purchased and approved far away from IT or the CISO's team. Consider door locks and light bulbs purchased by facilities, or beacons purchased by operations or marketing. Cases have been reported where penetration testing of a network — which is how a cyber thief might start testing for weaknesses prior to an attack — unintentionally released the IoT door locks at headquarters. IoT light bulbs have also been made to flicker in a way that broadcast messages to someone watching a window.

As IoT touches devices that have historically never needed IT approvals, this problem needs a fix.

Mission one: Train all employees in all departments what constitutes an IoT device, since manufacturers will use very different marketing terms.

Mission two: Require that IT or the CISO's office approve all of them, without exception.

One huge problem with IoT devices is that some house internal communications capabilities, such as a tiny antenna, ostensibly so that the devices can call home to get, for example, firmware updates. Although self-updating devices might seem great to a facilities manager, they open the door to two-way communications that can bypass all network security monitoring controls.

Yes, other monitors can track all independent wireless signals detected anywhere on a corporate campus, but with most campuses flooded with smartphones, tablets, wearables and wireless laptops, that may not always be a practical defense.

There's another issue involving oversight. Moving from regular devices to IoT devices often means a much higher price tag. And while that will almost certainly mean additional oversight (a.k.a. micromanaging), it's oversight from the perspective of cost, not security. A company's division general manager — or assistant treasurer or some other business manager — won't be thinking security when dealing with seem-

ingly innocuous items, and that is one of the first things that has to change.

"From a purchasing standpoint, that maintenance guy who usually buys the 55 cent light bulbs is now buying $40 light bulbs," said Thomas Pore, director of IT/services for Plixer, a security vendor that specializes in incident response. "But, clearly, security is not in the thought process."

Pore stressed that executives can be trained to recognize clues. If the device has its own antenna, for example, "4G is going to be labeled all over the box." But what if the device is using satellite communications. "OK, satellite-based? No visibility, none," Pore said.

Similar to the way that companies were forced to change their security thinking when printers and scanners started getting their own IP addresses, they need to change purchasing and oversight procedures to cope with the IoT. This is nothing that CIOs or CISOs can do on their own — and many executives would probably view any such move suspiciously, as a power grab. This kind of change has to come from the CEO — or, at the very least, the CFO, who does ultimately control the approval on all purchases.

Changing approval processes and adding a lot more (costly) training is never a fun recommendation to make. But unless you want to be done in by your own light bulbs and door locks, you're going to have to do it.

Governance

Having an IoT security policy and enforcing it strictly is a wise approach, says Laura DiDio, research director at 451 Research. "Organizations can mitigate and decrease the risk to an acceptable level by being proactive," she says. "That means that in IoT environments security must be built-in from inception. The IoT environment must be secure by design, secure by default, secure in use, secure in transmission and secure at rest."

Other "must dos" include training and recertifying IT staff on the latest security mechanisms and investing in security awareness training.

Companies using or planning to use the IoT can also work with other organizations to push for security standards for connected objects.

"It took years for the technology community to realize the need to build security protocols into internet communications," says Ed McNicholas, a co-leader of the privacy, data security and information law practice at Sidley Austin, LLP, who focuses on IoT as a part of his practice. "Companies can advance their security effectively by attempting to formulate and seek consensus on technical standards that allow for more secure communications."

Preparing IT staff for IoT

A key to developing strong IoT security will be acquiring the needed skills. "Most organizations do not have the internal skill sets that securing IoT devices will require," says Scott Laliberte, managing director and global lead of the security and privacy practice at consulting firm Protiviti. "Securing IoT devices requires a unique mix of hardware, development, network, and embedded security skills. Finding these at all, let alone in one person, is extremely difficult."

One of the skills most needed to develop better security protocols for IoT is the ability to communicate more effectively about risk, McNicholas says. This communication needs to take place among technologists, attorneys and business leaders.

"Only if the company can speak a common language can robust discussions about risks and rewards take place," McNicholas says. ■

Five best practices for building IoT offerings

Your IoT initiatives stand a better chance of success if you follow these steps

BY STACY COLLETT

With six in ten U.S. companies now having some type of IoT initiative underway, it's important to reduce IoT risks while delivering value to the business.

Successful IoT offerings rely on the perception of benefit they can deliver to businesses and consumers while creating a proportionate foundation of security, trust, and data integrity. There are important ways that IoT technology can reduce data security risk while improving customer experience in a connected world.

It's in every company's best interest to "do" IoT correctly, which will mean ratcheting up security measures to capture and ensure a good customer experience. Jack Nichols, director of product management at Genesys, provides six ways to do that.

1. Justify the business expense of "embedding" security: As with all technology, IoT security considerations should be embedded in every phase of development, from inception to deployment. Some organizations have a hard time justifying the added time and expense that accompany new security initiatives or adherence to continuous best-practice implementation. Everyone wants the new capabilities, but many balk at the price tag and operational complexity that goes with it. Security becomes an afterthought that is addressed at the end of the process, if at all.

Those same organizations should be aware that there are now numerous legal implications surrounding how an organization handles its IoT security. Much more importantly, "customer experience" is the reigning business differentiator, with loyal customers spending 300 percent more money with a trusted business than with others, Nichols says.

2. Test, test and re-test: Some 80 percent of IoT applications are not tested for security vulnerabilities, according to a report by Ponemon Institute, IBM and Arxan. That represents a staggering number of endpoints that leave themselves available for compromise.

As you develop your IoT applications and services, you need to conduct continuous internal and third party vulnerability analysis and penetration testing. Keep in mind that it's better to fold security into the product development cycle, rather than bolting it on after the fact. If you rush to market with an IoT system that isn't safe, then you're risking everything in invaluable consumer trust.

3. Proactively manage IoT security operations remotely: Many IoT product makers and app developers rely on the end user to install updates and configure security settings, which is ill-advised. Ideally, companies should be able to remotely push security patches and updates as soon as they're available to prevent vulnerabilities.

According to the most recent version of the IoT Trust Framework, such updates must either be signed and/or otherwise verified as coming

from a trusted source. Updates and patches should not modify user-configured preferences, security, and/or privacy settings without user notification. Automated (as opposed to automatic) updates increase customer trust because you do the heavy lifting, while still providing users with the ability to approve, authorize or reject changes.

4. Encryption is critical: Beefing up encryption is also advised in the new IoT Trust Framework. Show your customers you care about their privacy by ensuring that any support websites used in your IoT service fully encrypt user sessions, from the device to the backend. "Current best practices include HTTPS or HTTP Strict Transport Security by default, also known as AOSSL or Always On SSL." Furthermore, "Devices should include mechanisms to reliably authenticate their backend services and supporting applications."

5. Transparency matters: In February 2017, the Federal Trade Commission fined consumer electronics-maker Visio for collecting and selling its smart TV owner data. As outlined in a recent IEEE IoT newsletter, good transparency principles aren't exclusive to IoT, but require understanding that privacy threats in an IoT system are unique and require transparent disclosure related to three inputs:

- Personal data collected or generated.
- Data actions performed on that information.
- The context surrounding the collection, generation, processing, disclosure and retention of this personal data.

This isn't just a question of a company doing right by its consumer base. For example, the General Data Protection Regulation in Europe seeks verifiable consumer agreement to how each of these three inputs are managed via notice and consent. In general, it's best to state your data collection practices, as well as privacy, security and support policies, in an easily discoverable location on your company website, which can be reviewed prior to purchase or service opt-in. Further, disclose what and how features will fail to function if users decline to consent.

6. Embrace edge analytics and minimize the amount of sensitive data in transit: A natural byproduct of connecting everything is the creation of a surplus in valuable customer data, which can be both amazing and dangerous. In addition to safeguarding data warehouses, there is the added issue of securing massive amounts of data as it moves.

With IoT applications, as information is relayed from IoT endpoints to the cloud for computation and analysis, there's always a risk of exposure and threat of interception. But the current trend toward moving some computation to IoT endpoints and transmitting only prescribed information reduces the amount of potentially sensitive raw data in transit. While the arguments for edge computing generally center around increasing real-time functionality and the savings associated with machine learning and AI, mitigating customer data exposure is an added benefit. ■