NTT DATA Services

POINT OF VIEW | SECURITY SERVICES

Better Security for the Internet of Things

Security for IoT can no longer be ignored. Here's what every organization needs to know.

SEPTEMBER 2018

NTT DATA

Penetration of Internet of things (IoT)

Security researchers and white-hat hackers have been pointing out the potential for cyberattackers to target IoT for some years now.

The penetration of the internet of things (IoT) continues to grow — into consumers' home lives, but also into commercial applications in a broad range of industrial settings. By 2025, the number of connected devices worldwide is expected to reach 80 billion.[1] Or, to put that another way, more than 150,000 devices will be connected every single minute of the day.

The remarkable growth of IoT connectivity represents an alluring target for cyberattackers. The sheer volume of connected devices offers hackers an almost endless array of entry points, particularly because security protections are often minimal or non-existent. In addition, many of these devices connect to networks containing sensitive and valuable data.

Indeed, the fact that there have been relatively few security breaches exploiting the vulnerabilities of IoT is surprising. Security researchers and white-hat hackers have been pointing out the potential for cyberattackers to target IoT for some years now.

Still, several incidents provide just a taste of what could be to come. In 2017, the U.S. Food & Drug Administration ordered the recall of almost a half-million pacemakers amid concerns that, without a firmware update, these critical medical devices could be hacked — with potentially devastating results.[2] Previously, researchers staged a demonstration for Wired magazine in which they were able to take control of an SUV remotely using IoT, cut its brakes and engine, and drive it off the highway.[3] And as long ago as 2013, U.S. retailer Target Corp. saw 40 million customer credit card records compromised by an attack in which hackers gained entry via its heating systems.[4]

The stakes, in other words, could hardly be higher. IoT security vulnerabilities offer bad actors the opportunity to cause huge damage to individuals and corporations — even to pose a threat to life.

The scale of the challenge

The scale of IoT security challenges is difficult to overstate — but also difficult to quantify. With so many devices already deployed in what are often uncontrolled and unmonitored environments, getting on top of the size of the potential vulnerability is a challenge in its own right. So much so that for IoT developers, security has become their biggest current worry.[5]

It's not just the number of IoT devices that unnerves developers, or even the fact that they're deployed in such a broad range of settings — from home automation to smart cities, and from energy management systems to industrial engineering. It's also the breadth of the vulnerability of these devices. Key concerns include the following:

- Device constraints. Large numbers of IoT devices have very limited storage, memory, power and processing capability. As a result, traditional cybersecurity approaches, particularly those relying on complex encryption, aren't appropriate, because the device isn't capable of supporting them.
- Authentication failures. Preventing unauthorized devices from connecting to the network is difficult, because many rely on weak passwords or default settings that are easily compromised.
- Update management. Applying security updates, including patches, to devices can often be problematic. It may not be possible to track which devices are in operation where, older devices may not be compatible with newer devices, and not all devices will support remote updates or updates over the air. Users may simply opt out.
- Network insecurity. Even when a connected device is secure, its communications with the network and related apps may be difficult to protect, particularly because many devices lack encryption functionality. Network segmentation to control access to IoT devices should be part of an organization's in-depth network defense.
- Data privacy. The vast volumes of data created by IoT devices offer exciting opportunities, but also create a huge privacy and security headache — particularly in a regulatory environment that is becoming more complicated. It may be difficult to track, store and manage this data effectively, or to provide users with the right to opt-out or be forgotten.
- Detection problems. In complex networks with many connected devices of different types and variable communication protocols, detecting breaches is far from straightforward; incidents may remain undetected for some time. The same issues also make it very difficult to assess the extent of a breach, or the damage it has caused. Regular and automated network scans can help with device detection.

With so many problems to address and multiple points of vulnerability — from a smart television in someone's home to a factory valve connected to an industrial control system — it may be difficult to know where to start with IoT security. But organizations cannot afford to duck the issue of tackling this huge risk.

Taking responsibility

One fundamental question to address is who should take responsibility for equipping IoT with the security it so clearly needs. Lines of accountability and ownership are currently far from clear. IoT applications are being developed and distributed with little emphasis on security. End users, whether organizations or individuals, don't know how to manage their exposures — or even that they should.

Each constituency faces its own challenges. IoT device manufacturers, whether specialist developers or in-house operations developing their own solutions, must now take greater responsibility for their products. The issues of security should now sit at the heart of their development practices.

However, organizations with IT infrastructure into which IoT devices are incorporated can't afford to assume developers have built sufficient protections into these tools and systems. They must assess their own vulnerabilities and take steps to mitigate the risks where necessary.

Individual users of connected devices will also need to take care — thinking carefully about the data they're prepared to share via IoT, for example, and taking advantage of opportunities to manage and restrict their data profiles. Individuals will also need to continue to be vigilant about their broader exposure to cybersecurity, with this new potential entry point now emerging.

Leaving this final group aside, however, the evidence is that neither developers nor corporate are yet sufficiently engaged with the problems they face. For example, a recent study conducted by the Ponemon Institute warned:

- 75% of respondents believe IoT applications are being shipped without adequate security, because development teams are under pressure to get them shipped as quickly as possible
- 44% of organizations are taking no protective measures
- 75% of organizations aren't confident in their awareness of the apps their employees are using[6]

This is worrying. Security must become an intrinsic part of the development process as more devices and apps are rolled out. And corporate users with exposure to these tools need to be much more proactive in understanding the nature of those exposures and protecting themselves accordingly.

What does better IoT security protection look like?

How do organizations begin to reduce the vulnerabilities to which IoT now threatens to expose them? There is no one-size-fits-all approach to IoT security, but it's at least now possible to think in terms of separate workstreams.

Improving security barriers and protections

While both existing and new connected devices and apps pose multiple problems, it's possible to begin building more coherent defense systems. These defenses will require multiple layers, including segregated networks that keep the most insecure and vulnerable devices well away from the organization's core systems, with protections from firewalls.

The use of IoT platforms with security-by-default functionality will also make sense for many organizations. These platforms provide a means to determine which services, systems and resources any device can access on the system, with authentication and authorization protections applied automatically.

Device management must become a priority. Organizations need better visibility into the devices to which they're connected; specifically, more visibility into what systems these devices employ, and whether obsolete devices have been taken offline and disposed of efficiently. Use device registers to maintain these records. Change control and configuration management are the best tools to track devices on the network. Not changing default passwords becomes a critical security vulnerability.

Where possible, look for connected devices that are capable of supporting encryption. If this is out of the question, unencrypted devices should be subject to tougher segregation and authentication processes.

Testing and monitoring

Security testing is an increasingly vital element of any resilience strategy. In an IoT context, this will require a variety of different approaches. At its most basic, testing may be required simply to understand the security problems posed by older devices and systems, and their susceptibility to attack. Network segmentation and configuration control become more important to control IoT access. More sophisticated penetration exercises and simulations provide a means to assess the security of devices and systems considered more robust.

Threat modeling may also be appropriate for organizations with large-scale IoT exposures as they seek to identify and quantify the risks posed by their devices and applications. These risks may be multiple. Hackers have often focused on IoT devices as a means of entry, rather than as a target in themselves. However, threats, such as denial of service attacks, could target IoT systems, bringing key infrastructure or systems to a standstill.

Systems and networks need better monitoring, to both improve threat detection and identify penetrations. This will require scrutinizing network performance and activity logs for anomalies, and potentially the use of security intelligence analytics tools. Security and event management centers provide a means through which to take control of the organization's threat detection and management activities.

Improved governance

Many organizations have yet to take proper account of IoT vulnerabilities in their cybersecurity governance activities and planning. IoT needs to be addressed explicitly in this context, with governance policies and processes developed to counter the potential threat.

Building out governance planning may take some time, given the sprawling network of devices and systems that some organizations now have in place. But it will address both the management of the portfolio of devices in use and connected to the organization, and the vendors with which the organization works.

Conclusion

The rapid pace at which the IoT environment has grown and expanded has often resulted in security being regarded as something of an afterthought. Remedying that issue in previous deployments may be difficult, though organizations and developers shouldn't discount the possibility of retro-fitting better security protocols — or at least protecting themselves from the most serious vulnerabilities. Failing to prioritize IoT security in the months and years ahead would be unforgivable.

The stakes are high. Research from the McKinsey Global Institute predicts the annual economic impact of IoT globally could be between $3.9 trillion and $11.1 trillion by 2025.[7] But the consequences of poor IoT security may go well beyond economic damage — the opportunity is there for attackers to paralyze communities and the infrastructure on which they rely, or even to threaten life.

Let's get started

NTT DATA can support your organization with:

- Increased awareness of IoT on your network, including network segmentation
- Improved IoT device configuration management
- Improved IoT device log correlation and analysis within your security environment

Contact us today to learn more.

Sources

1. Kanellos, Michael. "152,000 Smart Devices Every Minute In 2025: IDC Outlines The Future of Smart Things." Forbes. March 3, 2016. https://www.forbes.com/sites/michaelkanellos/2016/03/03/152000-smart-devices-every-minute-in-2025-idc-outlines-the-future-of-smart-things/#7609f7714b63.
2. Hern, Alex. "Hacking risk leads to recall of 500,000 pacemakers due to patient death fears." The Guardian. August 31, 2017. https://www.theguardian.com/technology/2017/aug/31/hacking-risk-recall-pacemakers-patient-death-fears-fda-firmware-update.
3. Greenberg, Andy. "Hackers Remotely Kill a Jeep on the Highway—With Me in It." Wired. July 21, 2015. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.
4. Krebs, Brian. "Target hackers broke in via HVAC company." Krebs on Security. February 5, 2014. https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/.
5. Skerrett, Ian. "IoT Developer Trends Trends 2017 Edition." April 2017. https://ianskerrett.wordpress.com/2017/04/19/iot-developer-trends-2017-edition/.
6. Ponemon, Larry and Jones, Neil. "10 key findings from the Ponemon Institute's Mobile & IoT Application Security Testing Study." Security Intelligence. January 18, 2017. https://securityintelligence.com/10-key-findings-from-the-ponemon-institutes-mobile-iot-application-security-testing-study/.
7. Manyika, James, et. al. "Unlocking the potential of the Internet of Things." McKinsey & Co. June 2015. https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world.

Visit nttdataservices.com to learn more.

NTT DATA Services partners with clients to navigate and simplify the modern complexities of business and technology, delivering the insights, solutions and outcomes that matter most. As a division of NTT DATA Corporation, a top 10 global IT services and consulting provider, we wrap deep industry expertise around a comprehensive portfolio of infrastructure, applications and business process services.

NTT DATA
Trusted Global Innovator