INSIDER PRO
FROM IDG

EXPERT INSIGHT INTO HOW TECHNOLOGY DRIVES BUSINESS

INSIDER EXCLUSIVE

INSIDE IOT SECURITY: WHY IT'S YOUR biggest challenge

The internet of things encompasses connected devices on a mass scale, actionable data and innovative business models – **and also massive security headaches.**

POWERED BY CIO COMPUTERWORLD CSO InfoWorld NETWORKWORLD

IoT has emerged from the explosive growth of connected devices in industrial verticals, the consumer arena and enterprise networks. **The good news** is that it has generated massive amounts of data that can be analyzed and acted on, resulting in operational efficiencies and new, revenue-generating services. AI, though, may be at once the most transformative and least understood areas of technology today. Adding to the confusion, AI comprises concepts and terms that overlap and create misunderstanding about the field

The bad new: It's a security nightmare.

Vast IoT networks, transmitting data back to enterprise systems for analysis, have multiple points of weakness. The adoption of connected devices in every business sector is creating arguably the biggest tech-related security challenge ever.

Editor's NOTE

The numbers are mind-boggling. The number of connected devices globally could reach 30 billion by 2021, according IDC. That includes consumer items like watches, thermostats, and washing machines but also sensors on things like railway switches, telecom towers, and medical devices. All of this is in addition to sensors that have existed in manufacturing facilities for years.

IoT creates the ultimate security problem

IoT has produced the quintessential technology quandary: The value of such networks increases with the number of things that are connected, but so do security problems.

Because of the widespread adoption of connected devices, all business sectors have to be involved in related security issues, in consumer IoT, in enterprise IoT (EoT) and industrial IoT (IIoT).

One of the first rules of getting started in IoT is, if you are not sure whether your staff has a thorough understanding of the security issues involved, go no further until a full assessment is made.

What are IoT security problems and solutions?

IoT presents two basic challenges. First, IoT devices and systems represent valuable information and infrastructure: not just about consumer devices but buildings, vehicles, utilities and industrial machines, as well as information about users and their behavior. These are attractive assets for rogue nation-state actors and run-of-the-mill hackers alike. So, the number of potential targets as well as antagonists is virtually limitless, with no geographic boundary.

Secondly, the different types of devices, products, people, protocols, applications and computing systems involved means that there are multiple ways to attack any given network, along with related hacking techniques that can be used.

Fortunately, IoT has also given rise to best practices as enterprises of all stripes tackle the security challenges. So take heart. The challenges are great, but you can be helped by techniques for monitoring and managing endpoint devices, fast patching of system flaws, penetration testing, network gateways using the latest security software, and prioritization of exactly what needs to be secured.

METAMORWORKS / GETTY IMAGES

INSIDE

STAYING SECURE AS THE IOT TSUNAMI HITS

THINKSTOCK / NATALYA BUROVA / GETTY IMAGES

The ubiquitous adoption of devices in virtually every industry is creating a massive, global security gap, but data science can help rein in the risks

BY LESLIE K. LAMBERT

Just when we thought we were gaining control over our networks and computing environments, bam! Here comes the internet of things (IoT), and it's the wild, wild west all over again.

This new wave of device proliferation has moved more quickly than any other computing or technology phase we've experienced in modern times. IDC estimates that there were 13 billion connected devices in use worldwide last year, and that number could reach 30 billion in the next three years. To put this into perspective, Ericsson's most recent Mobility Report estimated that there are less than four billion active smartphone subscriptions active around the world. The IoT phenomenon is that big.

To comment on this story, visit Insider Pro's Twitter page.

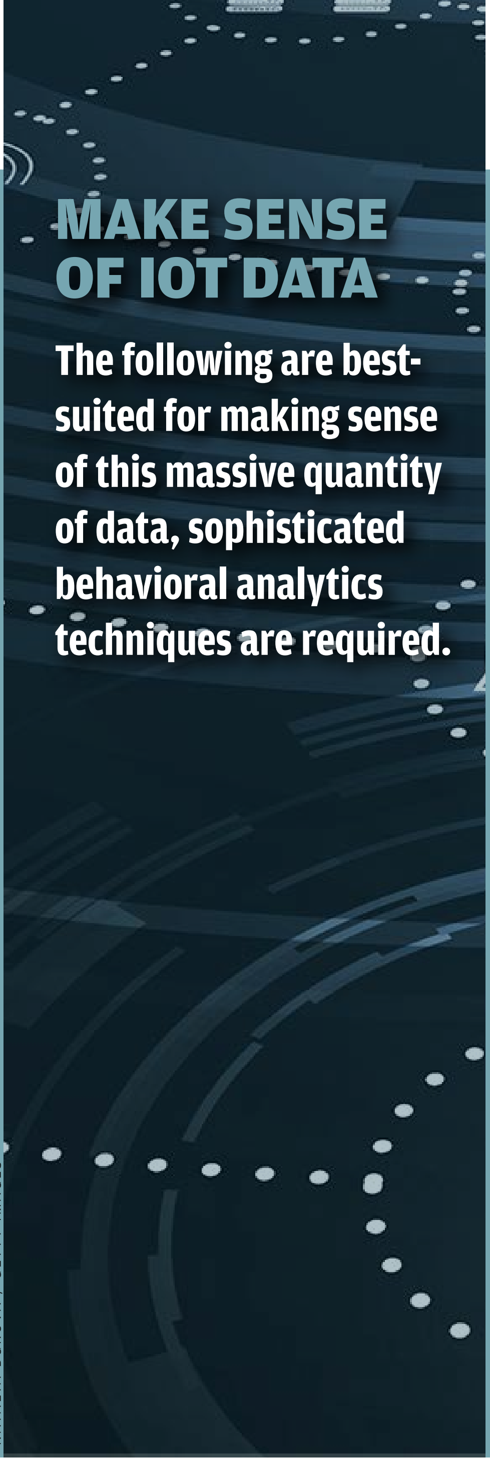
The more devices the better

The paradox of IoT is that its full potential is only realized when there is a large enough number of devices online to interact with one another. As the number and type of unsecured IoT devices has exploded, the amount of data they are generating has become nearly immeasurable. IoT devices have wiggled their way into every nook and cranny of computing, making our lives better, while at the same time, creating an overwhelming trail of log data that begs to be tamed and understood.

IoT devices are now touching almost every activity we engage in as consumers, and driving all forms of enterprise and industrial automation, most of which we have little or no knowledge of. They are generating mountains of data on the activities of individuals and machines around the world.

No seatbelts

Meanwhile, due to the simplistic and incomplete security models used in IoT devices, they are vulnerable to potential wide-scale hacking. This gap can lead to the compromise of enterprise networks, industrial processes, even


NATALYA BUROVA / GETTY IMAGES

MAKE SENSE OF IOT DATA

The following are best-suited for making sense of this massive quantity of data, sophisticated behavioral analytics techniques are required.

Cohort Analysis: associates devices by common characteristics, experiences, or time frames to understand what a group of devices is doing on a regular basis – and determine whether that set of behaviors is normal or appropriate. This method is looking for continuity of actions of a group of devices, including any instances of attrition. For example, IoT edge-based thermometers in a building should not be streaming inappropriate data to the internet.

Funnel Analysis: as the name implies, performs a narrowing of devices based on their actions as they move along a sequence to an end state. In the use case above, funnel analysis would identify which subset of the building thermometers are exhibiting the rogue behavior. Often, funnel analysis and cohort analysis are used together to demonstrate when a group of devices drop out at a particular stage of the expected sequence.

Path Analysis: examines the points and actions taken by devices along a known ‘path’. This analysis can identify streamlined paths to a desired state, including any barriers along the way that prevent the device from moving to the defined process and end state. This method goes beyond simple profiling of device behavior and provides unique visibility and insight into why devices are doing what they are doing, and at what points are they doing it.

critical infrastructure, with potentially disastrous consequences. In the event of a catastrophe, it is highly unlikely that IoT technologies could be dismantled, since they have become embedded in a pervasive manner. The proverbial horse is already out of the barn and enjoying the lush green grass of the pasture!

The myriad of security issues related to IoT implementations means we need to reduce the risks associated with a compromise by bad actors or disruptions caused by human error.

Starting point: IoT security is a data problem

A good way to begin addressing IoT security risks is focusing on what the data produced by devices is telling us. This can be accomplished using data science to determine what’s happening and who’s doing what. In the world of IoT, it does not matter if the “user” is a device, car or a machine. What’s important is understanding the patterns and behaviors associated with them.

Given the breakneck pace of IoT adoption, IT leaders need to rein in these devices in order to manage the risks they are introducing. Using artificial intelligence and behavioral analytics to process and monitor the enormous amount of data generated by IoT devices is the most logical path for detecting anomalous conditions, a starting point for remediating them before widespread damage can occur. ◆

LESLIE K. LAMBERT *is a contributor to CIO.com*

METAMORWORKS / GETTY IMAGES

A CORPORATE GUIDE TO Addressing IoT Security Concerns

The benefits of the internet of things are potentially great and can be achieved with less risk of harm by following these steps

BY BOB VIOLINO

The internet of things (IoT) promises benefits for companies, including rich supplies of data that can help them more effectively serve their customers. There's also a lot to be worried about.

Because so many devices, products, assets, vehicles, buildings, etc. will be connected, there is a possibility that hackers and other cyber criminals will try to exploit weaknesses.

"In IoT ecosystems, where myriad device types, applications and people are linked via a variety of connectivity mechanisms, the attack vector or surface is potentially limitless," says Laura DiDio, principal analyst at research and consulting firm ITIC.

"Any point in the network — from the network edge/perimeter to corporate servers and main line-of-business applications to an end-user device to the transmission mechanisms [is] vulnerable to attack. Any and all of these points can be exploited."

As a result, IoT security ranks as a big concern for many companies. Research firm 451 Research recently conducted an online survey of more than 600 IT decision-makers worldwide and found that 55 percent rated IoT security as their top priority when asked to rank which technologies or processes their organizations considered for existing or planned IoT initiatives. The very nature of IoT makes it particularly challenging to protect against attacks, the report says.

What can enterprises do to strengthen the security of their IoT environments? Here are some suggested best practices from industry experts.

SUGGESTED Best Practices

Identify, track, and manage endpoint devices

Without knowing which devices are connected and tracking their activity, ensuring security of these endpoints is difficult if not impossible.

"This is a critical area," says Ruggero Contu, research director at Gartner Inc. "One key concern for enterprises is to gain full visibility of smart connected devices. This is a requirement to do with both operational and security aspects."

For some organizations, "this discovery and identification is about asset management and less about security," says Robert Westervelt, research director of the Data Security Practice at International Data Corp. (IDC). "This is the area that network access control and orchestration vendors are positioning their products to address, with the added component of secure connectivity and monitoring for signs of potential threats."

Companies should take a thorough inventory of everything on the IoT network and search for forgotten devices that may contain back doors or open ports, DiDio says.

Patch and remediate security flaws as they're discovered

Patching is one of the foundational concepts of good IT security hygiene, says John Pironti, president of consulting firm IP Architects and an expert on IoT.

"If a security-related patch exists for an IoT device, that is the vendor's acknowledgement of a weakness in their devices and the patch is the remediation," Pironti says. "Once the patch is available, the accountability for the issue transfers from the vendor to the organization using the device."

It might make sense to use vulnerability and configuration management, and this would be provided in some cases by vulnerability-scanner products, Westervelt says. Then do the patching and remediation. "Configuration management may be an even bigger issue opening weaknesses than patching for some enterprises," he says.

It's important to remember that IoT patch management is often difficult, Contu says. "This is why it is important to do a full asset-discovery to identify where organizations are potentially vulnerable," he says. "There is as a result the need to seek out alternative measures and models to apply security, given [that] patching is not always possible." Monitoring network traffic is one way to compensate for the inability to apply patches, Contu says.

Prioritize security of the most valuable IoT infrastructure

Not all data in the IoT world is created equal. "It is important to take a risk-based approach to IoT security to ensure high-value assets are addressed first to try and protect them based on their value and importance to the organization [that] is using them," Pironti says.

In the case of IoT devices, an organization might have to contend with exponentially more devices then it did with traditional IT gear, Pironti says. "It is often not realistic to believe that all of these devices can be patched in short periods of time," he says.

METAMORWORKS / GETTY IMAGES

> "… **gain full visibility of smart connected devices.** This is a requirement to do with **both operational and security aspects."**
>
> -RUGGERO CONTU, RESEARCH DIRECTOR AT GARTNER INC.

Pen test IoT hardware and software before deploying

If hiring a service provider or consulting firm to handle this, be specific about what type of penetration testing is needed.

"The pen testers I speak to do network penetration tests along with ensuring the integrity of network segmentations," Westervelt says. "Some environments will require an assessment of their wireless infrastructure. I believe application penetration testing is a slightly lower priority within IoT for now, with exception for certain use cases."

Penetration testing should be part of a broader risk assessment program, Contu says. "We expect an increasing demand for security certification [related to] these activities," he says.

If an actual IoT-related attack occurs, be ready to act immediately. "Construct a security response plan and issue guidance and governance around it," DiDio says. “Put together a chain of responsibility and command in the event of a successful penetration.”

Know how IoT interacts with data

You might want to focus on secure sensor-data collection and aggregation, Westervelt says. This could require both cyber security and physical anti-tampering capabilities, depending on where the device will be deployed and the device’s risk profile.

“It may require hardware and/or software encryption – depending on the sensitivity of the data being collected – and PKI [public key infrastructure] to validate device, sensors and other components,” Westervelt says.

To comment on this story, visit Insider Pro’s Twitter page.

“Other IoT devices like point-of-sale systems may require whitelisting, operating-system restrictions and possibly anti-malware, depending on the device functionality.”

Don’t use default security settings

In some cases, organizations will choose security settings according to their unique security posture.

“If a network security appliance is being implemented in a critical juncture, some organizations may choose to deploy it in passive mode only,” Westervelt says. “Remember that with industrial processes – where we are seeing IoT sensors and devices being deployed – there may be no tolerance for false positives. Blocking something important could cause an explosion or even trigger a shutdown of industrial machinery, which can be extremely costly.”

Changing the security settings can also apply to the actual devices connected via IoT. For example, there’s been a distributed denial-of-service attack that arose from the compromise of millions of video cameras configured with default settings.

Provide secure remote access

Remote-access weaknesses have long been a favorite target of attackers, and within IoT a lot of organizations are looking for ways to provide contractors with remote access to certain devices, Westervelt says.

“Organizations must ensure that any solution that provides remote access is properly configured when implemented, and other mechanisms are in place to monitor, grant and revoke remote access,” Westervelt says “In some high-risk scenarios, if remote access software is being considered, it should be thoroughly checked for vulnerabilities.”

Segment networks to enable secure communication

Segmenting IoT devices within networks enable organizations to limit their impact if they are found to be acting maliciously, Pironti says.

“Once malicious behavior is identified from an IoT device, it can be isolated from communicating with other devices on the network until they can be investigated and the situation remediated,” he says.

> * “If the company policy is more than a year old, it’s outdated and needs revision to account for IoT deployments,” Laura DiDio says.

When segmenting IoT devices, it is important to implement an inspection element or layer between the IoT network segment and other network segments to create a common inspection point, Pironti says. At this point, decisions can be made about what kinds of traffic can pass between networks, as well as a meaningful and focused inspection of traffic.

This allows organizations to direct inspection activities at specific traffic types and behaviors that are typical to the IoT devices instead of trying to account for all traffic types, Pironti says.

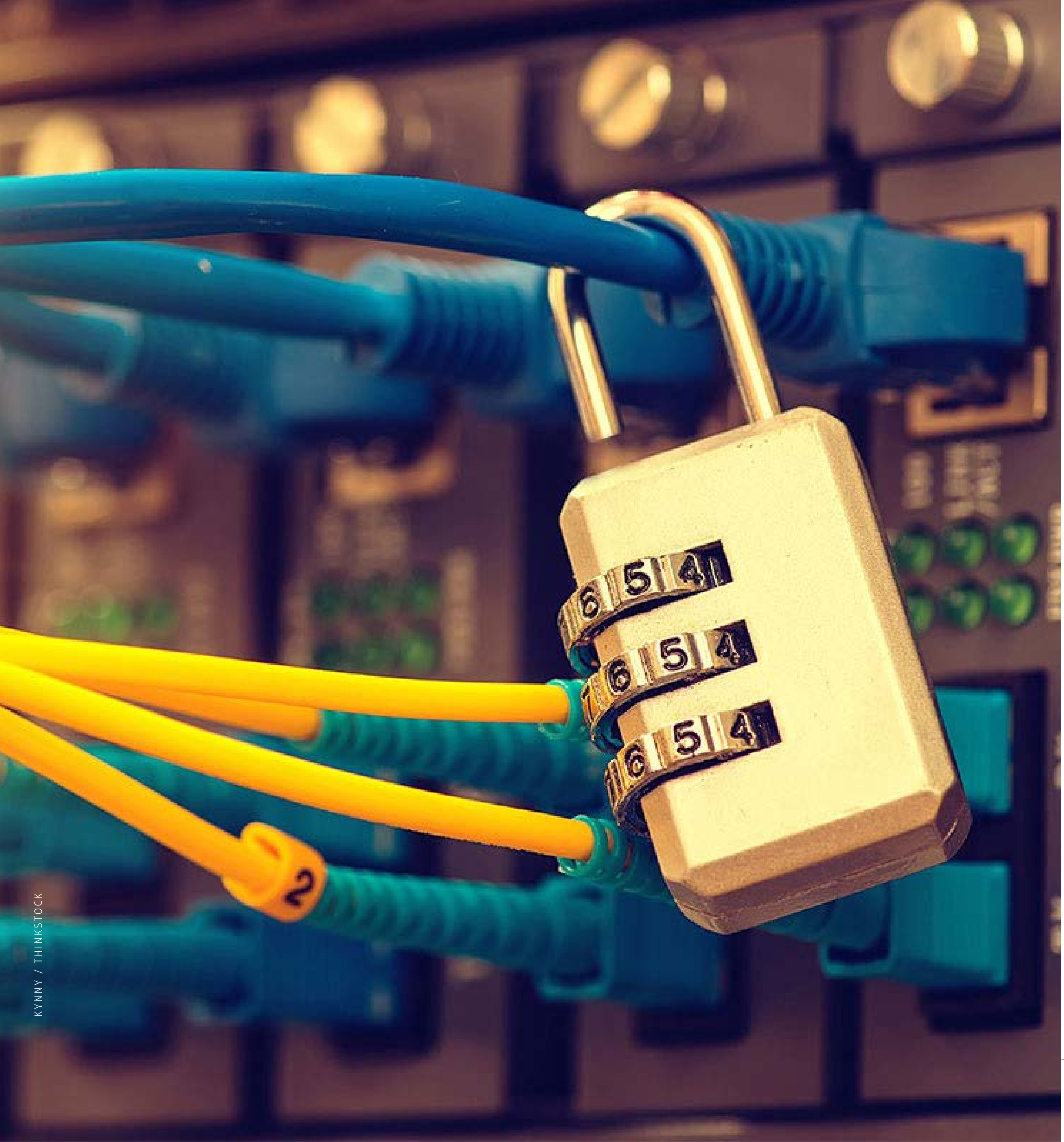
Remember people and policies

IoT is not just about securing devices and networks. It’s also crucial to consider the human element in securing the IoT ecosystem, DiDio says.

“Security is 50 percent devices and protection, tracking and authentication mechanisms and 50 percent the responsibility of the humans who administer and oversee the IoT ecosystem,” she says. “It is imperative that all stakeholders from the C-level executives to the IT departments, security administrators, and the end users themselves must fully participate in defending and securing the IoT ecosystem from attacks.”

In addition, review and update the existing corporate computer security policy and procedures. “If the company policy is more than a year old, it’s outdated and needs revision to account for IoT deployments,” DiDio says. “Make sure that the corporate computer security policy and procedures clearly specify and articulate the penalties for first, second and third infractions. These may include everything from warnings for a first-time offense up to termination for repeat offenses.” ◆

BOB VIOLINO *is a freelance writer who covers a variety of technology and business topics.*



KYNNY / THINKSTOCK

The Enterprise of Things troubling lack of security

Enterprise deployment of IoT devices brings a unique requirement to enterprise security that is distinct from normal end points and data centers - here are three strategies to address it

BY JACK GOLD

When it comes to security and manageability, corporate devices must have far more stringent requirements than consumer IoT devices, which often have virtually no built-in security.

To make the distinction between the consumer and the business world, I've called corporately connected/deployed devices the Enterprise of Things (EoT). EoT will comprise embedded sensors of all types, including tooling, usage monitors, personal concierge devices, location-based sensors, etc.

Making the matter even more urgent is the growing number of deployed EoT devices, which is expected to increase significantly over the next two to three years. (I estimate there will be more “things” in an enterprise than PC and mobile phone clients combined within three to four years.)

As a result, it is imperative that companies address the growing security requirements for these devices in order to avoid any potential catastrophic events (e.g., hacking of automated tools, disruption of processes, autonomous vehicles losing control, drones crashing, GPS systems redirected, etc.). While some may be costly in terms of data or production loss, others may be downright deadly.

3 STRATEGIES FOR IMPROVING EOT SECURITY

There are many issues involving EoT security, which should be seen as an integrated component of overall enterprise security and not a unique requirement. For this brief discussion, I’ll focus on three key points that can easily make or break an EoT installation.

1 > Hardening EoT devices

It’s imperative that companies deploy EoT devices that are built on secure and verifiable architectures for both hardware and software. Technology such as ARM’s TrustZone or Intel’s Trusted Execution Technology provides a secured area of the chip that can be used to store critical data that can securely identify and/or run kernel-level code to prevent malicious activity. Root of trust systems, now prevalent in many of the newer generation of chips and proven in the mobile device world, also provide a way to verify the OS on booting and/or before running so as to prevent hijacking of the device.

Unfortunately, many older, and even some current, EoT devices are built on lower-level, less-functional chips that do not provide such technology. And consumer-grade IoT devices generally have no protection. It’s imperative that companies identify and replace any such devices. The ease with which they can be hacked is appalling, and the damage potential is great. This is a liability enterprises should eliminate as soon as possible.

2 > Securing all code running on these devices

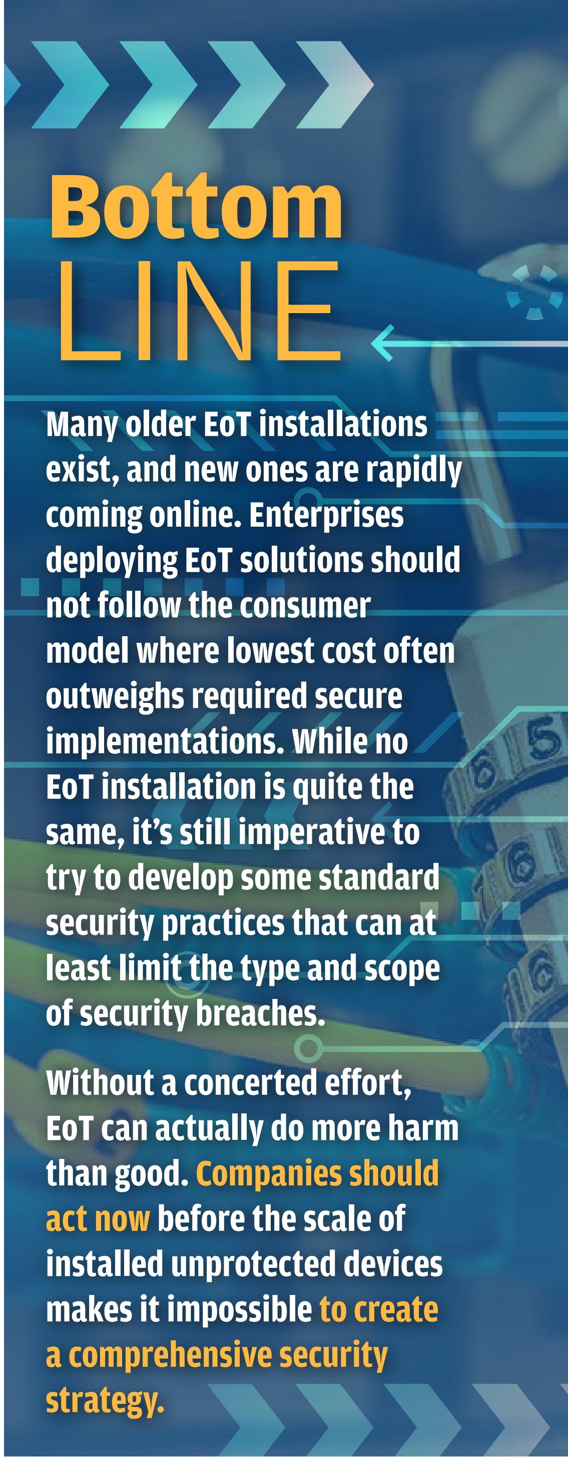
Code security requires both a hardware and software approach that work in unison. As indicated above, modern chips have built-in security functions to protect against errant code that can be used to hijack a device. In conjunction with a hardened operating system, such as BlackBerry QNX (which has been used in mission-critical applications for many years) and newer versions of Android and Windows for IoT, a combined front against malicious activity can be established.

But that is not enough. It’s also imperative that companies test their apps for any potential avenues of attack. Many test tools exist for apps running on virtually any OS, but many EoT products still contain custom-built, low-level code that has never been adequately screened. Along with the imperative to check the hardware technology stated above, it is equally important to assure that the software is fully secured through fault testing and simulations.

3 > Monitoring of all network traffic to/from EoT devices

Finally, its critical to prevent the hostile takeover of large numbers of devices. This has occurred in many consumer devices where DDoS attacks were delivered from wireless cameras, Wi-Fi access points, etc. An effective way to prevent such activity is to monitor traffic to and from the EoT endpoints. Many network monitoring tools already exist (e.g., RSA NetWitness, Citrix Netscaler), and they can prove valuable in finding suspicious network activity that could point to malicious behavior. While I believe all organizations should deploy network traffic monitoring as a security measure, it’s doubly important for EoT devices that could affect safety and/or operations of the organization. ◆

JACK GOLD *is a contributor to Network World*



Bottom LINE

Many older EoT installations exist, and new ones are rapidly coming online. Enterprises deploying EoT solutions should not follow the consumer model where lowest cost often outweighs required secure implementations. While no EoT installation is quite the same, it’s still imperative to try to develop some standard security practices that can at least limit the type and scope of security breaches.

Without a concerted effort, EoT can actually do more harm than good. Companies should act now before the scale of installed unprotected devices makes it impossible to create a comprehensive security strategy.

KOHB / GETTY IMAGES

EDGE COMPUTING: A Place to Address IOT Security Concerns

BY JON GOLD

NATALYA BUROVA / GETTY IMAGES

Edge computing can greatly improve the efficiency of gathering, processing and analyzing data gathered by arrays of IoT devices, but it's also an essential place to inject security between these inherently vulnerable devices and the rest of the corporate network.

First designed for the industrial IoT (IIoT), edge computing refers places placing an edge router or gateway locally with a group of IIoT endpoints, such as an arrangement of connected valves, actuators and other equipment on a factory floor.

Because the lifespan of industrial equipment is frequently measured in decades, the connectivity features of those endpoints either date back to their first installation or they've been grafted on after the fact. In either case, the ability of those endpoints to secure themselves is seriously limited, since they're probably not particularly powerful computing devices. Encryption is hard to cram into a system-on-a-chip designed to open and close a valve and relay status back to a central control pane.

IIoT can be a security blind spot

As a result, IIoT is a rich new target opportunity for malicious hackers, thanks in large part to the difficulty of organizing and gaining visibility into what's happening in IIoT, according to Eddie Habibi, CEO of PAS Global, an industrial cybersecurity company who has been working in the industrial control and automation for about 15 years.

A lot of connected IIoT devices have known, exploitable vulnerabilities, but operators might not have the ability to know for certain what systems they have on their networks. "The hardest thing about these older systems that have been connected over the past 25 years is that you can't easily do discovery on them," he said. Operators don't know all the devices they have, so they don't know what vulnerabilities to patch.

It'll be decades, Habibi said, before many IIoT users – whose core devices can date back to the 1980s and even the 1970s – update this important hardware.

Edge networks provide security

That's where the edge comes in, say the experts. Placing a gateway between the industrial endpoints and the rest of a company's computing resources lets businesses implement current security and visibility technology without ripping and replacing expensive and IIoT machinery.

The edge model also helps IIoT implementations in an operational sense, by providing a lower-latency management option than would otherwise be possible if those IIoT endpoints were calling back to a cloud or a data center for instructions and to process data.

Most of the technical tools used to secure an IoT network in an edge configuration are similar to those in use on IT networks – encryption, network segmentation, and the like. Edge networking creates a space to locate security technologies that limited-capacity endpoints can't handle on their own.

Mike Mackey is CTO and vice president of engineering at Atonomi, makers of a blockchain-based identity and reputation-tracking framework for IIoT security. He said edge computing adds an important layer of trust between a company's backend and its potentially vulnerable IIoT devices.

"[N]ow you're adding network translation to the end-to-end communication between that IoT device and whatever it's ultimately communicating with, which, today, is typically the cloud," he said.

> "Edge computing adds an **important layer** of trust between a company's backend and its potentially vulnerable IIoT devices," Mike Mackey says.

Other experts, such as Windmill Enterprise CEO Michael Hathaway, also highlighted that widely used cloud-based backends pose problems of their own. Enterprises are losing control over their security policies and access with every new cloud service they subscribe to, he said.

"Enterprise customers can be very nervous about hooking up an automation system directly to the Internet – it needs a last layer of intelligence and security," Hathaway said.

Consequently, some of the most effective IIoT implementations can be those that leave the existing structures and networks in place – hence the popularity of the edge architecture, which works both as a buffer and a link between the IT network and a company's operational technology.

Russ Dietz, chief product security officer at GE Digital, said that old-yet-irreplaceable technology already on the factory floor plays an enormous role in shaping the IIoT infrastructure laid on top of it.

"Over time, we might migrate to a fully digital world where we blend those two together, but because industrial is going to live in this very long-tail environment, we have to be able to provide separate trust for both of those," he said. "So we may weight how much we trust sensors in a different category than how much we trust a control system."

Edge networks must fit unique sets of needs

According to Hathaway, it's important to recognize that not all edge solutions are created equal, and that different businesses will have different requirements for an edge computing deployment. An automotive manufacturer might need to track a lot of process-oriented data and rate information about productivity, while an oil-production facility is likely to need to track things like pressures and volumes through a vast array of pipelines.

"You can't possibly have provided a cookie-cutter solution," said Hathaway, adding that, while the tools and approaches used will have commonalities, everyone's security needs will be different.

The eventual hope for most IIoT deployments is that they provide enough machine-generated data to help businesses make smart decisions for the future, according to Simon Dowling, CTO of edge compute vendor ORI.

Protecting the data those machines send back for analysis – whether at the edge layer or back in the cloud or data center – is of paramount importance.

"As we're moving towards a world where there is – whether it's industrial IoT or it's more commercial/consumer-focused IoT – a level of expectation that these devices will provide more meaningful action," he said.

And if businesses want to stay on top of cybersecurity threats, they have to realize that it's not simply a matter of pushing out updates and getting the latest and greatest technology up and running on their systems, said Aruba/HPE's vice president of strategic partnerships, Mike Tennefoss. It's also understanding the way those updates and additions will tie into the operational technology stack.

"Security is the heart and soul of IT, and what you see happening is that IT systems and processes of cybersecurity are pushing down deeper and deeper into the operational technologist's realm," he said. ◆

JON GOLD *covers IoT and wireless networking for Network World.*

BUILD SECURITY INTO YOUR IOT PLAN OR RISK ATTACK

LEO WOLFERT / GETTY IMAGES

CHUYN / GETTY IMAGES

There's huge potential with the IoT, but security must be built into a company's plan and not tacked on at the end

BY ZEUS KERRAVALA

The internet of things (IoT) is no longer some futuristic thing that's years off from being something IT leaders need to be concerned with. The IoT era has arrived.

A proof point is the fact that when I talk with people about their company's IoT plans, they don't look at me like a deer in headlights as they did a few years ago. In fact, often the term "IoT" doesn't even come up. Businesses are connecting more "things" to create new processes, improve efficiency, or improve customer service.

As they do, though, new security challenges arise. One of which is there's no "easy button." IT professionals can't just deploy some kind of black box and have everything be protected. Securing the IoT is a multi-faceted problem with many factors to consider, and it must be built into any IoT plan.

Top challenges associated with securing IoT endpoints

» **Physical security is overlooked.** Businesses devote a significant amount of time and energy to cybersecurity. However, physical security is often an afterthought or overlooked altogether. Devices need to be protected against theft or hacking of the hardware. Because IoT is often deployed by non-IT individuals, there can be many devices that IT departments are unaware of. These unknown devices can be breached from a console or USB port and create backdoors into other networks. IT and cybersecurity teams need a better way of automating the discovery of IoT endpoints.

» **Traditional security doesn't work with IoT.** Today's cybersecurity is primarily focused on protecting the perimeter of a network with a large, expensive firewall, but ZK Research found only 27 percent of breaches occur there. (Note: I am an employee of ZK Research.) Although firewalls are still required to protect the network, IoT devices enable breaches to occur inside the network. IoT requires organizations to rethink their security strategies and focus on the internal network. Another factor with IoT devices is that many connect back to a cloud service to provide status updates or provide other information. This punches a legitimate but hackable hole through the firewall from the inside.

» **Many IoT devices are inherently insecure.** Most IT endpoints such as PCs and mobile devices have some embedded security capabilities or can have an agent placed on them. While many IoT devices have old operating systems, embedded passwords, and no ability to be secured by a resident agent. This underscores the importance of rethinking security in a world where everything is connected. If the endpoint can't be secured, then protection needs to move to the network.

» **Cybersecurity is growing in complexity.** Protecting against external threats used to be a straightforward process: Place a state-of-the-art firewall at the perimeter, and trust everything inside of the network. That made sense when all the applications and endpoints were under the control of the IT department. Today, however, workers bring in their own devices, and the use of cloud services is extensive, creating new entry points. To combat this, security teams have been deploying more niche point products, which often increases the level of complexity. My research has found that organizations use an average of 32 security vendors, and this number is growing — leading to an environment that is becoming increasingly complex and less secure. Also, IT departments struggle today to manage the current set of connected devices. Adding three to five times more endpoints will overwhelm many security teams.

LEO WOLFERT / GETTY IMAGES

Organizations use an average of 32 security vendors, and this number is growing – leading to an environment that is becoming increasingly complex and less secure.

» **The number of blind spots has exploded.** Cobbling together a patchwork of security tools from different vendors may seem like a sound strategy, as each device was meant to solve a specific problem. However, this approach leaves massive blind spots because the devices have little to no communications among them. Also, this architecture lacks automation, so the configuration of these devices must be done one at a time, meaning changes can often take months to implement. This delay puts organizations at serious risk.

Failure to have a comprehensive IoT strategy puts you at risk

It's important to understand how big the risk is of not having a comprehensive IoT security strategy. Success with IoT requires a number of processes work together. A breach at any point can cause an outage and a possible loss of sensitive data. In many verticals, such as healthcare, state and local government, manufacturing and banking, IoT services are mission critical, so any kind of outage can cost companies millions.

There is tremendous business value in IoT, and I strongly recommend businesses be aggressive with deployments. However, I also advise building security into the plan instead of trying to implement it after deployment. ◆

ZEUS KERRAVALA *is the founder and principal analyst with ZK Research.*