

ANOMALIX WHITE PAPER

Securing the Internet of Things and Industry 4.0

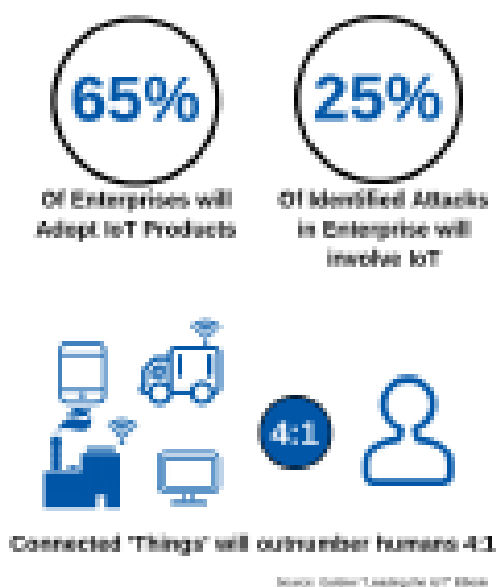


Securing the Internet of Things and Industry 4.0

Every day we move toward a more interconnected world. Every day, new devices, from manufacturing equipment to healthcare devices and financial services are being hooked up to the internet. These items help us live more productive lives by communicating with one another and with us. Collectively, these devices are known as the Internet of Things (IoT). The IoT, along with cyber-physical systems, cloud computing and cognitive computing in the manufacturing world make up Industry 4.0.

According to experts at Gartner, approximately 20 billion IoT devices will be connected in 2020, and that number will only grow in the future. Cars, medical devices, houses, refrigerators – it's all coming to market at a rapid pace. To be the first to market, many vendors are rushing their products into stores before a full security audit is complete. This leaves plenty of room for bugs, gaps in firewalls, and simple human error. Security will also be threatened as IoT evolves and needs to integrate with more and more new technologies. By 2020, Gartner estimates internet-connected things will outnumber humans 4-to-1. In addition, more than 25% of identified attacks in enterprises will involve the IoT, although the IoT will account for less than 10% of IT security budgets. IT professionals are focused on proactively finding ways to keep it all secure.

By 2020



Security Threats in IoT and Industry 4.0

Consumerized IoT

Corporate IT teams may be more prepared to properly secure “enterprise grade” IoT, the devices they connect to on a daily basis to maintain operations. These devices can be properly vetted, firewalled, and secured. But how can these companies protect their data from other IoT devices that may connect with them – Items like cell phones, smartwatches and fitness trackers, thermostats, etc.? If it connects to a router, any consumer items pose a threat to IoT and Industry 4.0 security since these devices often lack the comprehensive security features of enterprise IoT devices.

A Lack of Transport Encryption

Data may be fully encrypted when stored in your device, but lose that encryption when being transmitted to a second device – for instance, when your Fitbit sends your vitals to your cell phone, or when your pacemaker updates the data to your hospital server. During the transport process, hackers may be able to access the data.

Data Sharing

Enter any coffee shop with your smartphone, and you will be able to access the data of other IoT device users. Any device that connects to wifi is at risk. For in-house IoT, the problem is mitigated with proper firewalls and password encryption. It's harder to protect your IoT devices in public.

Insufficient Authentication Protocol

Creating firewalls, passwords, defense algorithms, and authentication processes are essential to protecting your security and the integrity of your IoT. But even with these things in place, hackers may be able to access your data if you have insufficient authentication protocols in place. Firewalls need to be accessible in-house, meaning there need to be ways around them. Be sure to have strong security practices in place to accurately identify who is allowed to circumvent this security and who is not.

Potential security threats as new devices, AI, and robotics are implemented

There is no way to know for sure what the future holds for IoT and Industry 4.0, but highly intelligent AI devices are on the way. The introduction of Siri on the iPhone, smart manufacturing (and smart factories), smart cars and more, are fundamentally changing the way we live. The following are potential threats to the Internet of Things and Industry 4.0 in the wake of AI and robotics.

Intelligent Communication between IoT Devices

All IoT devices have some level of AI. With the implementation of smart manufacturing and smart cars, these devices may soon be able to communicate on a much higher level. How will we protect individual connected IoT devices from others in the same web?

For instance, Tesla CEO Elon Musk has gone on the record to say that the difference between Tesla smart cars and other smart cars is that Tesla's cars work on a network: essentially when one car learns something, they all learn. How far can this intelligent communication go? Will IoT devices be able to elect to access data from other devices? Will firewalls and password protection be able to hold

up against smart IoT devices? Cybersecurity programs must be built to evolve with the always changing business environment. We need professionals who are skilled in managing risk, preventing security breaches and finding ways to keep data secure at every step of the collection process.

Increased Vulnerability

Just as we can use AI to improve cybersecurity, it can also be used to attack cybersecurity systems. As reported in the Malicious Use of Artificial Intelligence, "The use of AI to automate tasks involved in carrying out cyber attacks will alleviate the existing trade-off between the scale and efficacy of attacks." In other words, carrying out cyber attacks with AI will be simpler and cheaper than ever.

Threats of the Smart Factory and Virtual Manufacturing

Gone are the days of factories that run 100% on human resources. We have moved almost entirely to automated factories, with employees operating the machines to make sure they're functioning correctly. And soon, we will need even fewer employee oversight. Smart manufacturing (the use of smart factories) enables all information about the manufacturing process to be available when and where it is needed across entire manufacturing supply chains. The global market for smart factories is expected to grow by 13.2% and exceed \$39 billion between 2018-2028. Security teams must understand the threats of the smart factory and virtual manufacturing as they are incorporated into organizations.

GPS

Real-time GPS data allows smart factories to manage shipments from vendors, but the GPS data is open to potential hacking. GPS systems need to be firewalled and disconnected from other IoT smart devices that may contain company or customer data.

Cognitive Technologies

As more and more pieces of the digital supply chain become automated, customers are demanding higher-quality conversations with AI systems - this has led to the emergence of cognitive technology. These cognitive technologies complement or sometimes replace employees, to uncover marketing insights from customers and automate mundane tasks in the supply chain. Sometimes in the form of chatbots or AI, these systems are new and therefore do not have established best practices for security, but it's a good idea to consult with a professional to encrypt and secure the incoming data from users.

Workplace Safety

Outside of the scope of security, IoT in smart factories also increases the risk of workplace-related injuries. Any glitch in the system could cause machines to malfunction, which could make for an unsafe work environment. To prevent these issues, it's vital that you incorporate compliance practices with all of your IoT and Industry 4.0 connected devices.

Vision

To successfully secure IoT devices and smart factories, security leaders should:

- Gain visibility into devices that have network access to define governance
- Move IoT devices to the same network under one firewall
- Separate home and business connected devices
- Turn off devices when they are not in use
- Utilize data encryption whenever possible
- Ensure security software is always updated
- Create a roadmap to adopt new devices into the practice

Security leaders and staff must expand their knowledge of the new conditions and incorporate IoT and Industry 4.0 devices into their security programs. Leaders should know that all connected devices are a risk without proper security policies and governance.

Where to Begin?

Security begins with visibility. Security leaders should gain insight into all connected devices, access, resources, usage, and identities across the organization. Knowing the cyber risks involved with IoT and Industry 4.0 is essential but finding practical ways to protect your data is more critical. By gaining visibility into all connected devices, security teams can begin developing policies to manage, support and secure all IoT devices.

Conclusion

IoT and Industry 4.0 security is more vital than ever. Ignoring the threats to the Industry is a surefire path to put organizations at risk. Anomalix can solve your IoT and Industry 4.0 challenges by building custom solutions to properly define governance processes, policies, and lifecycle management. As trusted advisors, our Subject Matter Experts (SME) begin by defining business initiatives and determining how IoT devices can be integrated into the security infrastructure and create a roadmap to adopting all new devices.

What are the Results?

It takes more than awareness of security challenges to properly secure an organizations IoT and Industry 4.0 devices. In order to properly secure and govern devices, a number of steps need to be taken to protect connected devices from unwanted access.

Identify All Connected Devices

By identifying all devices connected to the internet, security programs gain visibility into all potential access points. Once devices are identified, define access governance processes, policies, and lifecycle management. This allows your organization so secure itself while also creating a program for new devices to be added in the future.

Move all IoT devices to the same network (and add a firewall)

Having all (firewall protected) IoT devices connected to the same network allows you to restrict any incoming traffic with network encryption. You can also profile traffic to identify anomalies that could pose a threat to your organization's security.

Separate Home and Business Devices

If a cybercriminal hacks a network, it's important to limit access to the amount of data and information attainable. Keeping devices separated whenever possible limits the ability for breaches that span across work and home data.

Turn Off Devices When Not in Use

As long as IoT devices have power, they are connected to the network. Power down devices when not in use including those at work or home. In addition, cover cameras and microphones on devices with when not active. Make sure smaller devices are kept in safe places where outsiders will not have access to attempt to change the passwords or get around firewalls.

Embrace Encryption

Whenever possible, encrypt your data. To be truly secure, you can limit access to your network to devices that are encrypted.

Update your Systems

It is not uncommon to install security software, firewalls, and other protection to your network and then "forget" to run the required updates. Make sure to always update your IoT device security according to manufacturer recommendations. When a device outgrows its security systems, it's time to replace it.

The growth of IoT devices has been exponential. With 20 billion IoT devices, including medical devices, cars, factory equipment, and robots, estimated to be connected in the near future, it must be a top priority to manage, support and secure IoT devices. Considering the industry is still in its infancy, now is the perfect time to integrate IoT devices into the existing security infrastructure. Considering the complexity of IoT devices, a proper governance model needs to be in place with rules and policies to protect organizations.



ANOMALIX

Third-Party Identity Management in a Decentralized World

Contact: info@anomalix.com

Headquarters
1180 Town Center Dr.
Suite 100
Las Vegas, NV 89144