KASPERSKY lab

INTERNET OF THREATS

SECURITY IN THE GROWING IOT MARKET

We live in a connected world. Your car relays data from dozens of onboard computers. Your house can be heated, cooled and secured according to your unique specifications. Businesses move goods and services with great efficiency and little human interaction. But how well is it all secured?

Living in a Connected World

With the number of connected "things" currently outnumbering people on the planet by 5:1, we are clearly in the era of the Internet of Things (IoT).[1] According to Gartner, there will be **6.4 billion connected "things" used worldwide in 2016, with 5.5 million new products connecting daily.**

The potential of this technology to improve customer experiences, move goods and services more efficiently and help businesses to capture data is enormous.

But where there is business opportunity, there is cybercrime. And that's where things get interesting.

What is IoT?

The Internet of Things (IoT) refers to the network of physical devices, vehicles, buildings and other devices that enables objects to select and exchange data. In practice, that means your smart coffee maker, home security and even your car can be considered part of the Internet of Things ecosystem.

We already live in a connected world where data about your home's temperature can be relayed back to you quickly, where cars operate with dozens of onboard computers and where you can access cameras in your home right from your smartphone.

The question is, how well is it all secured?

What's the risk?

Ask cybersecurity experts about the Internet of Things (IoT) and you will likely hear three observations consistently:

- The coming wave of connected products is unlike anything we could imagine, linking people, transportation and infrastructure in a way that will change the way we live, work and move from place to place. It's a wave that has already reached every corner of the globe with some predicting a **CAGR of 23% in IoT annual growth.**[2]
- Devices and things that are connected are being produced faster than architecture and security can keep up with them.
- Many of these "things" are being created without security in mind, making them only as strong as their weakest link.

So, where does that leave us? Connected. Informed. But not as secure as we need to be.

With the **Internet of Things exposing more attack surfaces** for cybercriminals to exploit, we'll take a closer look at some of the predictions around the oncoming wave of IoT and what we at Kaspersky Lab believe will be the best way to protect yourself and your business.

20.8 BILLION

Number of connected "things" in use worldwide by the year 2020, according to Gartner.[3]

[1] *5 IoT Trends to Expect in 2016*
[2] *Ericsson's Mobility Report*
[3] *Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent from 2015*

Home is Where the Security Starts

For many people, their first introduction to the Internet of Things (IoT) comes at home in the form of their smart refrigerator, coffee maker or home security system. Most people don't think of these things as part of the IoT ecosystem, but they are. **Most people also don't realize that many of these items have weak security and could be a potential breach for both homes and businesses.**

In November 2015, David Jacoby, a researcher on Kaspersky Lab's GReAT (Global Research and Analysis Team), tested several items in his home to see if they were hackable. Amongst a smart TV, an IP camera, coffee maker and home security system, he discovered that he was able to obtain the password to the home wireless network through his coffee maker. He reported the vulnerability to the manufacturer who correctly assessed it as a very low security threat, because of the short window of time in which the hacker could access this information. However, the vulnerability is still there and unpatched.

The other items Jacoby tested either had workarounds that could make them more secure or patches from the vendor that could be implemented to fix the security flaws.

As the Internet of Things moves into our homes more and more, this Kaspersky Lab research brings up some important issues around security that businesses should take into account.

For one thing, businesses should be aware that **security for IoT devices is a top concern of consumers** and that they look to vendors to be responsive to vulnerabilities. This means that all IoT manufacturers will have to build patching and updates into their business plan. Consumers and researchers will find any security flaws that are unfixed—hopefully, before the cybercriminals do.

In addition, **building in security right from the start is an important part of the development process**, saving businesses the hassle of sending out security updates to thousands of customers once the products are already in the field.

"Our experiment, reassuringly, has shown that vendors are considering cybersecurity as they develop their IoT devices. Nevertheless, any connected, app-controlled device is almost certain to have at least one security issue. Criminals might exploit several of these issues at once, which is why it is so important for vendors to fix all issues—even those that are not critical. These vulnerabilities should be fixed before the product even hits the market, as it can be much harder to fix a problem when a device has already been sold to thousands of homeowners."

– Victor Alyushin, Security Researcher at Kaspersky Lab

The Internet of Transportation

No discussion of IoT is complete without considering how it affects the transportation industry.

Both cars and the entire transportation industry—including trucking, railways and shipping—use connected things to move people and goods from place to place. It's fast. It's efficient. It also comes with big security concerns.

In Kaspersky Lab's survey of companies in the transportation sector, some alarming trends emerged. **89% of organizations in the transportation sector have had an external security incident**, and 51% have lost data as a result.[4] This means that a majority of transportation organizations are living in a high state of threat alert. With security as a consideration right from the start, transportation organizations could avoid a great deal of mitigation costs associated with a breach.

Equally as alarming is the fact that **71% of companies in the transportation sector have had an internal security incident** with 65% having lost data as a result.[5] The conclusion we can draw here is that employees of transportation companies need to be trained in security procedures. Human error is still a huge issue, even when dealing with the mass movement of people and goods. This makes it even more important that companies implement a multi-layered security system in order to account for human error and to keep transportation moving safely and effectively.

[4,5,7,8] *Do we really need to focus on transportation security?*

[6] *Hackers Remotely Kill a Jeep on the Highway—With Me in It*

Car hacking

Ever since Charlie Miller and Chris Valasek proved that it is possible to hack into a Jeep's controls while it was operating, the issue of car hacking has taken center stage.[6]

In most cars, the onboard electronics controlling various systems are connected to the same obsolete CAN-type bus that carries data without any encryption whatsoever. This means that once the external perimeter has been breached, the attacker or the virus gets full access to the system.

The path towards fixing security issues requires starting from the ground up. **With R&D work on automobiles being done 5-7 years ahead of release date, developers need to consider cybersecurity while they are still in the prototype stage.** At the very least, car makers are starting to recognize the need to keep the infotainment system separate from the functional systems that operate the car. This reduces the attack surfaces and provides fewer points of entry for a cybercriminal to access the vehicle. Not all car makers have implemented this change, however.

With 250 million cars in the U.S., there are more cars than licensed drivers, and each car has about 60 onboard computer systems operating different parts of the car.[7] All of this exposes hundreds of millions of lines of code in cars that were not built with security as a priority.

At Kaspersky Lab, we are working with major Tier 1 automotive vendors to make sure that they recognize the growing threat and prioritize cybersecurity for the software systems they are delivering before they reach the market. We are also collaborating with other researchers, policy makers and stakeholders of infrastructure so that there is a common language that administrators can use to deal with issues.

4 TRILLION

Number of miles Americans drive every day.[8]

Security in the City

One need only to look around your typical city block to see the implications of IoT.

Traffic signals are connected to an automated network. Buildings have temperature and lighting controls that are set to automatically turn on and off at certain times of the day. Transportation grids move people via computer networks in cities all over the world.

A quick read of news items about our energy sector shows that everything from nuclear power plants to dams have automated controls in place. Even entire seaports are run by a few people overseeing a complex network of computers.

Of course, as the attack surfaces grow, securing the buildings we live in, the transportation we rely on and the energy we need to stay up and running becomes an even greater concern.

Security Weaknesses in Our Infrastructure

Shodan—the search engine that collects information on roughly 500 million internet-connected items per month—easily reveals an exhaustive array of items that could be breached, including traffic lights, security cameras, and even the command and control systems for nuclear power plants. What is noteworthy is how few of these devices have security built into them.[9]

While searches on Shodan are limited to certain numbers per month, it's clear that many critical systems are connected to the web for convenience, primarily. Security concerns fall way down the list, leaving one to wonder how easily this information could fall into the wrong hands—even with search limitations in place.

30% Estimated CAGR of IoT spending by municipalities worldwide by 2019.[10]

[9] *Shodan: The Scariest Search Engine on the Internet.*
[10] *IoT Ecosystem Infographic by BI Intelligence*

Energetic Hackers

Stories of breaches into systems that control energy are becoming more and more common.

In 2013, seven Iranian hackers broke into a small dam in Westchester County, NY on behalf of their country's Revolutionary Guard Corps. While the dam is small and rather inconsequential, the hackers were able to access the sluice gate but were not able to activate it.[11] Was it a case of mistaken identity for a larger dam, or a trial run to see if they could access a critical piece of infrastructure? The FBI is still investigating, and an indictment has been brought.

In April of 2016, on the 30th anniversary or the Chernobyl nuclear power plant disaster, it was discovered during a routine security audit that hackers had broken into the Gundremmingen nuclear power plant in Germany. Officials said that the IT system was not connected to the internet and that they suspect someone brought in the malware by accident on a USB thumb drive.[12] The incident underscores the oversight that is needed towards critical infrastructure so that security is effective, routine and accounts for human error.

5.5
MILLION

In 2016, 5.5 million new things will get connected every day.[13]

[11] *A Dam, Small and Unsung, Is Caught Up in an Iranian Hacking Case*
[12] *Malware Shuts Down German Nuclear Power Plant on Chernobyl's 30th Anniversary*
[13] *Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015*

Smart Cities

A well-developed and smart public transportation is the lifeblood of any thriving city, and managing it well is is essential to keeping everyone moving safely and efficiently.

A smart public transportation system relies heavily on network communications and IT, leaving a city vulnerable to potential cyberintrusions. A hacker who gets into one of these systems could potentially create a domino effect of problems that could bring a whole city to a grinding halt.

Kaspersky Lab has been collaborating with policy makers and researchers on Securing Smart Cities, a not-for-profit global initiative that aims to solve the existing and future cybersecurity problems of smart cities. Working closely with policy makers and researchers, Kaspersky Lab has contributed to two studies of The European Union Agency for Network and Information Security (ENISA) on the cybersecurity of public transport in a smart city.[14]

Technology has enormous potential to bring cities together, keep people moving quickly and safely and eliminate inefficiencies. Working together with our partners in Securing Smart Cities, we can ensure that we are able plan ahead for potential problems, anticipate growth needs, and most important, get people going where they need to go safely and efficiently.

[14] *Securing Smart Cities Consults ENISA on cybersecurity and the Resilience of Intelligent Public Transport*

"It was a great honor for us to share our cybersecurity expertise in public transport and railways with ENISA and the working group. We believe that cooperation between regulators, hardware and software vendors, transport operators and security organizations is the only way to create a truly reliable and protected environment for modern city transport systems."

– Sergey Gordeychik, Head of Security Services, Deputy CTO at Kaspersky Lab and Securing Smart Cities contributor

Industrial Threats

Kaspersky Lab's recent research has found that **cyberattacks caused 35% of industrial network malfunction incidents**, demonstrating that security for industrial controls is becoming increasingly important.

With Kaspersky Industrial CyberSecurity (KICS), managers of industrial systems get a product that is specifically designed to protect complex industrial environments that contain a diverse range of proprietary systems.

Varied and Complex Threats

A lot of industrial systems were designed without internet connectivity in mind; yet today, many managers of these systems want to oversee their systems remotely. If there is bad weather that makes the system tough to get to, or if there is another need to check in from afar, connecting via the internet makes management much easier. Unfortunately, it also increases the attack surfaces and complicates security.

Furthermore, protecting industrial systems calls for a very different approach than what is used for securing business IT systems. With IT networks, security focuses on maintaining the confidentiality, integrity and availability of sensitive business data. The reverse is true for industrial control security where continuous availability is the primary goal, with integrity and confidentiality being of secondary importance. Add in the need to make that availability internet-connected, and the opportunities for cyberattacks increase exponentially.

Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity (KICS) is a purpose-built solution to protect ICS and SCADA servers, HMI panels, engineering workstations, PLCs and other similar devices. KICS takes into account that many threats can transfer between business IT systems and industrial systems, protecting the entire infrastructure.

In order to protect your business IT systems, we have a range of security solutions. In addition to award-winning security for endpoints and servers, our solution protects mail servers, collaboration servers, virtual environments and traffic flowing through web gateways.

Since industrial environments contain a diverse range of proprietary systems, we have designed KICS to be a highly flexible security solution that can be tailored to each installation's unique needs.

"What it shows is the main, basic issue of today's connected systems: critical infrastructure is as vulnerable as all other systems connected to the internet."

– Eugene Kaspersky

What's Around the Corner?

The Internet of Things has the potential to transform industries. Mass transit will move more efficiently. Homes will be tailor-made to suit how we wish to live. Even now, farmers track their cows in the field with IoT devices.

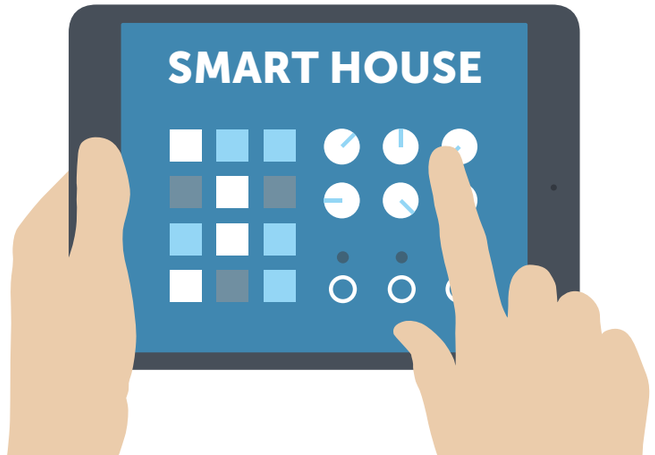
But one thing is clear. As we become increasingly dependent on the Internet of Things and what it can do for us, we need security more than ever.

A New Set of Customers

For cybercriminals, their biggest challenge has always been how to sell the data they steal without getting caught. The Internet of Things offers up a whole new market.

Whereas they usually sell data to other cybercriminals, now they have a whole new customer base—us. How much would you pay to get access back to your home? Your car? To protect your privacy? The data they steal is much more valuable to its owners than to cybercriminals on the black market, and they know it.

In addition, with the advent of bitcoin, cybercriminals have a new currency to carry out their transactions. Since bitcoin is largely untraceable, they have now eliminated another opportunity for law enforcement to track them down.



No One Is Immune

Very often, cybersecurity focuses on protecting consumers and businesses. With the IoT, everyone is affected. Cities, government agencies, corporations and individuals alike will all rely on the interconnectedness of things to keep our society running. Likewise, all will be equally vulnerable to cyberattacks.

Striking a delicate balance is the key. While we keep everything moving, we cannot do so at the expense of security. Many companies, such as Kaspersky Lab, recognize this and are moving to put security front and center, starting at the development phase.

IoT Security is a Shared Responsibility

Virtually all businesses will be touched by IoT, which means that virtually all businesses share the responsibility of security. Whether you are creating a smart device, relying on a smart production line, or need to get your employees from place to place on mass transit, vigilance about how it is all protected is warranted. Do your homework. Ask questions. And we will all be more secure.

TRY KASPERSKY LAB

Discover how Kaspersky Lab's premium security can protect your business from malware and cybercrime with a no-obligation trial. Register today to download full product versions and evaluate how successfully they protect your IT infrastructure, endpoints and confidential business data.

GET YOUR FREE TRIAL TODAY >

JOIN THE CONVERSATION

Watch us on YouTube

Like us on Facebook

Review our blog

Follow us on Twitter

Join us on LinkedIn

Learn more at usa.kaspersky.com/business-security

ABOUT KASPERSKY LAB

Kaspersky Lab is one of the world's fastest-growing cybersecurity companies and the largest that is privately-owned. The company is ranked among the world's top four vendors of security solutions for endpoint users (IDC, 2014). Since 1997, Kaspersky Lab has been an innovator in cybersecurity and provides effective digital security solutions and threat intelligence for large enterprises, SMBs and consumers. Kaspersky Lab is an international company, operating in almost 200 countries and territories across the globe, providing protection for over 400 million users worldwide. Learn more at usa.kaspersky.com.

Contact Kaspersky Lab today to learn more about Kaspersky Endpoint Security for Business and our other IT security solutions and services:
usa.kaspersky.com/business-security
(866) 563-3099
corporatesales@kaspersky.com

KASPERSKY lab
THE POWER OF PROTECTION