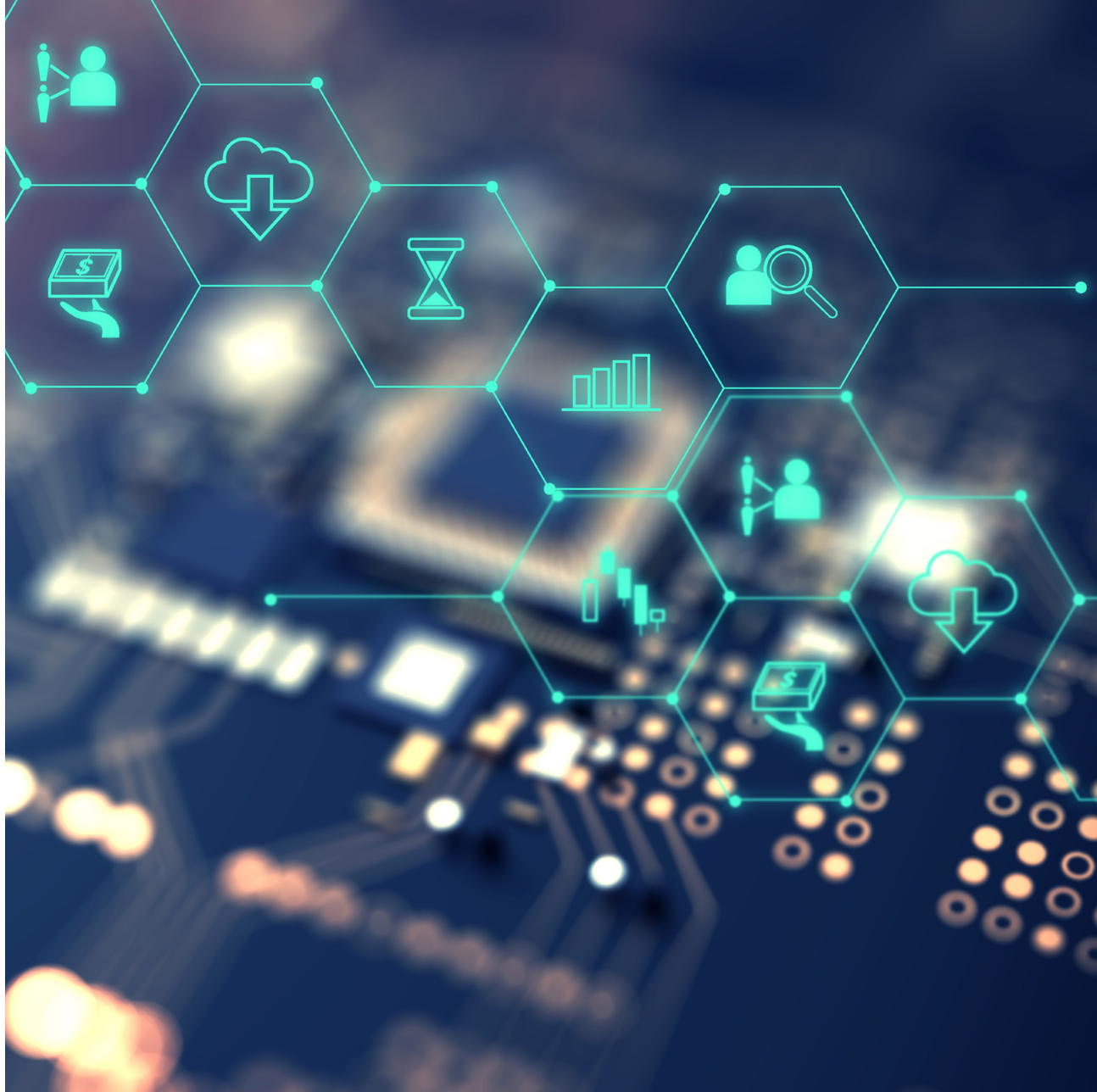
SECURITY SPOTLIGHT

Cybersecurity 101:

The Fundamentals of Today's Threat Landscape

KASPERSKY lab

The world of cybersecurity can sometimes feel like a moving target. Just when you think you've learned everything possible about a topic, something new happens that is a game changer. Protecting your company means staying on top of the latest trends in cybercrime and knowing the answers to the most important topics. By reviewing major topics in cybersecurity in this eBook, you can ensure that you are doing everything possible to protect your business.



Ransomware

When ransomware hits, it usually walks through a number of typical steps.

1. Installs when the user opens a file, usually via email, IM, social network or by visiting a malicious site.
2. Generates a pop-up window, web page or email warning from what looks like an official authority.
3. Encrypts the user's files with an AES-256, a randomly generated one-time key.
4. Creates an individual encryption key for each file.

Ransomware is, quite simply, a digital form of extortion. Cybercriminals hijack computers at a company and tell the victims that they can get their data back if they pay a ransom by a certain deadline. It's an insidious technique for extorting money from companies, forcing businesses to act quickly and irrationally out of fear and panic.

The stakes are very high. For companies who don't catch the infection within a day, 67% report significant amounts of encryption occurring—versus 43% that catch the infection within a few hours. Recovery of data is also less successful if companies do not catch the infection within hours. 41% report losing a significant number of files entirely if it takes a day or more to detect.[1]

The costs of an attack can be steep for any organization. In the case of cryptomalware, a common type of ransomware that encrypts your files, a single attack can cost a small- or medium-sized business $99,000. Crypto-malware is becoming increasingly popular with cybercriminals. Among companies that are victims of ransomware, the proportion who encounter cryptors specifically rose dramatically—up 25% from 2014/15 to 2015/16.[2]

Ransomware is becoming an increasingly damaging epidemic. Comprising almost 40% of all spam messages, ransomware spiked 6000% in 2016 compared with 2016.[3] Approximately one in three companies end up paying the ransom, but even then, almost one in five do not get their data back.[4] It should come as no surprise to anyone that the offer of cybercriminals to provide a decryption key may, in fact, be a lie.

Since paying the cybercriminals only perpetuates the problem, we do not recommend paying the ransom. Instead, we recommend taking several preventative measures to ensure that you are never in that position.

1. Back up your files regularly.
2. Check your backups.
3. Educate your employees on what to look for—phishing scams, suspicious attachments, social engineering.
4. Apply patches and updates.
5. Install a robust, multi-layered anti-virus solution.

Ransomware is an insidious problem that affects companies of all sizes and industries. But with some knowledge and a proactive approach, your company can protect itself and avoid the headaches and the downtime that come with a ransomware infection.

[1, 4] *Corporate IT Security Risks Survey 2016* from Kaspersky Lab and B2B International

[2] Kaspersky Lab's *KSN Report: Ransomware in 2014-2016*

[3] *IBM Security Services, "Ransomware: How Consumers and Businesses Value Their Data"*

IoT

Number of connected things predicted by Gartner to be in the marketplace by the year 2020[5]

You're locked out of your home. Your car won't start. The heat in your house won't turn on in the middle of winter. How much would you pay to get these important parts of your life back up and running? That's the question cybercriminals want you to ask when they take control of your home or your car.

All of these scenarios are possible with the vulnerabilities that are present within the Internet of Things (IoT). With 20.4 billion connected things predicted by Gartner to be in the marketplace by the year 2020[6], the opportunities that cybercriminals have to hold our lives hostage and extort payment from us is only growing.

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

As this ecosystem grows, so do the number of attack surfaces. Since many of these devices are not secured, the opportunities for infiltration are even greater—and growing.

The world at large

Beyond our homes and offices, the world is increasingly connected by the IoT. Traffic signals are connected to an automated network. Buildings have temperature and lighting controls. Trains and airports all operate through a vast network of devices that keep things running seamlessly.

When it comes to critical infrastructure, the need is even greater. Unlike business IT networks where security focuses mainly on maintaining the confidentiality, integrity and availability of sensitive data, the reverse is true of industrial security where continuous availability is the primary goal. Add in the desire to make that availability internet-connected, and the opportunities for cyberattacks increase exponentially.

The botnet

The IoT has another nefarious capacity—the ability to act as a botnet. Acting as a network of private computers infected with malicious software and controlled as a group without the owners' knowledge, your TVs, DVRs and IP-enabled cameras can be used to spread spam without you even being aware of it.

This is what happened in October 2016 when the Mirai botnet brought down more than 80 large web sites. The cause was a DDoS attack against the company that provided DNS services to the affected sites. By scanning the internet for IoT devices, connecting them using default logins and passwords, and then securing admin rights, the devices carried out the commands of the hacker.

With users rarely changing the passwords of their devices, it is actually quite simple to recruit several hundred thousands of zombies to create a botnet. Cybercriminals see this potential and will, most definitely, exploit this weakness again.

IoT security is a shared responsibility. Whether your business is producing a smart device, using on a smart production line or relying on transportation to get your employees from place to place, security of the IoT is something that concerns all of us. We all have a part in ensuring that the Internet of Things does not become the Internet of Threats.

We recommend three key steps in order to protect your business in a connected world:

1. Change the logins and passwords on any connected devices that your business uses.
2. Install the latest patches from the manufacturer.
3. Put a reminder on your calendar to do the above two things every three months.

[5, 6] *Gartner Says 8.4 Billion Connected "Things" WWill Be in Use in 2017, Up 31 Percent from 2016*

Cloud

48%

48% of all IT services are delivered via cloud service providers.[7]

Cloud computing is all about access. The ability to keep employees connected no matter where they are is invaluable, especially for small- and medium-sized businesses.

But that access comes at a price. When a single data breach can cost an SMB $86,500[8], businesses need to be prepared with security that protects sensitive data, while keeping business running.

Cybercriminals know that large enterprises invest heavily in cybersecurity, so they have shifted their focus—attacking more SMBs who may not have invested as heavily in security and, therefore, may be breached more easily. With many SMBs acting as clients or vendors to larger enterprises, this gives cybercriminals yet another way to access the sensitive data they're looking for.

Because of this, it is no longer sufficient to protect your own perimeter and your own data. You have to find out if your cloud provider is secure. Ask questions. Make sure you know what protections they have put in place to keep your sensitive information safe. With 47% of businesses concerned with the security of cloud infrastructure adoption and business process outsourcing[9], any cloud provider should be able to answer your questions.

[7, 8, 9] *Corporate IT Security Risks Survey 2016* from Kaspersky Lab and B2B International

On-premise or Cloud?

When deciding whether or not to go with a cloud solution, there are a few things you should keep in mind.

On-premise storage solutions are best if you need advanced protection capabilities, such as encryption, or targeted solutions for virtual environments. You will also need a dedicated staff to run any on-premise solution.

Cloud is best if you prefer to outsource security management or if you are an MSP and want to offer services for multiple customers. It is also good for companies that don't want to install or maintain an additional server in their office.

When it comes to critical infrastructure, the need is even greater. Unlike business IT networks where security focuses mainly on maintaining the confidentiality, integrity and availability of sensitive data, the reverse is true of industrial security where continuous availability is the primary goal. Add in the desire to make that availability internet-connected, and the opportunities for cyberattacks increase exponentially.

Other points to consider:

- Your cloud solution should not be too complex.
- It should scale with your operation. If you have multiple offices, cloud is a great way to connect them, and your solution should span all offices easily.
- Look for a simplified management console.
- Cloud setup should be straightforward and not require excessive IT knowledge. Any small business should be able to do it.
- It should work with existing policies.
- If you decide to install a cloud security solution, be sure to implement clear guidelines about passwords. Consider two-factor authentication. Apply patches and updates, just as you would on any on-premise solution.

As mobile devices increase, as your employees travel, as you open new office locations, are you prepared to protect each new attack surface? With a multi-layered cloud security solution, you can gain all the access you need from the cloud, while ensuring business continuity and employee access.

APT

68% **Targeted attacks that have resulted in data loss or exposure[10]**

Advanced Persistent Threats (APTs) are complex attacks, consisting of many different components. They are designed with one objective in mind: gaining undetected access to sensitive information.

APTs are "advanced" because the tools used in these attacks are more sophisticated than those usually used by cybercriminals. They are "persistent" because once an organization is breached, the threat can remain in the system for months or even years. In fact, according to a study by HP and Mandiant, the median amount of time before a company detects a data breach is 205 days, leaving cybercriminals with months of access to sensitive data before they are discovered.

APTs make up just 1% of the threat landscape. While they are rare and highly complex, they do cause an awful lot of damage. For this reason, it is important to research and name them, which makes up a bulk of the work that the threat intelligence community does.

At Kaspersky Lab, we conduct in-depth analysis of every APT we study to learn how the threat landscape is changing, what methods are being used, and how companies can protect themselves. We then share this information with the wider threat intelligence community, which helps keep all of us safer from these pernicious threats.

How does an APT work?

With an APT, cybercriminals target individuals through spear phishing messages or exploits, infiltrating an organization by individualized social engineering techniques.

Usually, an APT targets a handful of key individuals with known access to the targeted information, reeling them in with convincing emails that appear to come from a trusted source, such as HR. With one careless click, a cybercriminal then has access to a business, usually without anyone knowing they're there. Once they are in, they can use Trojans, worms and other malware to infect a whole network, ensuring that they can remain in your system indefinitely.

Examples of some of the most pernicious APTs that Kaspersky Lab has researched include Carbarnak, Duqu and Turla. You can read more about our APT research in our eBook, *Whodunit: The Mystery of the APT.*

How can you protect your company?

Start with the understanding that everyone is a target for APTs. You may be a small company, but if you are a vendor to a larger organization, cybercriminals will view you as a highly desirable target. It doesn't matter to them how big your organization is, only that you are a portal to highly valuable information.

By implementing a multi-layered security system that includes employee awareness, strong security policies and a robust security solution, you can protect against the threats that cause the most damage to your business.

[10] *Corporate IT Security Risks Survey 2016* from Kaspersky Lab and B2B International

Employee Threats

1 in 5

Careless of uninformed employees were involved in almost 1 in 5 serious data breaches.[11]

Your Employees Are Your First Line of Defense

Most organizations view their employees as their most valuable asset, and rightly so. They are the engine of your company that keeps revenue growing and keeps your business moving forward.

But even the most dedicated and well-meaning employees can threaten your company's security, usually without realizing it. According to leading industry and government reports, over 90% of all cyberattacks are successfully executed with information stolen from employees who unwittingly give away valuable information to hackers.[12]

Cybercriminals view your employees as the path of least resistance. For businesses in North America, two of the top causes of the most serious data breach were careless/uninformed employee actions (59 percent) and phishing/social engineering (56 percent).[13] Cybercriminals know who to target and how to exploit these weaknesses.

By putting into place a multi-layered system of defense that includes employee education, your company can ensure that your people understand the important responsibility they have in keeping your company and its data secure.

Every Size Company Is a Target

Many small businesses act as vendors to larger companies, making them a prime target for cybercriminals. If there is a hole in their security, they can use a smaller company as a portal through which they can get at the highly valuable data of large enterprises. Because enterprises continue to build up their perimeter, small- and medium-sized businesses are even more susceptible to attack as cybercriminals scan the whole marketplace for vulnerabilities.

With the average cost of a serious data loss event for an SMB at $86,500, most small businesses are not prepared for a sudden large hit to their budget. In order to prevent this unwelcome scenario, all employees must be educated about cybersecurity, starting at the very top where executives can help create a culture of awareness. By setting aside time and resources for employee education on cybersecurity, they can help build a culture where security is top of mind for all employees.

[11] *Employee Errors Cause Most Data Breach Incidents in Cyber Attacks*

[12] *Employees Are One of the Biggest Cyberthreats to Businesses in North America*

Common Attack Methods

Cybercriminals are quite creative in their methods. Social engineering tricks employees into breaking normal security procedures. Phishing is a targeted attack delivered via email to employees. Waterholing infects the sites that employees visit most often. All cybercriminals need is for any one of these kinds of attacks to be successful for them to infiltrate a company's network.

Tips for Enhancing Cybersecurity

The best place to start is by keeping your IT staff on top of current trends and risks and then implementing certain key policies, many of which can be automated, such as:

- Ensure that all users know and observe company security policies
- Inform users about possible consequences of key Internet threats, such as phishing, social engineering or malware sites
- Instruct all users to notify IT security staff about all incidents
- Maintain control over user access rights and privileges; any rights and privileges should be granted only when necessary
- Record all rights and privileges granted to the users
- Scan the systems for vulnerabilities and unused network services
- Detect and analyze vulnerable network services and applications
- Update vulnerable components and applications. If there is no update, vulnerable software should be restricted or banned

True Cybersecurity

Kaspersky Lab's True Cybersecurity approach combines multi-layered security with cloud-assisted threat intelligence and machine learning to protect against the threats your business faces. True Cybersecurity not only prevents attacks, but also predicts, detects and responds to them quickly, while also ensuring business continuity for your organization.

Watch us on YouTube

Like us on Facebook

Review our blog

Follow us on Twitter

Join us on LinkedIn

Get your free trial now >

Learn more at
kaspersky.com/business

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.

To learn more about Kaspersky Endpoint Security for Business, call Kaspersky Lab today at 866-563-3099 or email us at corporatesales@kaspersky.com.

www.kaspersky.com/business

KASPERSKY lab