Espionage, blackouts, stoppages affecting the authorities and production sites, manipulation of logistics processes and theft of millions of sensitive data records – scenarios that have already become a reality several times across the world in recent years and point to a very clear development: the threat of cyber attacks on governments and companies worldwide will continue to increase in the future.

The attackers not only focus on private individuals, but also on organizations, state and public institutions and private companies in a wide range of industries.

The financial losses that the victims have to report are often in the billions. In addition, the intrusion of unknown third parties into a state or economic system entails further risks, some of them severe, for the country and its people.

Security analysts from Hornetsecurity Security Lab have examined which industries have been most affected by cyber attacks in the past year and the exact types of attacks they have been exposed to, explaining why some companies are more frequently targeted by cybercriminals and the possible motives for this. Following a breakdown of the affected sectors, the following analysis focuses on the energy industry - because it is one of the most popular targets for hackers.
As part of a country’s critical infrastructure, it is considered particularly important to protect the energy industry and it is therefore also subject to strict legal requirements: when the IT Security Act came into force in 2015, the German government required operators of critical infrastructures to comply with certain minimum security standards for their IT infrastructure and to implement measures for their IT security in accordance with the “state of the art”. Compliance with these requirements must be demonstrated at least every two years in the form of security audits, checks or certification. In addition, significant IT security incidents must be reported to the Federal Office for Information Security (BSI). A failure or impairment of supply services would have enormous consequences for the economy, state and society, a fact of which cybercriminals are also aware.

In the case of cyber attacks on the critical infrastructure of a country, such as the energy industry, the success rate is not particularly high due to the high security standards — but that is often not what cybercriminals are after, according to the security experts at Hornetsecurity. Rather, the relevance of its objective to a country or a specific group is the basis for the decision.

“It is not unusual for larger, professionally organized teams of hackers to be behind such attacks: on behalf of governments or secret services, for example, they want to gain access to secret information or exert pressure on the state concerned in the event of possible conflicts. In many cases, this can be achieved by shutting down individual areas of a company, for example by encrypting important files”, says an IT security expert from Hornetsecurity Security Lab. “Attacks by smaller cybercriminal gangs are also conceivable, however. Basically, it stands to reason: the more critical the infrastructure under attack, the higher the probability that the victims of a ransomware attack, for example, will pay for a decryption key, in the hope that operations can continue as swiftly as possible.”

One of the most famous cyber attacks on a critical infrastructure occurred in December 2015 in Ukraine: about a quarter of a million inhabitants of the Ivano-Frankivsk region were without power for several hours, because hackers had infiltrated the system of the energy supplier “Prykarpat-tyaoblenergo” and caused a power failure by remote access. To date, it has not been possible to identify those responsible.

HOSPITALS AND AUTHORITIES ARE BECOMING TARGETS

In the past year, cyber criminals mainly targeted hospitals (July 13, 2019, attack on German Red Cross facilities in Rhineland-Palatinate) and state institutions and authorities (June 2019, ransomware attack on Florida City Council).

On January 5, 2020 the Austrian Foreign Ministry announced that it had been the victim of a “serious” cyber attack. The ministry suspects a “state actor” behind this attack and points out that “in the past, several European countries have been the target of similar attacks” In early 2018, for example, it became public that the German government’s federal network had been the target of a hacker attack and that, according to media reports, a group of hackers commissioned by the Russian government had carried out the attack.
The BSI forecasts an increase in cyber attacks on critical infrastructures in the future. The ongoing digitization of systems, processes and the infrastructure of utilities is making them increasingly dependent on a smoothly functioning IT system — but it also creates a lot of gateways for hackers. Accordingly, the Federal Office classifies the threat posed by cyber attacks to critical infrastructures as particularly high.

The BSI formulates the challenge that arises in this connection as follows in its “Status Report on IT Security in Germany 2019”: “Cyber security is asymmetrical: in order to be able to compromise critical infrastructure seriously, an attacker only needs to exploit a single vulnerability successfully. Operators of critical infrastructures, on the other hand, must ensure holistic protection in order to provide comprehensive security”

In addition to threat vectors such as hacked web applications, unpatched and outdated systems and unsecured servers, companies should pay special attention to email as a gateway for cyber attacks.

“Email has become the preferred service for business communication worldwide. It is thus not only the biggest way in for cyber attacks, but also brings together the two factors of technology and people that companies must take into account in delivering comprehensive IT security”, according to a security expert from Hornetsecurity.

According to analysis by Hornetsecurity Security Lab, last year hackers mainly attempted to penetrate the systems of companies in the energy sector by means of harmful links placed in email messages.

Malicious attachments and phishing emails are also among the preferred types of attack for cyber criminals.

One thing is clear: human beings are IT hackers’ favorite vulnerability. With little technical effort and social engineering tactics, cybercriminals entice employees to click on infected links that download malicious software or intercept login information that opens the door to hackers for further attacks.

Particularly in view of the high statutory IT security standards to which critical infrastructures are subject, human beings are often the one security loophole that can destroy supposedly comprehensive protection with one click.

**FIG. 1:** Types of attacks on the energy sector

- **21.51%** Phishing
- **31.47%** Malicious attachments
- **46.86%** Malicious links
- **0.16%** Targeted attacks
ANALYSIS A TARGETED PHISHING CAMPAIGN

The Hornet Security Lab was recently able to observe and analyze a phishing campaign which was designed to intercept email access data of its recipients. The attack focused primarily on companies in the electricity and gas supply industries.

The e-mail address joe.examplemail@companyname.tld is given as an example and was replaced by the email address of the recipient. This indicates a targeted phishing attack.

The content of the email is relatively authentic. Following a personal salutation, the recipient is informed that incoming messages could not be delivered. In order to receive the emails, the user should simply click on the button below. Otherwise the emails would be deleted six hours after receipt of the message.

The link leads to a web page on which a password form is displayed. The email field is already pre-filled with the parameters provided by the link in the email. The domain name (in this case, the company name) is printed in capital letters above the form, to inspire confidence in the user.

The timer displayed is probably intended to pressure the victim by setting a fictitious time limit – a classic social engineering technique.

As soon as the user has entered their login data, the information gets directly into the hands of the fraudsters, who now use it for further attacks or sell it on the dark web.
THE HACKER BUSINESS

In general, companies in all industries are facing more and more professionally designed cyber attacks from organized hacker groups. Although there are occasionally individual perpetrators, the motives behind such attacks strongly suggest planned, structured and experienced groups. Some of these cybercriminal gangs can now even be identified by means of certain tactics and the techniques they use, and some have specialized in certain industries or markets as targets for attacks.

FIG. 2: Hacker groups with a focus on specific industries

<table>
<thead>
<tr>
<th>Industry</th>
<th>Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>Energy</td>
<td>APT19, Dragonfly, Magic Hound</td>
</tr>
<tr>
<td>Logistics</td>
<td>Leviathan, Tropic Trooper</td>
</tr>
<tr>
<td>Automotive</td>
<td>OceanLotus</td>
</tr>
<tr>
<td>Software</td>
<td>Deep Panda, MuddyWater, OilRig</td>
</tr>
<tr>
<td>Factories</td>
<td>APT18, menuPass, SilverTerrier</td>
</tr>
<tr>
<td>Financial</td>
<td>admin@338, APT38, Cobalt Group</td>
</tr>
<tr>
<td>Pharmaceutical</td>
<td>FIN4, Orangeworm, Turla</td>
</tr>
<tr>
<td>Government</td>
<td>Ke3chang, Leafminer, Machete</td>
</tr>
<tr>
<td>Travel</td>
<td>APT39, FIN</td>
</tr>
<tr>
<td>Education</td>
<td>DarkHydrus, menuPass, SilverTerrier</td>
</tr>
</tbody>
</table>

INFAMOUS AND FEARED: APT19

The “APT19” hacker group from China, also known as the “Codoso Team”, targets a wide range of industries, but its attacks are mainly directed at companies in the energy sector. In its large-scale phishing campaigns, the group uses the “Cobalt Strike” software, among other things, from which it sends out the so-called “Beacon Implant” in infected RTF attachments and harmful Microsoft Excel files with macros (XLSM document).

“Cobalt Strike” was developed in 2010 by Raphael Mudge as a commercial penetration testing tool with the intention of simulating enemy software to execute targeted attacks and mimic the actions of advanced persistent threats. However, the tool is now also used by numerous cybercriminal groups, such as APT19. The “Beacon Implant” functions as a software component and is installed on the victim’s system. Ultimately, the malware enables attackers to carry out a number of different functions, including command execution, key logging, file transfer, authorization extension, use of Mimikatz, and port scanning.

“Depending on the industry, company and motive targeted by the cyber criminals, their tactics and techniques also vary. So a hacker group that primarily uses espionage to gain access to secret and confidential information would have different tactics to a group that is primarily intent on manipulation.

Building on this, the groups use various techniques. “Brute force attacks, harmful attachments in phishing emails and so-called deep fake videos, which are currently becoming increasingly popular”, explains a security analyst from Hornetsecurity.
"In addition, hackers do not launch a single attack on a target. By using different attack vectors and methods, they also target different vulnerabilities, thereby increasing their chances of success. Publicly available information, such as legal security requirements for specific companies in a particular industry, email addresses, names and phone numbers of management or key contacts in a company, enables cybercriminal groups to plan their operations very precisely and adapt them to their specific target."

Some attacks on a single company are are committed at different times, because the groups use certain tactics, such as phishing emails, as a preparation for further attacks. Through phishing campaigns, cybercriminals are trying to obtain additional internal information (who has what position and is responsible for what) or access data, as in our example above.

The “malicious link” placed in emails is becoming increasingly popular globally: “This is probably because many anti-spam solutions already detect viruses in the attachment and hackers are now looking for other ways to send their malware to their victims. The links lead to infected or fake websites which download malware when opened, or access data is intercepted and forwarded directly to the hackers”, says a security specialist from Hornetsecurity.

The security analysts of Hornetsecurity Security Lab see a clear trend towards "Targeted Frauds", also known as Business Email Compromise (BEC). Along with ransomware and banking Trojans, BEC incidents are responsible for many of the financial losses caused by cybercrime worldwide. According to the latest Internet Crime Report of the FBI, BEC attacks in 2019 led to global losses of around 1.7 billion dollars.

THE TOP TEN INDUSTRIES TARGETED

The list of the top 10 industries worldwide that have been targeted by cyber attacks in 2019 also includes companies in the logistics (14%) and automotive sectors (13%), the software market (9%), followed by factories (9%), the financial sector (8%), pharmaceuticals and government institutions (7% each), travel companies (6%), the education sector (6%) and insurance (5%).

FIG. 3: Top 10 industries targeted in 2019

<table>
<thead>
<tr>
<th>Industry</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Energy</td>
<td>16%</td>
</tr>
<tr>
<td>Logistics</td>
<td>14%</td>
</tr>
<tr>
<td>Automotive</td>
<td>13%</td>
</tr>
<tr>
<td>Software</td>
<td>9%</td>
</tr>
<tr>
<td>Factories</td>
<td>9%</td>
</tr>
<tr>
<td>Financial</td>
<td>8%</td>
</tr>
<tr>
<td>Pharmaceutical</td>
<td>7%</td>
</tr>
<tr>
<td>Government</td>
<td>7%</td>
</tr>
<tr>
<td>Travel</td>
<td>6%</td>
</tr>
<tr>
<td>Educational</td>
<td>6%</td>
</tr>
<tr>
<td>Insurance</td>
<td>5%</td>
</tr>
</tbody>
</table>
A MODERN, DIGITAL WORLD: OPPORTUNITIES AND CHALLENGES

Changes in business processes, new customer requirements and digital services require a rethink within companies – many companies benefit from the advantages of technological progress, new companies emerge from this development, long-established companies in turn have to rethink their business models due to the changing needs of their consumers and in order to remain competitive on the market, they are increasingly investing in their digitization strategy. In general, the issue divides market participants into different camps: on the one hand, new technologies and processes drive the national economy, while on the other hand, changes also give rise to new and now increasingly obvious risks. Cybercrime is having an increasing impact on national economic and political processes.

IT security in companies has acquired a completely new significance and will occupy an even more important position in the future. Even if some industries are much more clearly the focus of hacker attacks, companies in all industries should prepare themselves against growing cybercrime in view of the increasing scope of attacks, their complexity and the resulting losses.

DIGITIZATION AND SOCIAL MEDIA: DRIVERS FOR CYBERCRIME

Law enforcement agencies and IT specialists worldwide agree: cyber crime is the world’s fastest growing area of crime. According to a forecast by the international market research company Cybersecurity Ventures, the worldwide damage caused by cyber crime will add up to around 6 trillion dollars annually by 2021. The losses include damage caused by manipulation or theft of internal company, personal and financial data, disruption of business operations, damage to systems, recovery of hacked data and systems, and damage to image.

Security experts see digitization and new technologies as the main drivers of this development: cloud computing, big data, robotics and artificial intelligence offer companies across sectors and industries advantages such as optimization of processes, saving of resources and rapid exchange of data and information. More and more companies use the cloud to store and share sensitive internal data.

However, in addition to networking of all devices, machines and systems and a permanent connection to the internet, outdated servers, unpatched systems and a lack of employee expertise lead to unexpected security loopholes. First and foremost, cybercriminals recognize the weak points early on in order to use them for their own intentions.

In addition, the expansion of the digital infrastructure offers numerous opportunities for criminals to expand or move their attacks online. On the dark web, for example, hackers offer cybercrime-as-a-service, and by means of social engineering and phishing, criminals can access online accounts, email inboxes or internal data even without programming knowledge.

Free web services and cost-effective use of computing capacity also simplify the creation of a wide range of malware and tools – in the digital age it seems to be easy for criminals to cover their basic crimeware needs. Social and business networks such as Facebook, Twitter and LinkedIn and company websites play into the hands of cybercriminal activity.

Publicly viewable names, email addresses, information about current events at a company, freely accessible logos and private information about employees through their social media profiles can be used by hackers to make their attacks as authentic as possible.
Hornetsecurity is the leading German cloud security provider for email in Europe, protecting IT infrastructure, digital communication and data of companies and organizations of all sizes. The IT security specialist from Hanover provides its services via nine redundantly secured data centers worldwide. Its product portfolio includes email, web and file security solutions. All of the company’s services can be implemented quickly and are available around the clock. Hornetsecurity has a global presence at eleven locations with around 200 employees. Customers include Swisscom, Telefónica, KONICA MINOLTA, LVM Versicherung, DEKRA and Claas.
Sources


(3) https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/ (accessed on 01/16/2020)

(4) Analyses and evaluations of the Hornetsecurity Security Lab