HORNETSECURITY

# CYBERTHREAT REPORT
## 1ST EDITION 2020

Now that information technology systems are no longer used in isolation, but are connected globally via the Internet and mobile communications, the threat of cyberattacks is also increasing. Illegal activities on the Internet range from attempted fraud, phishing and DDos attacks to the sale of black market goods, such as drugs and weapons. According to the Federal Criminal Police Office, hardly any other area of crime is showing such a continuous increase in criminal activity.[1]

Cyberspace is undergoing rapid change – as the methods hackers and fraudsters are using. The 1st Edition of the Hornetsecurity Cyberthreat Report in 2020 examines why cybercrime is one of today's global threats, what role artificial intelligence is likely to play in future cyberattacks and warding them off, and why hackers are increasingly targeting Microsoft Office 365.

## **Cybercrime:** A global risk

The Global Risk Report 2019 shows that, for the third year in a row, cyberattacks figure among the most serious global threats, alongside weather extremes, the failure of climate protection and natural disasters. Large-scale cyberattacks and the resulting **breakdown of critical infrastructures due to a cyberattack are even classified as the second most common threat.** There is growing concern about cyberattacks on public utilities (critical infrastructures), as the consequences of a prolonged outage are enormous and almost equivalent to the effects of weather extremes.[2]

Cybersecurity is becoming increasingly important when it comes to corporate security. A full 92 percent of respondents in a cybersecurity study conducted by TÜV see cyberattacks as a serious threat.[3]

**Global Threat Report:** 1st to 3rd place on the list of global threats in 2019

1 Weather extremes & failure of climate protection

2 **Large-scale cyberattacks and the subsequent breakdown of critical infrastructures**

3 Mass unemployment and other negative consequences of technological progress

The integration of technology into almost every component of human life not only opens up new possibilities, but also offers countless, not yet clearly definable gateways for criminal activities. New technologies are being introduced – faster than it takes to check and guarantee them for security.

## **Spam:** Malicious attachments and espionage

There are different types of spam, including traditional spam, which prompts the recipient to make an advance payment for a service or product, for example. Another type is malware spam. Cybercriminals attempt to infect the recipient's systems by including malware in the attachment or a link in the email. The third type is phishing – in this case the user isasked to enter access data for online banking or social media accounts, for example.[4]

The experts from the Hornetsecurity Security Lab analyzed the spam emails from October 2018 to October 2019 and discovered that **91.7 percent was classic spam**. The remaining **8.3 percent were malicious spam emails (malicious attachments, URLs, or phishing).**

**Fig. 1:** Top 5 malicious attachments

1 **Word** (.doc, .docx)

2 **Excel** (.xls, .xlsx)

3 **Zip archive** (with executable files)

4 **Disc image files** (.img)

5 **RTF documents**

**Fig. 2:** Proportion of spam emails received

**91.7%**
**Classic spam**

**8.3%**
**Malicious spam emails**


**Fig. 3:**
Distribution of threat types in malicious spam emails

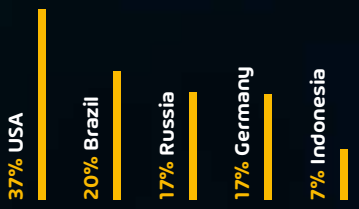



**Fig. 4:**
Origin of spam emails


**Fig. 5:**
Proportion of malware in malicious emails

**More than half of malicious spam emails contain spyware, Trojans and keyloggers.** Hackers are increasingly using them to carry out espionage and collect information for another cyberattack.[5] Although the total number of spam emails has decreased, the risk posed by spam should not be underestimated. The effort of the cybercriminals and the exploitation of personal data resulting from data leaks significantly increase the risk of infection.[6]

## **Social engineering:** Human weakness as a basis for cyberattacks

Although social engineering has long been the basis for all kinds of fraudulent practices, this perfidious form of manipulation opens doors for cybercriminals especially in the era of digitalization. Companies are **almost three times more likely to fall victim to cybercriminals as a result of social engineering attacks** than due to actual weaknesses in their IT security architecture.[7]

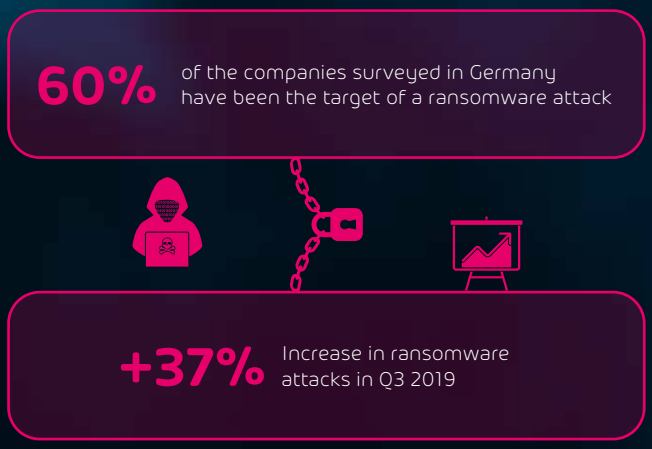
Cybercriminals not only use fake sender email addresses as well as fake ads and websites, they also put sensitive information in their messages. In 2019, for example, the uncertainty surrounding the basic data protection regulation was used as a cover for several fake emails.

## **Ransomware:** Damages totaling several millions

Ryuk, GandCrab and Locky are back – and are more dangerous than ever. In October 2019, even the Federal Bureau of Investigation (FBI) send out warnings about ransomware attacks that threaten companies and organizations in the USA. A warning of this kind was last issued in 2016, a few months before the wave of attacks with WannaCry and NotPetya.[8] Ransomware is clearly one of the biggest threats in the cyber world, as attacks repeatedly result in **complete failure of entire computer networks and production facilities.**[9] According to a study conducted by KPMG, **60 percent of respondents have been the target of ransomware attacks in the past two years.** In one of five companies, as much as 75 percent of the IT landscape was compromised following a successful ransomware attack.[10]

In the third quarter of 2019, the insurance company Beazley reported an **increase of around 37 percent** in ransomware attacks compared to the previous three months.[11]

Cybercriminals continue to see ransomware as a lucrative business opportunity. Ryuk illustrates this as well: According to the BSI (German Federal Office for Information Security), close observation of the Bitcoin addresses used allows conclusions suggesting a ransom amount of **USD 600,000.** Ransomware is an established and constantly evolving business model for hackers today: GandCrab, for example, has a version number and is also offered as ransomware-as-a-service on the Internet.[12]




## **Emotet:** The most dangerous malware in the world?

When the word ransomware comes up, Emotet is often also mentioned in the same breath. Emotet caused considerable damage last year, not only to the German economy but also to public authorities and organizations. In September 2019, BSI reported **several thousand compromised email accounts** to the responsible providers.[13]

But what makes Emotet so dangerous? The malware has proven to be extremely mutable since it first appeared in 2014. The first version of Emotet was propagated through links or attachments in spam campaigns using fake messages from banks. Emotet later also circulated via PDFs disguised as invoices and as fake shipping confirmations from Amazon.[14, 15] What is termed **"Outlook Harvesting", the content-related analysis of the email communication** on an infected device, plays a particularly decisive role in the detection of Emotet. The malware not only reads contact relationships from the history, but also the contents of the emails, helping cybercriminals perfect their social engineering techniques and send even more precisely targeted emails.[16]

Emotet now behaves like a dropper, downloading further malware following successful infection: currently, the banking Trojan Trickbot for example, which is capable of spread independently in networks by reading access data, among other things. This is often followed by the ransomware Ryuk, which can encrypt entire systems.[17]

**Fig. 6:** Extensions and dangers of Emotet

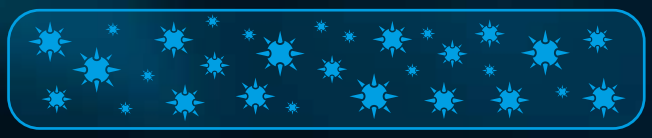
- Outlook Harvesting
- Data theft from web browsers
- Reloading of malware and ransomware
- Exploitation of unpatched vulnerabilities
- Propagation in local networks

The BSI **already called Emotet the most dangerous malware in the world back in 2018.** This reputation also clearly remained the same in 2019.

## **Destructive malware:** The destructive fury of hackers

Cybercriminals are increasingly resorting to malware attacks with destructive elements. According to a study conducted by IBM, the **number of attacks of this kind worldwide doubled in the second half of 2019.**[18] Since August 2019, for example, the **ransomware GermanWiper** not only encrypts the data on the affected computers during activation, but overwrites it with zeros. Although the developers of GermanWiper demand ransom from the victims as part of their attacks, there is no way to recover the encrypted data. The **ransomware RobinHood** also contains destructive elements and has already caused great damage in Baltimore (USA) by not only encrypting the files on the users' computers, but also obstructing backup and service functions.[19]

**2019:** Attacks in the first half of the year



**2019:** Attacks in the second half of the year **(+116%)**

Destructive attacks cost multinational companies an average of around **$239 million** whereas data leaks cost $3.92 million on average. According to IBM, companies need around **512 hours** to recover from a malicious malware attack, and a single attack can damage an average of **12,000 devices per company**.[20]

**Fig. 7:** Average damages malware can cause with destructive elements

| 512 hours | $239 million | 12,000 devices |
|---|---|---|
| ...is the time companies need to recover from an attack using destructive malware. | ...is the cost of an attack using destructive malware. | ...are damaged per company in a single attack. |

The increasing number of cyberattacks with destructive malware is worrying. Cybercriminals can cause immense damage with this type of attack and even if companies do not pay the ransom for encrypted information there are often long-term operational disruptions and considerable monetary losses.

## **Phishing:** Still a threat

The experts from the Hornetsecurity Security Lab identified an average of around **12.3 percent of all incoming emails as phishing attacks**. Despite declining in the summer, the number of phishing emails rose once again towards the end of the year, as hackers expect higher success rates during the Christmas season and due to the associated increase in the use of online shops such as Amazon.[21]

In **2018, 51 per cent of UK organizations took action to increase cybersecurity, compared to 57 per cent in 2019.**[22] Despite increasing awareness of the dangers posed by phishing emails, the risk to users remains high.

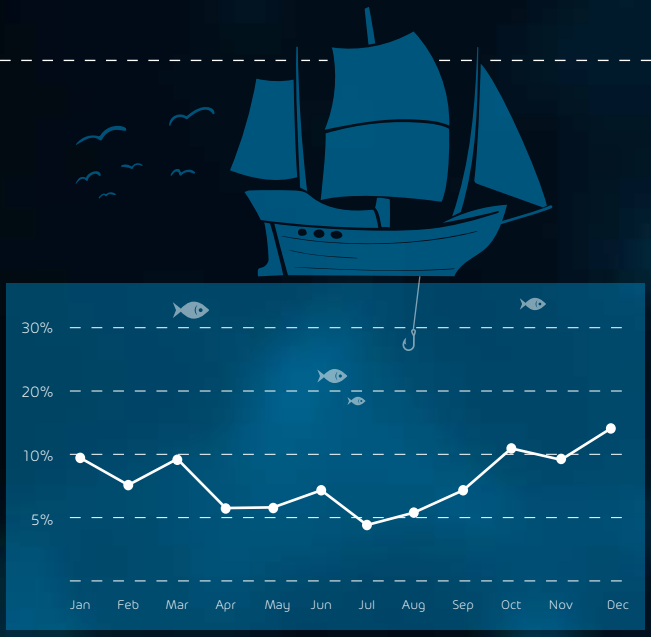


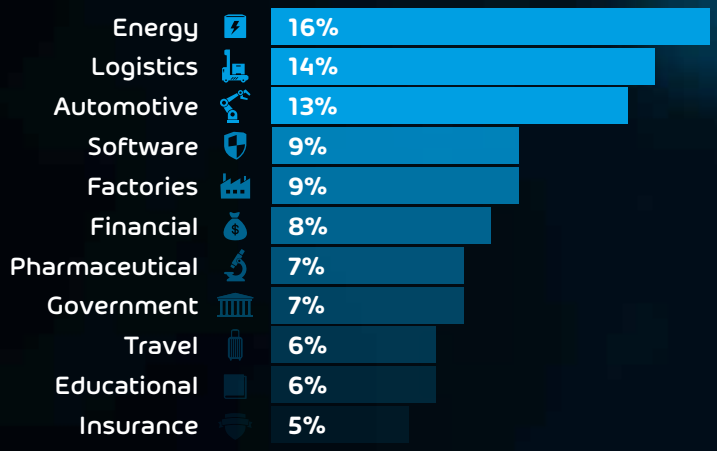

**Fig. 8:** Development of the phishing percentage of all incoming emails in 2019[24]

Hackers are increasingly using current topics to make their phishing emails look as real as possible. As already mentioned in the chapter on social engineering, last year hackers exploited the uncertainty of many users regarding the General Data Protection Regulation as a basis for authentic phishing emails, while also using more sensitive topics such as current disasters as a basis for phishing attacks.

## **Threatened industries:** Energy and logistics sectors particularly vulnerable

The Hornetsecurity Security Lab has analyzed the top 1000 domains with the largest email volume and categorized them by industry. Our experts have delivered a clear result: **Energy utilities top the list of the 10 most frequently attacked sectors with 16 percent.** The logistics sector comes next with 14 percent, followed by the automotive sector with 13 percent. Hackers nevertheless also increasingly targeted software companies, the pharmaceutical industry and the financial sector in 2019.

**Fig. 9:** Top 10 industries under attack in 2019




Energy supply is one of the critical infrastructures, as are individual areas of the logistics sector, such as food transport. In both sectors, operational processes have an impact on the general welfare of society. Cyber-attacks using ransomware put a lot of pressure on the operators. The probability that the money required for decryption is paid in this case may be higher than with other companies.

It is also conceivable that attacks on these sectors are often politically motivated. For example, hackers could use the installation of a backdoor in a critical infrastructure system in order to apply pressure in the event of a crisis.

**Fig. 10:** Attack types on the **energy industry**

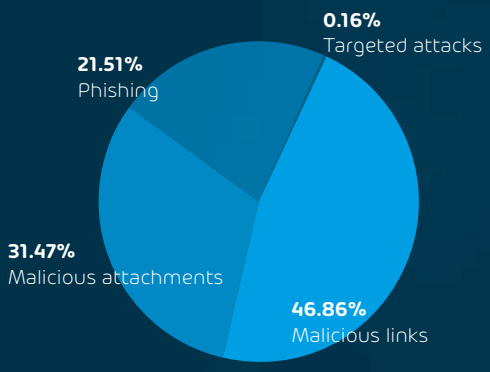



**Fig. 11:** Attack types on the **logistics industry**

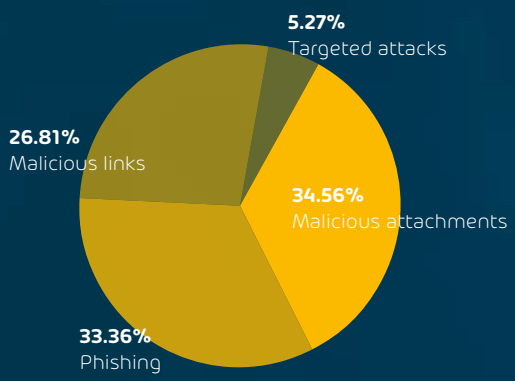
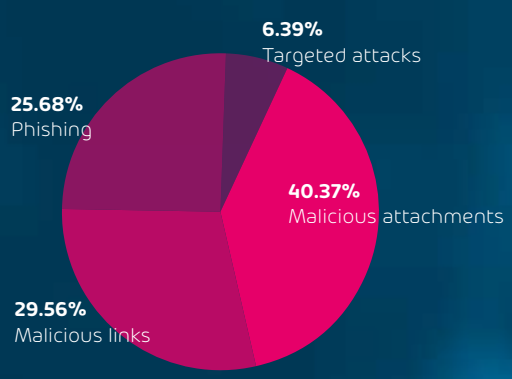



**Fig. 12:** Attack types on the **automotive industry**




**Almost half of the attacks on energy companies were carried out using emails with malicious links.** This trend is due to the fact that many anti-spam solutions can already detect viruses in the attachment. However, emails with malicious attachments continue to be a common route of infection. Almost 20 percent of the attacks were identified as phishing emails and only 0.16 percent as targeted attacks.

The Hornetsecurity Security Lab identified malicious attachments as a popular method of cybercriminal attacks in the logistics and automotive sectors. However, phishing campaigns are also suitable for collecting internal information - particularly in large corporations. The information can be used for industrial espionage as well as for other cyber-attacks, such as spear phishing.

Hackers also use targeted social engineering attacks, such as CEO fraud, to encourage individual employees to transfer large sums of money or to carry out industrial espionage. **Although the methods of attack individual hackers use differ from one industry to another, their motives play an especially decisive role.**

Especially in the area of critical infrastructures, it is safe to assume that the motivation behind cybercriminal activities is not limited to making big money. Strict government system security regulations show that public utilities are considered worthy of protection. The next chapter takes a closer look at the topic of critical infrastructures.

## **When the electricity stop flowing:** Attacks on critical infrastructures

According to the BSI, there were around 157 IT security incidents in the second half of 2018 – compared to only 145 for all of 2017.[25] The threat situation also continued at a consistently high level in 2019, as Security Lab's analysis in the previous chapter shows. While cybercriminals only need to identify a single vulnerability, critical infrastructure operators are faced with the challenge of providing their systems with full and holistic protection.[26]

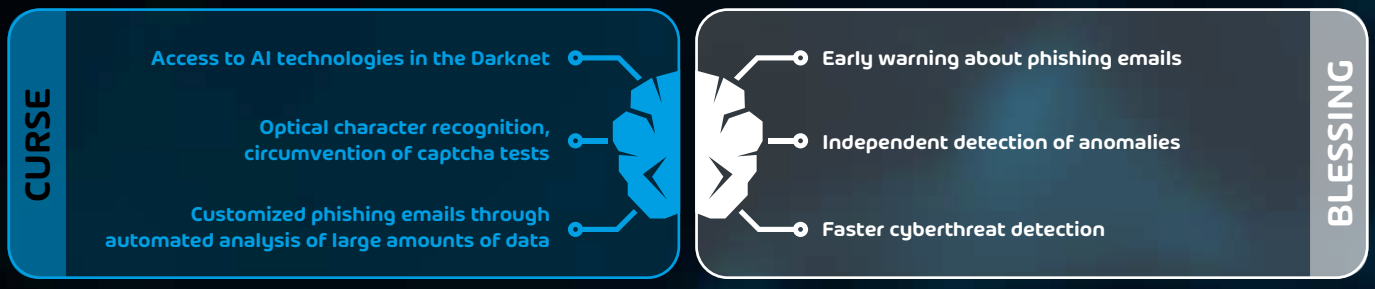
More than half of respondents in a Federal Ministry of Education and Research study on the topic of **IT security in critical infrastructures** stated that they had been victims of cyberattacks last year. There is a wide spectrum of attacks: the use of phishing and ransomware was mentioned above all in connection with critical infrastructures. **60 percent of respondents said they had been hit by cyberattacks of this type.**[27]


As mentioned in the previous chapter, the experts from Hornetsecurity Security Lab reached similar conclusions: The energy industry has been the most frequently attacked industry since the beginning of 2019, with the majority of attacks being carried out via emails containing malicious links or attachments, and around 20 percent as phishing attacks. As even a single successful attack on a public utility can have serious consequences for everyday life, the cybersecurity of critical infrastructures merits special attention.

## **Artificial intelligence:** Curse or blessing?

AI technologies are constantly evolving - just like the complexity of cyberattacks using artificial intelligence as a tool, as the growing AI offering in Darknet shows. Easy access to these technologies likewise increases the risk of hackers exploiting them.

Conventional security technologies, such as captcha tests, can already be circumvented with AI software capable of recognizing and evaluating optical characters.[28] Cybercriminals can also use artificial intelligence to analyze user data, for example **to make phishing emails look even more credible.** Increasing automation through AI will also result in an increasing number of attacks, which in turn will present IT managers with another major challenge.[29]




Companies are nevertheless capable of fighting cybercriminals with their own weapons. **72 percent of corporate decision-makers believe that AI can support cybersecurity when it comes to routine tasks.** For example, artificial intelligence can issue phishing email alerts at an early stage and independently detect anomalies by automatically analyzing metadata. AI can also reduce the number of false-positive alerts because it can precisely and quickly evaluate large amounts of data.[30, 31]

**The length of time viruses, malware and ransomware remain undetected has also fallen by 11 percent thanks to the use of AI.**[32] Artificial intelligence will play a major role in the field of cybersecurity in the future, whether in case of cybercriminal attacks or for defensive purposes.

## **Microsoft Office 365:** Hackers' favorite target

Outsourcing IT infrastructures is becoming increasingly popular, especially with companies and organizations. Two-thirds were already using the Cloud by 2017, and one in five organizations was planning to implement it. **A large part of data traffic will likely be transmitted via the Cloud in the future.** Microsoft's Office 365 Cloud is one of the most popular services of its kind, with the number of subscribers growing by **320 percent between 2015 and 2017**.[33]

Around 100 million business customers use the Microsoft Office 365 Suite – with sensitive data, company secrets and personal information being exchanged and stored there. The high number of users nevertheless also attracts cybercriminals. For example, a considerable increase in attacks was identified as early as 2018. According to Recorded Future, Microsoft occupied eight places on the top ten list of the most exploited vulnerabilities – **six of them in Office applications**.[34] Microsoft itself reported a **250 percent increase in attacks.**[35]

**The top 6** security vulnerabilities are found in Office applications

## How vulnerable is the MS Office Cloud?

**Protection mechanisms controlled by companies, such as the firewall, are no longer available** in the Cloud. Cybercriminals only need to find a single vulnerability in the system to gain access to a wide range of data. Cybercriminals use various methods of concealment to smuggle emails into users' mailboxes and are then capable of accessing the login data of an Office account.

Even a single compromised account in the data cloud offers cybercriminals a platform for many more attacks.[36] From this basis, hackers can prompt other users to transfer large sums of money or carry out espionage, for example through business email compromise attacks.

## **Business email compromise:** Global losses

The financial damage caused by business email compromise is immense. The FBI found out that 166,349 incidents occurred in the USA between June 2016 and July 2019, resulting in more than 26 billion dollars in losses. If you compare the average proceeds that criminals get from a bank robbery with the proceeds generated by business email compromise attacks, the reason for rising cybercrime rates is more than evident.

Bank robbery: **$ 3,000**
Business email compromise: **$ 130,000**

According to the FBI, although cybercriminals use business email compromise to target anyone with money, large companies and organizations with great sums of money are their preferred victims.[37]

Its high number of users had made the Microsoft Office 365 Cloud an attractive target for cybercriminals. Companies are advised to use third-party solutions to ensure they are comprehensively protected. Additional authentication mechanisms prevent unauthorized logins, while the encryption of data in the Cloud offers security against unauthorized access by third parties.

## Outlook

Cybercrime is a growing threat and a downward trend is not expected in the near future. According to the latest findings of the BSI, Emotet is still the most dangerous malware in the world, while ransomware is generally considered the greatest threat to companies and organizations. Despite growing cybersecurity awareness, phishing emails still pose a major threat as cybercriminals continue to perfect their fraud techniques to outwit even trained users.

Critical infrastructures are also increasingly at risk. Cyberattacks on public utilities can pose **a threat to national security**, since an attack on the power grid or water supply can cause massive supply bottlenecks.

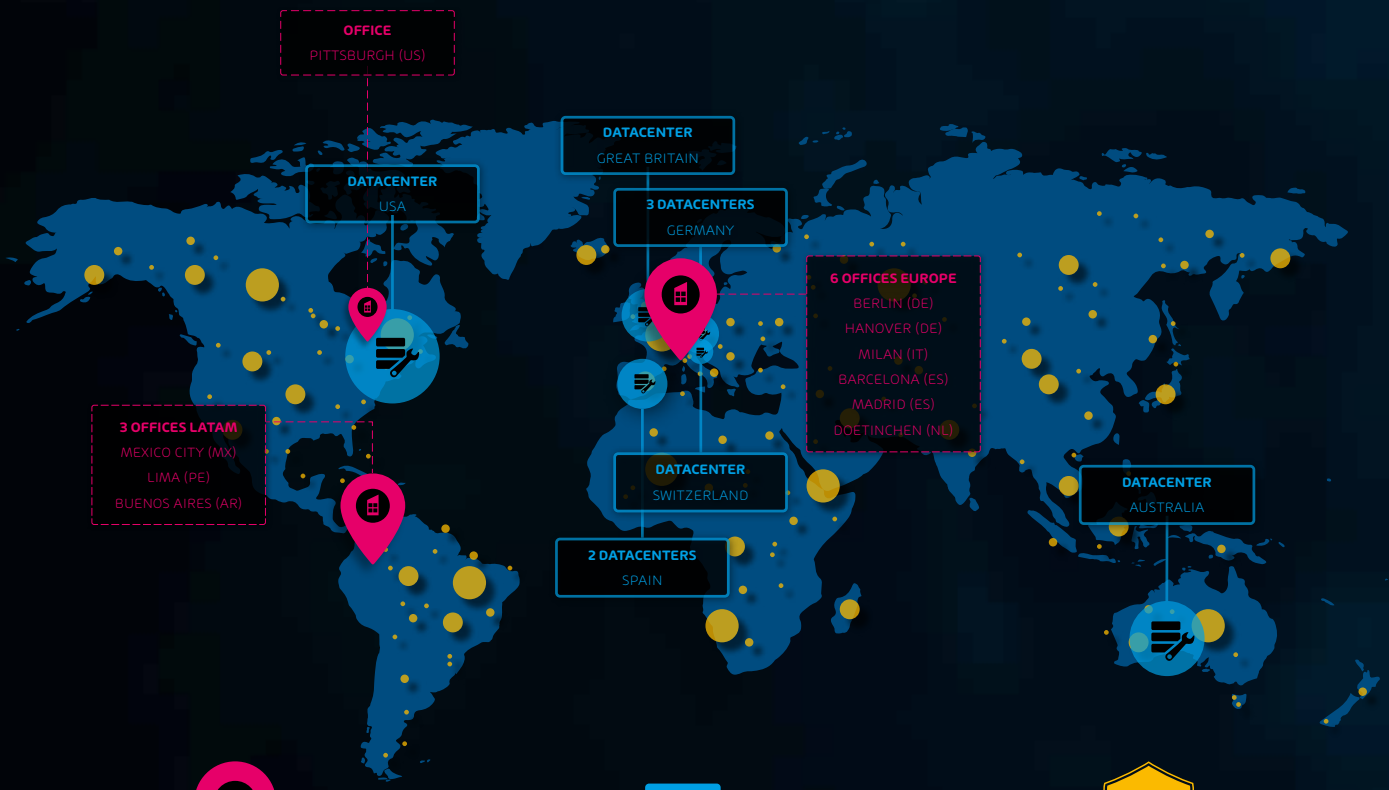

The following can be concluded: cybercriminals are keeping up with technological progress. Their attack patterns are becoming more complex and multi-vector attacks are no longer a rarity. Companies are finding it increasingly difficult to protect themselves against such attacks. **Emails are still the main vector of attack for the majority of cyberattacks.** Office 365 Suite users run an especially high risk of cyberattacks via the email gateway. For them it is essential to protect email communication at all levels with third-party security solutions.


Cyberattacks should be taken as seriously as other crimes. Alongside the theft of sensitive data from private individuals, cyberattacks can inflict immense financial and reputational damage on an organization. This explains why governments around the world have formed alliances or created offices to inform and protect the population about cybercrime and its effects.

## About Hornetsecurity

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 in a short time and are available around the clock. Hornetsecurity has around 200 employees worldwide at ten locations. Its customers include Swisscom, Telefónica, KONICA MINOLTA, LVM Insurance, DEKRA and Claas.

## Hornetsecurity international




**10 OFFICE LOCATIONS**
WORLDWIDE, INCLUDING SIX IN EUROPE

**9 DATACENTERS**
WORLDWIDE, INCLUDING THREE IN GERMANY

**40,000 COMPANIES**
PROTECTED BY US

## Sources


**(1)** https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Internetkriminalitaet/internetkriminalitaet_node.html

**(2)** http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

**(3)** https://www.vdtuev.de/dok_view?oid=769635

**(4)** https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2019.pdf;jsessionid=22BBCB1FB5A36FEE55694AF116A57CB8.1_cid341?__blob=publicationFile&v=6

**(5)** Spam-Statistik Security Lab, Jan 2019 to September 2019

**(6)** https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2019.pdf?__blob=publicationFile&v=6

**(7)** https://www.securitymagazine.com/articles/88907-verizon-2018-data-breach-investigations-report-ransomware-still-a-top-cybersecurity-threat

**(8)** https://www.it-daily.net/shortnews/22517-neue-ransomware-warnung-des-fbi-was-sie-wissen-muessen

**(9)** https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2019.pdf;jsessionid=22BBCB1FB5A36FEE55694AF116A57CB8.1_cid341?__blob=publicationFile&v=6

**(10)** https://klardenker.kpmg.de/der-erpresser-aus-dem-internet/

**(11)** https://www.beazley.com/news/2019/beazley_breach_insights_october_2019.html

**(12)** https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2019.pdf;jsessionid=22BBCB1FB5A36FEE55694AF116A57CB8.1_cid341?__blob=publicationFile&v=6

**(13)** https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2019/Emotet-Warnung_230919.html

**(14)** https://www.heise.de/security/artikel/Emotet-Trickbot-Ryuk-ein-explosiver-Malware-Cocktail-4573848.html

**(15)** https://www.stern.de/digital/online/emotet--darum-ist-der-trojaner-so-gefaehrlich---und-so-schuetzen-sie-sich-8548334.html

**(16)** https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2018/BSI_warnt_vor_Emotet.html

**(17)** https://www.heise.de/security/meldung/Trojaner-Alarm-BSI-warnt-vor-zunehmenden-Emotet-Angriffen-4537594.html

**(18)** https://siliconangle.com/2019/08/05/ibm-report-finds-destructive-malware-attacks-doubled-since-january/

**(19)** https://www.sentinelone.com/blog/robinhood-ransomware-coolmaker-function-not-cool/

**(20)** https://securityintelligence.com/posts/from-state-sponsored-attackers-to-common-cybercriminals-destructive-attacks-on-the-rise/

**(21)** https://www.welivesecurity.com/deutsch/2016/12/13/12-sicherheitstipps-zur-weihnachtszeit/

**(22)** https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/813599/Cyber_Security_Breaches_Survey_2019_-_Main_Report.pdf

**(24)** https://www.heise.de/newsticker/meldung/Mehr-Hacker-Angriffe-auf-kritische-Infrastruktur-beim-BSI-gemeldet-4311172.html

**(25)** Phishing-Statistik aus dem Hornetsecurity Security Lab

## Sources


**(26)** https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/bsi-lagebericht-2019.pdf?__blob=publicationFile&v=4

**(27)** https://monitor.itskritis.de/ITSKRITIS_Monitor_2_digital.pdf

**(28)** https://www.it-daily.net/it-sicherheit/cyber-defence/20434-cyberangriffe-kuenstliche-intelligenz-als-fluch-oder-segen

**(29)** https://www.wissenschaftsjahr.de/2019/neues-aus-der-wissenschaft/das-sagt-die-wissenschaft/kuenstliche-intelligenz-schutzschild-und-einfallstor-fuer-cyberattacken/

**(30)** https://www.eco.de/presse/internet-security-days-2019-mit-ki-cyberangriffe-abwehren/

**(31)** https://www.eco.de/presse/das-sind-die-it-security-trends-2019/

**(32)** https://www.capgemini.com/de-de/wp-content/uploads/sites/5/2019/07/Report_AI_in_Cybersecurity_Capgemini_Research_Institute.pdf

**(33)** https://www.computerwoche.de/a/datenschutz-in-microsoft-office-365-ist-lueckenhaft,3546637

**(34)** https://www.recordedfuture.com/top-vulnerabilities-2018/

**(35)** https://businessinsights.bitdefender.com/microsoft-phishing-attacks-increased-250-from-january-to-december-2018

**(36)** https://www.beazley.com/news/2018/beazley_breach_insights_april_2018.html

**(37)** https://www.secureworldexpo.com/industry-news/new-business-email-compromise-statistics-bec