Cybersecurity: main and emerging threats

Find out about the top cyber threats in 2022, the most affected sectors and the impact of the war in Ukraine.

The digital transformation has inevitably led to new cybersecurity threats. During the coronavirus pandemic, companies had to adapt to remote working and this created more possibilities for cybercriminals. The war in Ukraine has also affected cybersecurity.

In response to the evolution of cybersecurity threats, Parliament adopted a new EU directive introducing harmonised measures across the EU, including on the protection of essential sectors.

Read more on new EU measures to fight cybercrime

Discover the main cybersecurity threat types

Source: European Union Agency for Cybersecurity (2022)
PRIME CYBERSECURITY THREATS

**Threats against data**
82% of data breaches involve a human element. Manipulation of people and human errors are among the main patterns.

**Threats against availability**
**DENIAL OF SERVICE**
Distributed denial-of-service (DDoS) attacks are getting larger and more complex and are moving towards mobile networks and Internet of Things devices.

**Availability of the Internet**
This includes the physical take-over and destruction of Internet infrastructure. According to the Ukrainian government, around 15% of the country’s Internet infrastructure had been destroyed as of June 2022.

Source: European Union Agency for Cybersecurity (2022)

Discover the main cybersecurity threat types

---

**Disinformation/misinformation**
AI is becoming central in creating and spreading disinformation, for example through deepfake technology and bots impersonating people.

**Supply chain threats**
Attacking, for example, a service provider in order to access customer data. The complexity of supply chains has increased the risk and consequences of these attacks for many organisations.

Source: European Union Agency for Cybersecurity (2022)

Discover the main cybersecurity threat types
Top 8 cybersecurity threats in 2022 and beyond

According to the Threat Landscape 2022 report by the European Union Agency for Cybersecurity (Enisa), there are eight prime threat groups:

1. Ransomware: hackers seize control of someone’s data and demand a ransom to restore access

In 2022, ransomware attacks continued to be one of the main cyberthreats. They are also getting more complex. According to a survey quoted by Enisa that was conducted at the end of 2021 and in 2022, over half of respondents or their employees had been approached in ransomware attacks.

Data quoted by the EU Agency for Cybersecurity shows that the highest ransomware demand grew from €13 million in 2019 to €62 million in 2021 and the average ransom paid doubled from €71,000 in 2019 to €150,000 in 2020. It is estimated that in 2021 global ransomware reached €18 billion worth of damages – 57 times more than in 2015.

2. Malware: software that harms a system

Malware includes viruses, worms, Trojan horses and spyware. After a global decrease in malware linked to the Covid-19 pandemic in 2020 and early 2021, its use increased heavily by the end of 2021, as people started returning to the office.

The rise of malware is also attributed to crypto-jacking (the secret use of a victim’s computer to create cryptocurrency illegally) and Internet-of-Things malware (malware targeting devices connected to the internet such as routers or cameras).

According to Enisa, there were more Internet-of-Things attacks in the first six months of 2022 than in the previous four years.

3. Social engineering threats: exploiting human error to gain access to information or services

Tricking victims into opening malicious documents, files or emails, visiting websites and thus granting unauthorised access to systems or services. The most common attack of this sort is phishing (through email) or smishing (through text messages).
Almost 60% of the breaches in Europe, the Middle East and Africa include a social engineering component, according to research quoted by Enisa.

The top organisations impersonated by phishers were from the financial and technology sectors. Criminals are also increasingly targeting crypto exchanges and cryptocurrency owners.

4. Threats against data: targeting sources of data to get unauthorised access and disclosure

We live in a data-driven economy, producing huge amounts of data that are extremely important for, among others, enterprises and Artificial Intelligence, which makes it a major target for cybercriminals. Threats against data can be mainly classified as data breaches (intentional attacks by a cybercriminal) and data leaks (unintentional releases of data).

Money remains the most common motivation of such attacks. Only in 10% of cases is espionage the motive.

Read more about how the EU wants to boost data sharing and regulate AI

5. Threats against availability - Denial of Service: attacks preventing users from accessing data or services

These are some of the most critical threats to IT systems. They are increasing in scope and complexity. One common form of attack is to overload the network infrastructure and make a system unavailable.

Denial of Service attacks are increasingly hitting mobile networks and connected devices. They are used a lot in Russia-Ukraine cyberwarfare. Covid-19 related websites, such as those for vaccination have also been targeted.

6. Threats against availability: threats to the availability of the internet

These include physical take-over and destruction of internet infrastructure, as seen in occupied Ukrainian territories since the invasion, as well as the active censoring of news or social media websites.
7. Disinformation/misinformation: the spread of misleading information

The increasing use of social media platforms and online media has led to a rise in campaigns spreading disinformation (purposefully falsified information) and misinformation (sharing wrong data). The aim is to cause fear and uncertainty.

Russia has used this technology to target perceptions of the war.

Deepfake technology means it is now possible to generate fake audio, video or images that are almost indistinguishable from real ones. Bots pretending to be real people can disrupt online communities by flooding them with fake comments.

Read more about the sanctions against disinformation the Parliament is calling for

8. Supply-chain attacks: targeting the relationship between organisations and suppliers

This is a combination of two attacks - on the supplier and on the customer. Organisations are becoming more vulnerable to such attacks, because of increasingly complex systems and a multitude of suppliers, which are harder to oversee.
Top sectors affected by cybersecurity threats

Cybersecurity threats in the European Union are affecting vital sectors. According to Enisa, the top six sectors affected between June 2021 and June 2022 were:

1. Public administration/government (24% of incidents reported)
2. Digital service providers (13%)
3. General public (12%)
4. Services (12%)
5. Finance/banking (9%)
6. Health (7%)

Read more on the costs of cyberattacks

The impact of the war in Ukraine on cyberthreats
Russia’s war on Ukraine has influenced the cyber sphere in many ways. Cyber operations are used alongside traditional military action. According to Enisa, actors sponsored by the Russian state have carried out **cyber operations** against entities and organisations in Ukraine and in countries that support it.

**Hacktivist** (hacking for politically or socially motivated purposes) activity has also increased, with many conducting attacks to support their chosen side of the conflict.

**Disinformation** was a tool in cyberwarfare before the invasion started and both sides are using it. Russian disinformation has focused on finding justifications for the invasion, while Ukraine has used disinformation to motivate troops. Deepfakes with Russian and Ukrainian leaders expressing views supporting the other side of the conflict were also used.

Cybercriminals tried to **extort money** from people wanting to support Ukraine via fake charities

**Cybercrime and cybersecurity**

Enisa: Cybersecurity Threats Fast-Forward 2030
Europol: cybercrime