IW-Kurzbericht Nr. 15/2022

How the Russian cyber warfare threatens European businesses

Vera Demary, 25.02.2022

The Russian attack on Ukraine took place long before the current ground, sea, and air attack: It started online. The conflict is also a cyber war with extensive cyberattacks. This can severely impact European businesses.

In general, hackers often pursue goals such as personal enrichment with their attacks on the systems and devices of private individuals, companies or even states, for example through extortion using ransomware or the manipulation or outflow of data. In addition, cyberattacks are also used to pursue political, strategic, and military goals. Russia has been waging such cyber warfare against Ukraine for a long time and is also using cyberattacks during the current invasion. It is likely that collateral damage will occur in other countries and that European businesses will also be affected.

War with cyberattacks

The measures of cyber warfare are manifold. They range from targeted misinformation in social networks to espionage on the data, systems and hardware of the adversary and its allies to cyberattacks aimed at sabotaging their information and communications infrastructure or even the physical destruction of industrial facilities or the like (CSIS, 2022).

The goals of these measures are to weaken the enemy, demoralize the population and the foreign public, and thus ultimately to "win" the war and achieve political, strategic, or military objectives. In this context, the attackers themselves do not necessarily have to be state actors but can also be private attackers tolerated by the state (CISA, n.d.).

Even before the Russian invasion in Ukraine, the majority of cyberattacks perpetrated against Ukrainian government agencies, defense, and high-tech companies were the work of Russian actors (figure). The total number of cyber incidents in Ukraine recorded in the Center for Strategic and International Studies database since 2011 was similar to that in Germany. However, the actors differed significantly: four out of five cyberattacks on Ukraine originated in Russia. In Germany, most attacks could not be attributed to any state. Russian actors accounted for 28 percent of cyber incidents in this country.

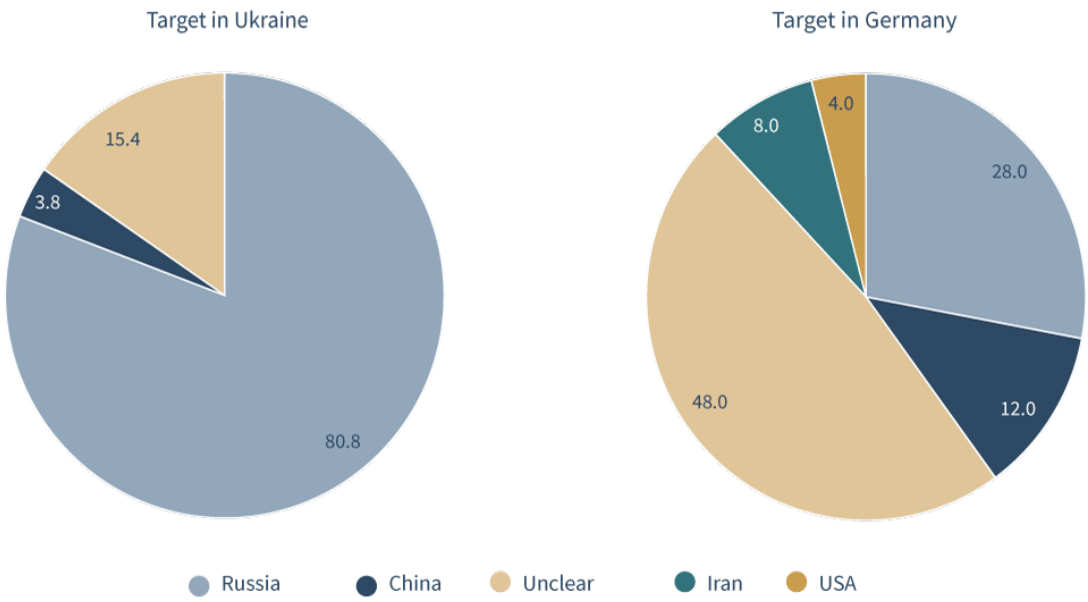
Since the Russian invasion, Ukrainian authorities and companies have repeatedly been the target of cyberattacks: The websites of banks and military organizations have been crippled. Software that systematically deletes data has been installed on hundreds of computers (Tidy, 2022). It can be assumed that the intensity of these attacks will continue to increase (Alazab, 2022).

Potential impact on European companies

The Russian cyber war with Ukraine may also spread to other states. The German Federal Office for Information Security (BSI) warned German companies of this this week (Tagesschau.de, 2022). First, the danger is that cyberattacks on Ukraine are not limited to systems, hardware, and data there, but also spread to

Cyberattacks on Ukraine and Germany

Significant cyberattacks on government agencies, defense and high-tech companies, or with more than $1 million in damage, since 2011, as a percentage of attacks



As of January 2022
Source: Own calculations based on Center for Strategic and International Studies, 2022

connected accounts in other states. The "Petya/NotPetya" malware, which spread beyond Ukraine to the United States and Europe in 2017, is an example of such an effect (Alvarez de Souza et al., 2022). Second, the Russian president has threatened consequences if other states interfere in the war. It is therefore possible that EU sanctions against Russian companies and sectors could also result in cyberattacks on European businesses. The risk of this appears considerable against the backdrop of the BSI warning.

Even without this additional risk, European companies are already often the target of cyberattacks. Take Germany, for example: In 2020, damages of 223.5 billion euros were estimated for the German economy due to data theft, espionage and sabotage (Bitkom, 2021). Many cyberattacks as well as the associated damage in companies are not even reported; therefore, the numer of cases as well as the damages are likely underestimated. However, the impact of such incidents on companies is enormous: In addition to the direct costs of repairing the damage and the loss of data, there are indirect costs, for example, for lost sales or damage to reputation and brand (Engels, 2017, 12 ff.).

The immense extent of the damage that cyberattacks can have is also confirmed by a survey conducted by the BSI for Germany: 26 percent of the companies affected by cyberattacks during the pandemic stated that the damage was very great or even threatened their very existence (BSI, 2021, 17). At the same time, only 16 percent sought to increase their IT security budget (ibid., 13). This is alarming in view of the threat situation. To keep damage to a minimum in the event of a cyberattack, resilient IT security systems are urgently needed - even in companies that do not belong to the critical infrastructures. This requires investments in smart security solutions as well as regular checks and updates.

References

Alazab, Mamoun, 2022, Russia is using an onslaught of cyber attacks to undermine Ukraine's defence capabilities, https://bit.ly/3ta47gD [25.2.2022]

Alvarez de Souza, Philipp / Holzki, Larissa / Karabasz, Ina, 2022, Hackerangriffe. Telekomchef Höttges warnt vor Cyberattacken in der Ukrainekrise: „Die Bedrohung ist da", https://bit.ly/3t4TnQB [25.2.2022]

Bitkom, 2021, Wirtschaftsschutz 2021, Berlin

BSI – Bundesamt für Sicherheit in der Informationstechnik, 2021, IT-Sicherheit im HOME-OFFICE, Bonn

CISA – Cybersecurity & Infrastructure Security Agency, o. J., Cyber Threat Source Descriptions, https://bit.ly/36GPJVx [25.2.2022]

CSIS – Center for Strategic and International Studies, 2022, Significant Cyber Incidents since 2006, Washington

Engels, Barbara, 2017, Wirtschaftliche Kosten der Cyberspionage für deutsche Unternehmen. Cybersicherheit als Grundvoraussetzung der digitalen Transformation, IW-Policy Paper, Nr. 6, Köln

Tagesschau.de, 2022, Ukraine-Krise. BSI warnt vor Cyberattacken, https://bit.ly/3t45H3G [25.2.2022]

Tidy, Joe, 2022, Ukraine crisis: 'Wiper' discovered in latest cyber-attacks, https://bbc.in/3pfrW5t [25.2.2022]