Bitkom e.V. |

German businesses under attack: losses of more than 220 billion euros per year

- **Theft, espionage, sabotage: nine out of ten companies have been victims**
- **Blackmail, system failures, and malfunctions more than quadrupled**
- **Every tenth company is already seeing this as a threat to their existence**

Berlin, 5th August 2021 – Theft, espionage, and sabotage cause total annual losses of 223 billion euros for German businesses. Again, these are record losses caused by criminal attacks: Total losses are more than twice as high as during the years 2018–2019, when they were still at 103 billion euros per year. Nine out of ten companies (88 percent) were affected by attacks in the years 2020–2021. Between 2018–2019, three quarters (75 percent) have been victims. These are the results of a representative study of more than 1,000 companies across all industries, which was commissioned by Germany's digital industry association, Bitkom.

The main driver behind this enormous increase were cases of blackmail connected to failing information and production systems and the disruption of business operations. They are mostly the immediate consequence of ransomware attacks, which block computers and other systems, then blackmail the operators. The losses caused by this have more than quadrupled (+358 percent) compared to the previous years, 2018–2019. Presently, every tenth company (9 percent) sees its existence threatened by cyberattacks.

"The force with which ransomware attacks are shaking our economy is alarming and affects companies of all industries and sizes," says Bitkom's president Achim Berg, speaking on the current development. By encrypting systems, a company's business operations are brought to a standstill. Stolen customer and company data do more than damage reputations. They also deplete competitiveness, warns Berg: "For an innovation-driven economy like Germany's, theft of intellectual property can have dire consequences."

During the presentation of the results with Berg, Sinan Selen, president of the Federal Office for the Protection of the Constitution, explained: "The recent Bitkom survey underscores how important a resilient economy is for Germany as a business location. The coronavirus pandemic has drastically reinforced this need. The only way we can effectively counter threats of sabotage and espionage is through in-depth cooperation between businesses and the authorities."

Social engineering is the starting point of many attacks, working-from-home provides additional gateway

Most attacks start with social engineering, i.e., the manipulation of employees. Criminals make use of "human error", identifying the weakest link in a security chain to procure sensitive data like passwords. Most recently, 41 percent of the surveyed companies experienced such attempts – 27 percent of respondents reported being contacted via telephone, 24 percent via email. It can be surmised that this is mainly due to a changing working environment during the coronavirus pandemic.

Of the surveyed companies that principally enable staff to work from home (817 companies), 59 percent reported IT security-related incidents since the start of the pandemic that can be attributed to working from home. At 24 percent of these companies, this has happened frequently. Half of those incidents that could be attributed to working from home also incurred damage. Berg: "Simply sending staff home is not enough. Devices must be secured, communication channels to companies must be protected, and staff need to be made aware of dangers. It would be negligent not to do so."

Responding to the worsening threat situation, companies have upped their investment in IT security: 24 percent made significant increases, 39 percent some. Expenditures remained unchanged at 33 percent of the surveyed companies. Compared to the overall IT budget, however, expenditures for more security are continually low. Companies spend an average of 7 percent of their IT funds on security.

Malware, DoS attacks, and spoofing are on the rise

Malware infection is putting particular pressure on German businesses: in 2020–2021, malware has incurred losses at 31 percent of the surveyed companies. So-called DoS attacks, in which the perpetrators overload certain resources, for example, by bringing down servers with mass requests, were registered by 27 percent. Spoofing, i.e., assuming a false identity, or phishing, i.e., intercepting personal information have incurred losses at 20 and 18 percent of companies, respectively. The number of spoofing attempts rose sharply by 12 percent compared to the years 2018–2019. The occurrence of DoS attacks rose by 9 percent.

Attacks focus on communication data and intellectual property

More than ever, data thieves go after communication data and intellectual property. In companies that have recently had sensitive digital data stolen from them, 63 percent of those were communication data. Intellectual property like patents or research information were stolen from 18 percent – an increase of 11 percent compared to the years 2018–2019. In other cases, the loot consisted of non-critical business data (44 percent), customer data (31 percent), financial data (29 percent), and critical business data such as market analyses (19 percent). In 19 percent of cases, access information to cloud services were stolen.

Organised crime continues to grow

A closer look at those perpetrating these damaging actions (multiple responses possible) showed the following: at 61 percent of the companies affected by theft, espionage, and sabotage, the damage was caused by employees, some of which after they had already left the companies in question. Of those companies, 42 percent reported that the employees acted unintentionally. In contrast, 28 percent of the companies assumed that the damage was caused intentionally. Insufficiently trained or inattentive staff also continue to be a pivotal problem for German businesses. Many attacks come from outside the companies, including private individuals and hobby hackers (40 percent). However, the starkest increase compared to previous years can be accounted to organised crime: in the years 2016–2017, 7 percent of the affected companies traced back attacks to organised crime; 21 percent in 2018–2019. In 2020–2021, this number has risen to 29 percent.

Most attacks come from Germany: 43 percent of the affected companies suspect the attackers to be of domestic origin. 37 percent state that the criminal acts were committed from Eastern Europe (not counting Russia) (2018–2019: 28 percent). China (30 percent) and Russia (23 percent) were also frequently identified as the countries of origin, less frequently the US (6 percent), while 31 percent of the companies could not specify where they were attacked from. This number increased by 7 percent compared to 2018–2019 – indicating successful concealment on behalf of the attackers.

No relief in sight: Critical infrastructure is particularly under threat

The prevailing opinion among German businesses is that the threat situation caused by cyberattacks will become increasingly serious in the months to come: 83 percent of the surveyed companies expect the number of attacks to increase until late this year, 45 percent expect a strong increase. Operators of critical infrastructure see themselves under particular threat (52 percent of them expect a strong increase in attacks on their companies) as well as medium-sized companies with

between 100 and 499 employees (50 percent of them expect a strong increase).

Companies view ransomware attacks as the greatest danger. 96 percent see themselves as threatened by such attacks. Exploiting new security holes (so-called zero-day vulnerabilities) are feared by 95 percent of the companies. Other threats feared by the business community include spyware attacks (83 percent), attacks with quantum computers (79 percent), and so-called backdoor attacks (78 percent).

The German business community expects an effective political response to be better protected against theft, espionage, and sabotage in the future: 99 percent of companies call for stronger action against foreign cyberattacks, increased EU cooperation on cybersecurity as well as improved information sharing on IT security issues between the government and the business community. 94 percent would like to see a funding programme for more IT security for staff working from home. 85 percent of companies hope for an increased commitment on behalf of the government to protect businesses against cyberattacks.

Bitkom's president Berg has already appealed to the nascent federal government: "Protecting German businesses is crucial to ensuring the continued success and the global appeal of Germany as a business location. In addition to an open and honest dialogue with the business community, more action is needed at all levels during the next legislative period," says Berg. Upping the protection of businesses and building the necessary cyber resilience can only succeed "if the coming federal government stands shoulder-to-shoulder with the business community."

Methodology note: The basis of these data is a survey conducted by Bitkom Research, commissioned by Germany's digital industry association, Bitkom. It involved interviewing 1,067 companies with 10 or more employees. The interviews were conducted with executives who are responsible for security in their respective companies. This includes managing directors and executives from the areas corporate security, IT security, risk management, or finance. The survey results are representative of the business community as a whole.

Contact person

Andreas Streim
Press Officer
Phone: +49 30 27576-112
E-Mail: a.streim@bitkom.org
Download press photo

Felix Kuhlenkamp
Policy Lead Security Policy
Download press photo
Send message

Direct link: ***https://www.bitkom.org/EN/List-and-detailpages/Press/German-business-losses-more-than-220-billion-euros-per-year***