Economic Security 2022

Achim Berg, President of Bitkom e.V.

Berlin, 31 August 2022
German trade and industry as a whole under attack

Has your company been the target of theft, industrial espionage or sabotage within the past twelve months (2017 and 2019: within the past two years)?

<table>
<thead>
<tr>
<th>Year</th>
<th>Presumably targeted</th>
<th>Definitely targeted</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017</td>
<td>53</td>
<td>26</td>
</tr>
<tr>
<td>2019</td>
<td>75</td>
<td>13</td>
</tr>
<tr>
<td>2021</td>
<td>88</td>
<td>12</td>
</tr>
<tr>
<td>2022</td>
<td>84</td>
<td>9</td>
</tr>
</tbody>
</table>

Basis: All the companies taking part in the survey (n=1,066) | Source: Bitkom Research 2022
Attacks shifting into the digital sphere

What was the kind of attack carried out against your company in the past twelve months, among the following ones?

- Theft of IT or telecommunications devices
- Theft of sensitive digital data and/or information
- Spying on digital communications
- Digital sabotage of information and production systems or operational procedures
- Analog theft of sensitive physical documents, papers, patterns, equipment, components etc.
- Eavesdropping on discussions or phone conversations
- Analog sabotage of information and production systems or operational procedures

Basis: All the companies taking part in the survey (n=1,066) | Source: Bitkom Research 2022
Data theft: More and more frequently it is third parties who are concerned

What was the kind of digital data stolen in your company, among the following ones?

Basis: All the companies taking part in the survey which have been targets of the theft of sensitive digital data in the past 12 months (2019: past 2 years) (2022: n=383; 2021: n=330; 2019: n=229) | Multiple choices were possible | Source: Bitkom Research 2022

- Communications data, such as email
- Customer data
- Noncritical business information
- Access data for Cloud services
- Critical business information, such as market analyses, pricing
- Data on employees
- Intellectual property, such as patents, information from research and development
- Financial data

in percent
Cyber attacks threaten existence of many companies

Do you agree with the statement or not?

Cyber attacks threaten our corporate existence.

9% (2021)
45% (2022)

Basis: All the companies taking part in the survey (n=1,066) | Source: Bitkom Research 2022
Critical infrastructures increasingly targeted by cyber attacks

How have the numbers of cyber attacks staged against your company developed in the past twelve months?

<table>
<thead>
<tr>
<th>Basis: All the companies taking part in the survey (n=1.066)</th>
<th>Source: Bitkom Research 2022</th>
</tr>
</thead>
</table>

- **In total**: 39% significant increase, 45% moderate increase, 14% no change, 2% significant decrease
- **Sectors in critical infrastructure**: 49% significant increase, 38% moderate increase, 10% no change, 4% significant decrease
- **Sectors in noncritical infrastructure**: 37% significant increase, 46% moderate increase, 15% no change, 2% significant decrease
More damage due to phishing & theft of passwords

What was the kind of cyber attack that has inflicted damage on your company in the past twelve months, among the following ones?

- Attacks on passwords
- Phishing
- Infection with malware
- Distributed Denial of Service (DDoS)
- Spoofing
- Cross Site Scripting (XSS)
- SQL injection
- Ransomware
- "Man in the middle" attack
- CEO fraud

2022
2021

Basis: All the companies taking part in the survey (n=1,066) | Multiple choices were possible | Source: Bitkom Research 2022
Social Engineering: Every second company among the targets

As for attempts to influence your employees through social engineering made in the past twelve months: In which of the following situations did they take place?

- On the phone: 38% (2022), 34% (2021)
- Via email: 27% (2022), 24% (2021)
- In a private environment: 13% (2022), 10% (2021)
- In job-related social networks: 9% (2022), 5% (2021)
- In private social networks: 5% (2022), 4% (2021)
- In video conferences: 4% (2022), 3% (2021)
- At fairs or events: 3% (2022), 4% (2021)
- n/a: 4% (2022), 3% (2021)

48% There have been attempts of social engineering (2021: 41%)

Basis: All the companies taking part in the survey (n=1,066) | Multiple choices were possible | Source: Bitkom Research 2022
# Annual damage of 203 billion euros

What have been the circumstances causing damage to your company due to theft, industrial espionage or sabotage in the past twelve months?

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure, theft or impairment of information and production systems or operational procedures</td>
<td>41.5</td>
<td>61.9</td>
<td>13.5</td>
<td>5.3</td>
</tr>
<tr>
<td>Blackmailing using stolen or encrypted data</td>
<td>10.7</td>
<td>24.3</td>
<td>5.3</td>
<td>0.7</td>
</tr>
<tr>
<td>Measures under data protection law (e.g. informing of customers)</td>
<td>18.3</td>
<td>17.1</td>
<td>4.4</td>
<td>3.2</td>
</tr>
<tr>
<td>Violations of patent law (also before the application)</td>
<td>18.8</td>
<td>30.5</td>
<td>14.3</td>
<td>7.7</td>
</tr>
<tr>
<td>Revenue losses through losing competitive advantages</td>
<td>41.5</td>
<td>29</td>
<td>11.1</td>
<td>8.6</td>
</tr>
<tr>
<td>Revenue losses through imitated products (plagiarism)</td>
<td>21.1</td>
<td>22.7</td>
<td>11.1</td>
<td>3.5</td>
</tr>
<tr>
<td>Tarnished image in the eyes of customers or suppliers / Negative press coverage</td>
<td>23.6</td>
<td>12.3</td>
<td>9.3</td>
<td>7.7</td>
</tr>
<tr>
<td>Costs for investigations and compensating measures</td>
<td>10.1</td>
<td>13.3</td>
<td>18.3</td>
<td>10.6</td>
</tr>
<tr>
<td>Costs for legal disputes</td>
<td>16.2</td>
<td>12.4</td>
<td>15.6</td>
<td>5.5</td>
</tr>
<tr>
<td>Increase in staff fluctuation / Poaching</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>2.2</td>
</tr>
<tr>
<td>Other losses</td>
<td>0.9</td>
<td>0</td>
<td>&lt;0.1</td>
<td>&lt;0.1</td>
</tr>
<tr>
<td><strong>Total annual damage</strong></td>
<td><strong>202.7</strong></td>
<td><strong>223.5</strong></td>
<td><strong>102.9</strong></td>
<td><strong>54.8</strong></td>
</tr>
</tbody>
</table>

Basis: All the companies taking part in the survey which have been targets of theft, data theft, industrial espionage or sabotage in the past 12 months (2019 and 2017: past 2 years) (2022: n=899; 2021: n=935; 2019: n=801; 2017: n=571) | Multiple choices were possible | Source: Bitkom Research 2022
Attacks against Germany: The East has come to the fore

Have you been able to ascertain from where and/or from what region these activities were undertaken?

- 32% in Germany (32% -11%P)
- 27% in Eastern Europe (Russia excluded) (-10%P)
- 8% in EU countries (Germany excluded) (+5%P)
- 4% in n/a (Region not known) (+4%P)
- 35% in Region not known (+4%P)
- 21% in USA (+5%P)
- 43% in China (+13%P)
- 36% in Russia (+13%P)

Basis: All the companies taking part in the survey which have been targets of theft, industrial espionage or sabotage in the past 12 months (2022: n=899; 2021: n=935) | Multiple choices were possible | Source: Bitkom Research 2022
Attacks against trade and industry becoming more professional

Who were the perpetrators undertaking pertinent activities in the past twelve months?

Organised crime / gangs
Private persons / hobby hackers
(Former) employees acting unintentionally
(Former) employees acting intentionally
Competitors
Customers
Foreign intelligence services
Suppliers
External service providers

Basis: All the companies taking part in the survey which have been targets of theft, data theft, industrial espionage or sabotage in the past 12 months (2019: past 2 years) (2022: n=899; 2021: n=935; 2019: n=801) | Multiple choices were possible | Source: Bitkom Research 2022
Trade and industry expect cyber attacks to increase

How do you expect the number of cyber attacks against your company to develop in the next 12 months in comparison with the last 12 months?

<table>
<thead>
<tr>
<th></th>
<th>Will significantly increase</th>
<th>Will moderately increase</th>
<th>No change</th>
<th>Will moderately decrease</th>
<th>Will significantly decrease</th>
<th>n/a</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sectors in critical infrastructure</td>
<td>51</td>
<td>33</td>
<td>10</td>
<td>6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sectors in noncritical infrastructure</td>
<td>40</td>
<td>37</td>
<td>20</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>In total</td>
<td>42</td>
<td>36</td>
<td>18</td>
<td>4</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Basis: All the companies taking part in the survey (n=1.066) | Source: Bitkom Research 2022
Cyber security: Percentage of investment for protection purposes increases – but too slowly

According to your assessment: What is the percentage of the proportion of the IT security budget in relation to the total IT budget in your company?

Basis: All the companies taking part in the survey (n=1,066) | Source: Bitkom Research 2022
## Companies fear ransomware & zero-day exploits

How much do you consider the following scenarios a future threat to your company’s IT security?

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Significant threat</th>
<th>Moderate threat</th>
<th>Insignificant threat</th>
<th>No threat at all</th>
<th>n/a</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ransomware attack</td>
<td>59</td>
<td>33</td>
<td>5</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Zero-day exploit</td>
<td>55</td>
<td>36</td>
<td>9</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Spyware attack</td>
<td>49</td>
<td>36</td>
<td>12</td>
<td>21</td>
<td></td>
</tr>
<tr>
<td>Backdoors and/or trapdoors</td>
<td>35</td>
<td>38</td>
<td>18</td>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>Attacks using quantum computers</td>
<td>42</td>
<td>30</td>
<td>11</td>
<td>11</td>
<td>6</td>
</tr>
<tr>
<td>Lack of IT security experts</td>
<td>37</td>
<td>35</td>
<td>16</td>
<td>10</td>
<td>3</td>
</tr>
<tr>
<td>Increasing interconnectedness of devices and equipment</td>
<td>27</td>
<td>42</td>
<td>24</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Social engineering</td>
<td>41</td>
<td>22</td>
<td>17</td>
<td>16</td>
<td>4</td>
</tr>
<tr>
<td>Misconfigured Cloud environment</td>
<td>32</td>
<td>26</td>
<td>23</td>
<td>16</td>
<td>3</td>
</tr>
<tr>
<td>Increasing staff fluctuation</td>
<td>23</td>
<td>35</td>
<td>31</td>
<td>10</td>
<td>1</td>
</tr>
<tr>
<td>Tapping of processing power, e.g. for covertly mining cryptocurrency</td>
<td>14</td>
<td>33</td>
<td>23</td>
<td>22</td>
<td>8</td>
</tr>
</tbody>
</table>

Significant threat & Moderate threat

- Ransomware attack: 92%
- Zero-day exploit: 91%
- Spyware attack: 85%
- Backdoors and/or trapdoors: 73%
- Attacks using quantum computers: 72%
- Lack of IT security experts: 72%
- Increasing interconnectedness of devices and equipment: 69%
- Social engineering: 63%
- Misconfigured Cloud environment: 58%
- Increasing staff fluctuation: 58%
- Tapping of processing power, e.g. for covertly mining cryptocurrency: 47%

Basis: All the companies taking part in the survey (n=1,066) | Source: Bitkom Research 2022
More initiative from political circles demanded

Do you agree with the following general statements on current political debates in the field of economic security?

Policy makers should take stronger action against cyber attacks from abroad. 98%

Policy makers should actively promote EU-wide cooperation in the field of cyber security. 97%

Policy makers should expand investigatory powers for the investigation of cyber attacks. 77%

The bureaucratic expense for reporting incidents is too large. 77%

Basis: All the companies taking part in the survey (n=1.066) | Percent points for “Totally agree” and “Rather agree” | Source: Bitkom Research 2022
## Survey design

<table>
<thead>
<tr>
<th>On behalf of</th>
<th>Bitkom e.V.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Methodology</strong></td>
<td>Computer-Assisted Telephone Interview (CATI)</td>
</tr>
<tr>
<td><strong>Statistical population</strong></td>
<td>Companies based in Germany having at least 10 staff members and an annual turnover of 1 million euros or more</td>
</tr>
<tr>
<td><strong>Selection procedure</strong></td>
<td>Variable sampling</td>
</tr>
<tr>
<td><strong>Audience</strong></td>
<td>Executives in charge of economic security. These include managers as well as executives from the fields of corporate security, IT security, risk management, law, finances, controlling, internal revision or compliance.</td>
</tr>
<tr>
<td><strong>Nominal sample size</strong></td>
<td>n=1.066</td>
</tr>
<tr>
<td><strong>Period of interviewing</strong></td>
<td>Between 10 January and 13 March 2022</td>
</tr>
<tr>
<td><strong>Weighting</strong></td>
<td>Variable sampling has ensured that companies from various sectors and size categories have been represented in numbers sufficient for statistical analyses. The statements of the interviewees have been weighted during analysis in a way that the results show a picture, considering sectors and size categories, representative for all companies based in Germany having at least ten staff members.</td>
</tr>
<tr>
<td><strong>Statistical fault tolerance</strong></td>
<td>+/- 3 percent</td>
</tr>
</tbody>
</table>
Contact

Bitkom e. V.
Albrechtstraße 10
10117 Berlin
T 030 27576-0

@Bitkom
bitkom@bitkom.org

bitkom.org

Simran Mann
Security Policy
Bitkom e.V.
s.mann@bitkom.org
T 030 27576-214

Andreas Streim
Press Spokesman
Bitkom e.V.
a.streim@bitkom.org
T 030 27576-112

Felix Lange
Research Consultant
Bitkom Research
f.lange@bitkom-research.de
T 030 27576-546