A Large-Scale Interview Study on Information Security in and Attacks against Small and Medium-sized Enterprises

Nicolas Huaman
CISPA Helmholtz Center for Information Security & Leibniz University Hannover

Bennet von Skarczinski
PwC Germany

Christian Stransky
Leibniz University Hannover

Yasemin Acar
Max Planck Institute for Security and Privacy & Leibniz University Hannover

Arne Dreißigacker
Criminological Research Institute of Lower Saxony

Dominik Wermke
CISPA Helmholtz Center for Information Security & Leibniz University Hannover

Sascha Fahl
CISPA Helmholtz Center for Information Security & Leibniz University Hannover
Cyber Attacks in Small- and Medium-sized Enterprises

- Cybercrime as a whole has been on the rise in recent years
- SMEs have become a major focus of these attacks
- Limited resources make them easier targets

Spike in Emotet activity could mean big payday for ransomware gangs

A big rise in Emotet attacks has provided hackers with more machines to offer up to cyber criminals for ransomware and other malware campaigns.

Germany logs rise in cybercrime as pandemic provides 'attack potential'

Germany's federal police documented a nearly 8% increase in cybercrime in 2020. Criminals especially took advantage of the coronavirus pandemic, selling fake vaccines and targeting people working from home.
Data about Cybercrime

Yearly reports concerning cybercrime exist

Focus:

- Cybercrime Measurement
- Security Recommendations
Research Questions

- We want to look at potential influences for the risk of attack.

Areas of focus:

- Company Security Perception
- Security Measures in SMEs
- Cyberattacks in Companies
- Correlations between these three Factors
Approach
Approach

- Conducted computer-assisted telephone interviews (CATI) with 5,000 SMEs in Germany

<table>
<thead>
<tr>
<th>Category</th>
<th>Selection Criteria</th>
<th>Sample Size</th>
<th>Percent</th>
<th>Dataset</th>
<th>Real World</th>
</tr>
</thead>
<tbody>
<tr>
<td>10–49 employees</td>
<td>Proportional to the selection population by company size and industry; Industry by WZ08-Classification A to S¹</td>
<td>1,000</td>
<td>23.8%</td>
<td>79.1%</td>
<td></td>
</tr>
<tr>
<td>50–99 employees</td>
<td></td>
<td>1,000</td>
<td>23.6%</td>
<td>10.5%</td>
<td></td>
</tr>
<tr>
<td>100–249 employees</td>
<td></td>
<td>1,000</td>
<td>22.4%</td>
<td>6.5%</td>
<td></td>
</tr>
<tr>
<td>250–499 employees</td>
<td></td>
<td>1,000</td>
<td>20.1%</td>
<td>2.2%</td>
<td></td>
</tr>
<tr>
<td>500+ employees</td>
<td></td>
<td>500+</td>
<td>10.1%</td>
<td>1.8%</td>
<td></td>
</tr>
<tr>
<td>Enterprises providing services of general interest [16]</td>
<td>Best Effort Base by industry; Selected industries (Subindustries of WZ08-D, E, H, J, K, L, O, P, Q)</td>
<td>500</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>5,000</td>
<td>100%</td>
<td>100%</td>
<td></td>
</tr>
</tbody>
</table>
## Interview Design

<table>
<thead>
<tr>
<th>1. Design Phase</th>
<th>2. Recruitment</th>
<th>3. Piloting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Literature review, six expert interviews and input from regional business advisory council.</td>
<td>Stratified random sampling (n=5000) by industry sector.</td>
<td>Discussions with twelve security experts and five pilots</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4. Training</th>
<th>5. Execution</th>
<th>6. Data Handling</th>
</tr>
</thead>
<tbody>
<tr>
<td>Training sessions with the 141 telephone interviewers</td>
<td>5000 computer assisted telephone interviews (CATI); August 2018 to February 2019</td>
<td>Quality checks &amp; anonymization by service provider; open coding &amp; evaluation by authors</td>
</tr>
</tbody>
</table>
Survey

Main areas:

- **Company Perception**
  - Risk Perception
  - Security Awareness

- **Security Measures**
  - Firewalls, Antivirus
  - Employee Training
  & more

- **Cybercrime Incidents**
  - Phishing, DDoS
  - Ransomware
  & more

- **Company Demographics**
  - Budget, Size
  - Tech-employees
  & more
Results
### Demographics

<table>
<thead>
<tr>
<th></th>
<th>Ratio</th>
<th>Companies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company Age &gt; 10 Years</td>
<td>83.8%</td>
<td>4,192</td>
</tr>
<tr>
<td>Export Activity</td>
<td>39.9%</td>
<td>1,997</td>
</tr>
<tr>
<td>Interviewee position</td>
<td></td>
<td></td>
</tr>
<tr>
<td>● Tech &amp; Information Security</td>
<td>69.7%</td>
<td>3,484</td>
</tr>
<tr>
<td>● Management</td>
<td>23.4%</td>
<td>1,171</td>
</tr>
<tr>
<td>● More in paper...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT-Department Inhouse</td>
<td>85.2%</td>
<td>4,262</td>
</tr>
<tr>
<td>Information Security Staff Inhouse</td>
<td>73.6%</td>
<td>3,682</td>
</tr>
</tbody>
</table>
To find correlations within the data, we conducted regressions.

General findings:

- Interviewee position bias
- Self reporting of incident counts likely of low quality
Company Security Awareness

Ratings:

- High self-reported security awareness
- Low estimation of attack risk
- Especially low risk of targeted attacks

➔ Misconceptions?
Security Measurements

Basic technical measures are available in all companies

Limited distribution:

- Certification & Training
- Risk Analysis
- Emergency Drills

→ Risk awareness and estimation is low
Cybercrime Incidence

Takeaways:

- Most common successful attack (within 12 months before the interview): Phishing
- Some industry sectors correlate with certain attack vectors
- Companies with higher coverage of measures also report higher incidence!
- More in the Paper...
Recommendations
Recommendations

● For Companies:
  ○ Investigate discrepancy between employee and management security awareness.
  ○ More in paper...
Recommendations

● For Legislators:
  ○ Industry sectors with higher legislative security requirements tend to report lower incidences.
  ➔ Security policies are important to control direction of company security
  ➔ More in paper...
Future Work

- Misconceptions in risk awareness and how to approach security should be investigated.

- In-depth investigation of the correlations we found regarding security measures and incidence reporting.

- Future work needs to consider: The interviewee position had a significant influence on almost all areas!
Key Takeaway

- Information Security has arrived in companies!
  - Security in practice might be flawed however
  - Factor “Human” is still not appropriately considered!
Conclusion

Interviewed 5000 company representatives:

- Created an overview of cybercrime effects in Germany
- Found interesting tendencies to follow
- Found a few important indicators for self-reporting quality (e.g. interviewee position)

Nicolas Huaman huaman@sec.uni-hannover.de | Bennet von Skarczinski bennet.simon.von.skarczinski@pwc.com | Christian Stransky stransky@sec.uni-hannover.de | Dominik Wermke wermke@sec.uni-hannover.de | Yasemin Acar yasemin.acar@mpi-sp.org | Arne Dreißigacker arne.dreissigacker@kfn.de | Sascha Fahl sascha.fahl@cispa.de