



## Risk analysis and simulation

The increasing complexity of our networked world also leads to an increase in risks. For suitable countermeasures to be initiated, these risks need to be identified and analyzed. We offer a number of procedures for this, including:

- Risk-threat analyses
- Protection requirements analyses
- Impact analyses
- Security scans

If a concrete incident does occur despite all the measures in place to protect against it, an immediate analysis of this situation is extremely important. The results must then be documented accurately and in a tamper-proof way. However, it is often difficult for internal employees to find the resources needed to do this, as their efforts are primarily focused on restoring smooth operation.

As external specialists, we are on hand immediately to investigate the incident thoroughly. The scope of the incident and its effects must be clarified, along with possible motives. It is extremely important to find out whether the attack was directed at the company specifically, or whether it was random.

The aim of both simulation and forensics is to optimize security measures in order to protect business processes effectively from internal and external threats.

While a simulation deals with possible disruption scenarios, forensics is concerned with identifying and logging traces in the event of actual incidents and attacks. Appropriate evaluation tools should be installed in advance for both.