Info Blatt

Information sheets on economic security

Protection against sabotage

Sabotage is a serious threat to many aspects of life – politics and administration, public life, but also companies and research institutions can be affected. State actors from other countries, but also extremists target institutions and facilities in order to cause damage. German companies and research institutions can protect themselves against this threat by taking security measures.

BfV and the domestic intelligence services of the federal states are in charge of countering espionage and sabotage activities carried out by foreign intelligence services as well as of countering extremism and will be at your disposal for confidential consultation.

1 Definition and aims of sabotage

- Sabotage in the field of economy and science refers to deliberate and targeted **interference** with production processes and/or **damage** on or **destruction** of facilities and institutions.
- Sabotage may be committed from the outside as **physical acts of sabotage and cyber attacks** or from the inside by ***inside agents***.
- Especially foreign intelligence services but also extremist forces are capable of **planning and staging combined and concerted acts of sabotage in the long-term**. These acts can be part of ***hybrid threats*** used against Germany by a foreign state.

Inside agents

Inside agents are, for example, employees who carry out damaging acts from the inside. Since inside agents usually have extensive internal knowledge and access possibilities, attackers can use them for acts of sabotage like IT manipulations or physical damage.

*Please also visit our website and note the flyer "Methods of Insider Threat" at **www.verfassungsschutz.de** (Service > Publications).*

AIMS OF SABOTAGE

Foreign state actors and extremist forces try to pursue their aims by way of sabotage.

- Interfering with critical infrastructures, for example the Internet or the supply of energy, fuel or water
- Influencing the opinion of the public and of policy makers
- Impairing work procedures and communications in politics and administration
- Inciting political groups
- Interfering with work processes of other businesses

Hybrid threats

German companies and research institutions can become victims of hybrid threats. Hybrid threats refer to numerous methods used on purpose to weaken an opposing state and to unsettle its society. The acts can be directed against the social cohesion, infrastructures, public goods or services, for example by means of:

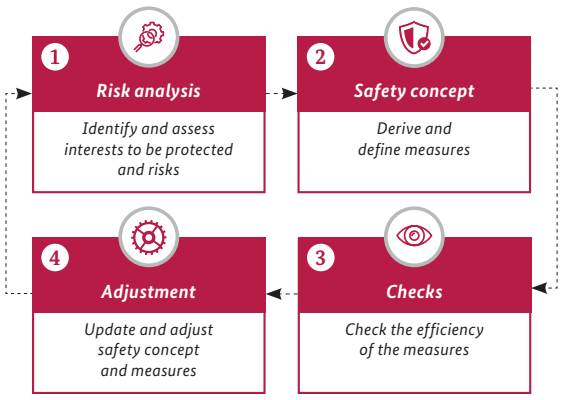
- *cyber attacks*
- *influence on elections*
- *disinformation campaigns*
- *sabotage*

2 Protection against sabotage

Protection against sabotage includes the IT as well as physical, personnel, procedural and organisational aspects. These can differ widely between specific sectors. **Preventive protection of information** and **efficient communication in case of emergency** are helpful in any case.

Attackers also use openly accessible information to prepare acts of sabotage.

- Check **publications** like presentations, guidelines, survey maps etc. **for sensitive data**.
- If possible, publish **information** only within the scope of **the statutory obligations**.
- For the sharing of information, set up a **Two-Factor-Authentication** area or use **email distribution lists**.
- Handle **contact details restrictively**. Individual email signatures might e.g. be misused for spear phishing mails.
- **Suppliers** can also be a **gateway** for acts of sabotage (supply chain attack). If necessary, prohibit **naming** your company **as a reference**.



Protection against sabotage as part of a comprehensive safety concept

CYBER SABOTAGE

Cyber sabotage refers to the deliberate damaging of IT infrastructures and data.

- *Port scans provide clues about unsecured services that might be used to introduce e.g. data-deleting wiper malware.*
- *Pre-positioning refers to attackers intruding an IT system but keeping a low profile until committing the act of sabotage.*
- *Keep your software up to date. Carry out port scans and limit the access to services on the Internet.*

Communication is one of the vital key factors in a case of emergency.

- Define appropriate forms of communication in a communication concept: Who communicates with whom, when, and how?
- Identify **responsible (security) authorities and service providers**.
- Make sure that all necessary contact data and information is known and available – also in case of an IT system breakdown.
- Make **contacts that are relevant in terms of security** and establish a continuous exchange of information.
- Enable the **employees** to respond to crisis situations in a **competent and active** way.

Wirtschaft & Wissenschaft. Zukunftssicher.
Verfassungsschutzverbund des Bundes und der Länder

*BfV (Bundesamt für Verfassungsschutz) and the 16 domestic intelligence services of the federal states are the domestic intelligence community. They cooperate closely in the field of preventive economic security. Thus a strong network is formed that extends to where your company is based. Please visit **www.verfassungsschutz.de** to find a list of contacts at the federal state authorities.*

initiative wirtschaftsschutz
Gemeinsam. Werte. Schützen.

*The Economic Security Initiative (Initiative Wirtschafts-schutz) is an initiative by BfV, BKA, BND and BSI. On their information platform **www.wirtschaftsschutz.info** they offer their expertise in the field of economic security together with various partners. This includes the issue of cyber crime as well as economic and scientific espionage or IT security.*

Your direct contact to economic security

Ministerium des Innern und für Sport Rheinland-Pfalz
Wirtschaftsschutz
Schillerplatz 3-5
55116 Mainz
Tel.: 06131/16-3773
Email: wirtschaftsschutz@mdi.rlp.de