Bundesamt für Verfassungsschutz

Info Blatt

Informationsblätter zum Wirtschaftsschutz

Schutz vor Sabotage

Sabotage stellt für viele Lebensbereiche eine ernst zu nehmende Gefahr dar – Politik und Verwaltung, das öffentliche Leben, aber auch Unternehmen und Forschungseinrichtungen können betroffen sein. Staatliche Akteure aus dem Ausland, aber auch Extremisten nehmen Einrichtungen und Anlagen ins Visier, um diese zu schädigen. Deutsche Unternehmen und Forschungseinrichtungen können sich mit Sicherheitsmaßnahmen vor diesen Gefahren schützen.

Der Verfassungsschutz ist für die Abwehr von Spionage und Sabotage durch ausländische Nachrichtendienste sowie von Extremismus zuständig und steht als vertraulicher Ansprechpartner zur Verfügung.

1 Definition und Ziele von Sabotage

- Unter Sabotage im wirtschaftlichen und wissenschaftlichen Bereich versteht man die absichtliche und zielgerichtete **Beeinträchtigung** von Produktionsabläufen bzw. **Beschädigung oder Zerstörung** von Anlagen und Einrichtungen.
- Sabotage kann dabei von außen durch **physische Sabotagehandlungen und Cyberangriffe** erfolgen oder von innen durch sogenannte ***Innentäter***.
- Insbesondere ausländische Nachrichtendienste, aber auch extremistische Kräfte sind zu **kombinierten und abgestimmten** Sabotagehandlungen in der Lage und können diese **langfristig planen und durchführen**. Diese Handlungen können Teil ***hybrider Bedrohungen*** sein, die ein fremder Staat gegen Deutschland einsetzt.

Innentäter
Bei Innentätern handelt es sich z. B. um Beschäftigte, die von innen heraus schädigende Handlungen ausführen. Da Innentäter zumeist über tiefgehende interne Kenntnisse und Zugangsmöglichkeiten verfügen, können diese von Angreifern für Sabotagehandlungen wie IT-Manipulationen oder physische Beschädigungen genutzt werden.

*Beachten Sie auch das Informationsblatt „Bedrohung durch Innentäter“ auf **www.verfassungsschutz.de** (Service > Publikationen).*

ZIELE VON SABOTAGE

Ausländische staatliche Akteure und extremistische Kräfte versuchen mittels Sabotage ihre Ziele zu verfolgen.

- Störung kritischer Infrastrukturen, wie z. B. Internet, Energie-, Treibstoff-, Wasserversorgung
- Beeinflussung der Stimmung der Bevölkerung und politisch Verantwortlicher
- Behinderung von Arbeitsabläufen und Kommunikation in Politik und Verwaltung
- Aufstachelung politischer Gruppierungen
- Störung der Betriebsabläufe sonstiger Wirtschaftsunternehmen

Hybride Bedrohungen
Deutsche Unternehmen und Forschungseinrichtungen können Opfer hybrider Bedrohungen werden. Letztere beschreiben eine Vielzahl von Methoden, die gezielt eingesetzt werden, um einen gegnerischen Staat zu schwächen und dessen Gesellschaft zu verunsichern. Die Handlungen können sich gegen den gesellschaftlichen Zusammenhalt, Infrastrukturen, öffentliche Güter oder Dienstleistungen richten, z. B. mittels:

- *Cyberangriffen*
- *Einflussnahme auf Wahlen*
- *Desinformationskampagnen*
- *Sabotage*

2 Schutz vor Sabotage

Der Schutz vor Sabotage umfasst informationstechnische, physische, personelle, prozessuale und organisatorische Aspekte. Diese können sich von Branche zu Branche stark unterscheiden. In jedem Fall hilfreich sind ein **präventiver Informationsschutz** und eine **effiziente Kommunikation im Ernstfall**.

Angreifende nutzen zur Sabotagevorbereitung auch öffentlich zugängliche Informationen.

- Prüfen Sie **Veröffentlichungen** wie Präsentationen, Leitfäden, Übersichtskarten etc. **auf sensible Daten**.
- Veröffentlichen Sie ggf. nur **Informationen** im Rahmen der **gesetzlichen Pflicht**.
- Richten Sie für die Weitergabe von Informationen einen durch **Zwei-Faktor-Authentifizierung** geschützten Bereich ein oder nutzen Sie für eine gezielte Adressierung **E-Mail-Verteiler**.
- Gehen Sie **restriktiv mit detaillierten Kontaktinformationen** um. Persönliche E-Mail-Signaturen können z. B. für Spear-Phishing-Mails missbraucht werden.
- Auch **zuliefernde Unternehmen** können ein **Einfallstor** für Sabotagehandlungen darstellen (Supply-Chain-Angriff). Untersagen Sie ggf. die **Nennung** Ihres Unternehmens **als Referenz**.

Sabotageschutz als Teil eines ganzheitlichen Schutzkonzepts

CYBERSABOTAGE

Cybersabotage beschreibt das absichtliche Schädigen von IT-Infrastrukturen und Daten.

- *Portscans geben Hinweise zu ungesicherten Services, die genutzt werden können, um z. B. datenlöschende Wiper-Malware einzuschleusen.*
- *Beim „Pre-Positioning" dringen Angreifende in ein IT-System ein, verhalten sich jedoch bis zur Sabotagehandlung unauffällig.*
- *Halten Sie Software immer aktuell. Führen Sie Port-Scans durch und beschränken Sie die Erreichbarkeit von Diensten im Internet.*

Kommunikation ist einer der maßgeblichen Schlüsselfaktoren im Ernstfall.

- Legen Sie **geeignete Kommunikationsformen** in einem **Kommunikationskonzept** fest: Wie muss wann mit wem kommuniziert werden?
- Identifizieren Sie **zuständige (Sicherheits-)Behörden und Dienstleistungsunternehmen**.
- Stellen Sie sicher, dass alle **notwendigen Kontaktdaten und Informationen** bekannt und vorhanden sind – auch bei einem Ausfall der IT-Systeme.
- Knüpfen Sie **sicherheitsrelevante Kontakte** und etablieren Sie einen kontinuierlichen **Informationsaustausch**.
- Befähigen Sie die **Beschäftigten**, in Krisensituationen **kompetent und aktiv** zu handeln.

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

*Das Bundesamt für Verfassungsschutz und die 16 Landesbehörden für Verfassungsschutz bilden gemeinsam den Verfassungsschutzverbund. Auch im Bereich des präventiven Wirtschaftsschutzes arbeitet dieser eng zusammen. Auf diese Weise entsteht ein starkes Netzwerk bis zu Ihnen vor Ort. Eine Übersicht über die Ansprechbarkeiten in den Landesbehörden finden Sie unter **www.verfassungsschutz.de**.*

initiative wirtschaftsschutz
Gemeinsam. Werte. Schützen.

*Die Initiative Wirtschaftsschutz ist ein Zusammenschluss von BfV, BKA, BND und BSI. Auf der Informationsplattform **www.wirtschaftsschutz.info** stellen sie zusammen mit verschiedenen Partnerverbänden ihre Expertise im Bereich Wirtschaftsschutz zur Verfügung. Dazu gehört das Thema Cyberkriminalität genauso wie Wirtschafts- und Wissenschaftsspionage oder das Thema IT-Sicherheit.*

Ihr direkter Kontakt zum Wirtschaftsschutz

SCAN ME

Bundesamt für Verfassungsschutz
Bereich Prävention (Wirtschafts- und Wissenschaftsschutz)
030 18792-3322
wirtschaftsschutz@bfv.bund.de

Scannen Sie den QR-Code und gelangen Sie direkt zu allen bisher erschienenen Infoblättern.