Bundesamt für Verfassungsschutz

Info Blatt

Informationsblätter zum Wirtschaftsschutz

Bedrohung durch Innentäter

Unternehmen und Forschungseinrichtungen besitzen Know-how und Informationen, an denen auch Dritte interessiert sind. Mit verschiedenen Mitteln versuchen sie, sich dieses Wissen anzueignen. Dabei spielen neben Cyberangriffen auch Innentäter eine wichtige Rolle. Diese Gefahr können Sie jedoch durch die folgenden Informationen und Empfehlungen reduzieren.

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 Was sind Innentäter und warum sind sie so gefährlich?

Definition

- Innentäter sind Personen, die in Unternehmen, in Forschungseinrichtungen oder anderen Organisationen **Informationen entwenden**, unautorisiert **weitergeben** oder andere **schädigende Handlungen** ausführen.
- Beschäftigte können auch **unbewusst zu Innentätern** werden, z. B. wenn sie durch Social Engineering manipuliert wurden.
- **Ausländische Nachrichtendienste** nutzen Innentäter, da diese über tiefe, interne Einblicke und über kritische Zugangsmöglichkeiten verfügen.
- Mittels einer sogenannten ***HUMINT-Spionageaktion*** werden Beschäftigte **ausgeforscht oder** für eine Zusammenarbeit **angeworben**.

MÖGLICHE ANGRIFFSVEKTOREN

Die Gefahr von Innentäterhandeln droht aus verschiedenen Richtungen. Es ist nicht nur das Stammpersonal betroffen: Auch Personen, die nur vorübergehend Zugriff auf Firmeninterna haben, können Innentäter sein.

- aktuelle und ehemalige Beschäftigte
- geschäftliche Kontakte wie Kundinnen und Kunden oder Lieferunternehmen
- externe Dienstleistungen (Beratung, IT-Service, Personal, Reinigung etc.)

HUMINT-Spionageaktion

HUMINT beschreibt die Gewinnung von Informationen mittels menschlicher Quellen. Ausländische Nachrichtendienste können dabei auf umfangreiche Ressourcen und Know-how zurückgreifen.

Beachten Sie auch das Informationsblatt „Methoden der Spionage: HUMINT“ auf www.verfassungsschutz.de (Service > Publikationen).

Beispiel-Situationen

- Eine Sachbearbeiterin in der Abrechnung wird Opfer eines Social Engineering-Angriffs und öffnet eine maliziöse Datei.
- Die Bürokraft eines Patentanwalts liefert vertrauliche Unterlagen an einen fremden Nachrichtendienst.
- Ein Gastwissenschaftler wird durch den Nachrichtendienst des Heimatlandes unter Druck gesetzt und entwendet daraufhin Forschungsdaten.
- Der Angestellte eines Klinikums ruft personenbezogene Daten ab und leitet diese an die extremistische Szene weiter.

2 Warum werden Menschen zu Innentätern?

Beschäftigte können aus verschiedenen Gründen zu Innentätern werden. Es lassen sich persönliche, aber auch arbeitsplatzbezogene Ursachen identifizieren.

- Streben nach Anerkennung, Respekt oder Freundschaft
- politische, kulturelle oder religiöse Überzeugungen
- Druckaufbau durch Externe (Erpressung, z. B. durch ausländische Nachrichtendienste)
- Unzufriedenheit am Arbeitsplatz und fehlende Identifikation mit dem Unternehmen / der Institution
- finanzielle Probleme oder auch Angst vor Arbeitsplatzverlust

TATGELEGENHEITEN

Neben der Motivation müssen sich aber auch entsprechende Tatgelegenheiten bieten.

- *unzureichende interne Kontrollen*
- *fehlende Schulungen am Produkt*
- *Unkenntnis über Arbeitsprozesse*
- *Einsatz privater Geräte im geschäftlichen Kontext*
- *allgemein unzureichende Sicherheitskultur*

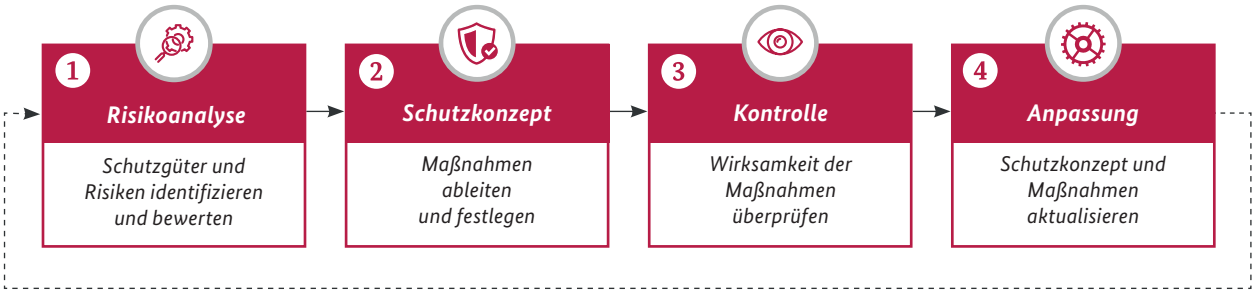
HOMEOFFICE

Die Arbeit im Homeoffice ist für die Unternehmenssicherheit eine besondere Herausforderung.

- *Die verwendete IT kann eine spezielle Angriffsfläche darstellen und z. B. bei einer unsachgemäßen Handhabung zu einem Schadensfall führen (unbewusste Innentäterschaft).*
- *Darüber hinaus kann sich Homeoffice auf die Bereitschaft, auf illegitime Ansprachen durch Dritte einzugehen und Folgeaktivitäten von Beschäftigten auswirken, soweit die Unternehmensbindung nicht durch entsprechende Maßnahmen kompensiert wird.*

3 So können Sie sich schützen.

Generell gilt:
Sicherheit muss Chefsache sein und in eine positive Sicherheitskultur eingebettet sein. Der Schutz vor Innentäterschaft muss dabei im Rahmen eines Schutzkonzeptes ganzheitlich angegangen werden.



- **Die Etablierung eines Schutzkonzepts ist ein fortlaufender Prozess.**

1 *Risikoanalyse*

Identifizieren Sie unter Einbeziehung der Beschäftigten die wesentlichen Schutzgüter über alle Bereiche hinweg.

LEITFRAGEN

- Welches sind die schützenswerten Güter?
- Wer könnte Interesse an diesen haben?
- Welche Bereiche, Funktionen oder Stellen sind besonders sicherheitssensibel?
- Wie könnten Angreifer an diese gelangen?
- Welche Regeln zum Umgang mit unternehmensinternen Informationen gibt es und sind diese bekannt?
- Wie stark ist die Loyalität der Beschäftigten ausgeprägt?

- *Beachten Sie auch die Broschüre „Informationsabfluss aus Unternehmen – Innentäterschaft als unterschätztes Massenphänomen“ auf **www.wirtschaftsschutz.info**.*

3 So können Sie sich schützen.

2 Schutzkonzept

Leiten Sie aus der Risikoanalyse passende Schutzmaßnahmen ab und halten Sie diese in einem Schutzkonzept fest. Berücksichtigen Sie dabei neben der IT-Sicherheit auch die physische und personelle Sicherheit.

INFORMATIONSSICHERHEIT

- Benennen Sie eine **sicherheitsverantwortliche Person**.
- Erfassen Sie systematisch die **schützenswerten Informationen** und klassifizieren sie diese.
- Bauen Sie ein **robustes IT-Sicherheitsmanagement** auf und pflegen Sie dieses.
- **Beschränken Sie den Informationszugriff** nach den Prinzipien Need-to-Know, Need-to-See und Need-to-Go.
- Berücksichtigen Sie den Informationsschutz auch bei **externen Geschäftsbeziehungen**.

SICHERHEITSKULTUR

- Sorgen Sie für ein **angenehmes Arbeitsklima** und schaffen Sie eine **positive Fehlerkultur**.
- Sensibilisieren und trainieren Sie die Beschäftigten zu **Spionage und Know-how-Abfluss**.
- Bieten Sie die Möglichkeit zur **anonymen Meldung** von Missständen und Vorfällen.
- Unterstützen Sie Beschäftigte in **Notlagen und persönlichen Krisen**.

PERSONAL

- Etablieren Sie eine **sicherheitsorientierte Personalauswahl** (→ Infoblatt „Pre-Employment Screening“).
- Managen Sie den **Austritt von Beschäftigten**.
- Detektieren Sie → ***kritische Verhaltensindikatoren*** von Beschäftigten.
- Führen Sie **interne Ermittlungen** konsequent durch und verhängen Sie ggf. Strafmaßnahmen.

> → ***Kritische Verhaltensindikatoren***
>
> *Bestimmte Verhaltensweisen können Anzeichen für eine Innentäterschaft sein.*
>
> - *ungewöhnliches Interesse an Informationen außerhalb der eigenen Zuständigkeit*
> - *Versuch der Erweiterung oder Überschreitung der Zugriffsberechtigungen*
> - *verdächtige Kontakte zu Staaten oder Konkurrenzunternehmen*
> - *regelwidriges Einbringen und Nutzen mobiler Endgeräte und Datenträger*

3 4 Kontrolle und Anpassung

Prüfen Sie das Schutzkonzept und die ergriffenen Maßnahmen systematisch und regelmäßig auf deren Wirksamkeit und passen Sie das Schutzkonzept ggf. an.

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