Publikationen

Informationsblätter zum Wirtschaftsschutz

*Die **Informationsblätter zum Wirtschaftsschutz** („Infoblatt“) werden vom Bundesamt für Verfassungsschutz herausgegeben.*
*Sie bieten zu verschiedenen Themen Informationen und Hilfestellungen und können über **www.verfassungsschutz.de** kostenlos bezogen werden.*

Bisher erschienene Themen:

Sicherheit auf Geschäftsreisen

Die Checkliste gibt Ihnen Hinweise, wie Sie sich vor, auf und nach einer geschäftlichen Auslandsreise vor Spionageaktivitäten schützen können.

Pre-Employment Screening

Mittels Pre-Employment Screening als Teil einer sicherheitsorientierten Personalauswahl tragen Sie dazu bei, sensible Daten und Informationen zu schützen.

Sicherheit auf Geschäftsreisen: China

In diesem Infoblatt finden Sie spezifische Verhaltenshinweise für Ihre Geschäftsreise nach China.

Bedrohung durch Innentäter

Dieses Infoblatt bietet Ihnen Informationen über Motivation und die Gefahr von Innentätern und gibt Hinweise zur Etablierung eines Schutzkonzepts.

Schutz vor Phishing

Was sich hinter der Angriffsmethode Phishing verbirgt und wie Sie sich davor schützen, können Sie in diesem Infoblatt nachlesen.

Spionage in Wissenschaft und Forschung

Das Infoblatt beschreibt Ziele und Folgen von Wissenschaftsspionage und gibt Anregungen und Tipps zum Umgang mit Bedrohungen.

Methoden der Spionage: HUMINT

Hier erhalten Sie einen Einblick, wie ausländische Nachrichtendienste spionieren und was Sie selbst dagegen tun können.

Schutz vor Sabotage

Sabotageschutz umfasst verschiedene Sicherheitsaspekte. Dieses Infoblatt gibt Hinweise zum präventiven Informationsschutz und zur Kommunikation im Ernstfall.

Schutz vor Social Engineering –
Hinweise für Leitungsebene und Sicherheitsverantwortliche

Hier finden Sie Informationen, wie ein Social-Engineering-Angriff abläuft und wie Sie Ihr Unternehmen und Ihre Beschäftigten vor Manipulation schützen können.

Schutz vor Social Engineering –
Hinweise für Beschäftigte

In diesem Infoblatt erfahren Sie, wie Sie sich als Beschäftigte im Umgang mit Social-Media, E-Mail und Co. gegen Social-Engineering-Angriffe wappnen können.

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

SCAN ME
Direkt zu den Infoblättern

Informationsblätter zum Wirtschaftsschutz

Schutz vor Desinformation

Fremde Staaten nutzen Desinformation auch, um ihre wirtschaftspolitischen Interessen durchzusetzen. Im sich zunehmend verstärkenden Kampf um Meinungshoheit setzen diese Staaten neben offenen Mitteln überdies ihre Nachrichtendienste ein. Unternehmen und Forschungseinrichtungen können sich mit geeigneten Maßnahmen vor dieser Form der illegitimen Einflussnahme schützen.

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

1 Was ist Desinformation und wie wirkt sie?

- Bei Desinformation handelt es sich um das
  - **bewusste und zielgerichtete** Verbreiten
  - **falscher oder irreführender** Informationen
  - bzw. wenn **wesentliche Teile** einer Information **verschwiegen** werden.
- Angreifer nutzen für die Verbreitung von Desinformation den **gesamten Informationsraum**, also alle digitalen und analogen Kanäle, Medien und Formate.
- Auch **Unternehmen, Forschungseinrichtungen oder herausgehobene Einzelpersonen** können das Ziel von Desinformationsangriffen werden.

Mehr zum Thema Desinformation erfahren Sie auf:
www.euvsdisinfo.eu
www.verfassungsschutz.de
www.bpb.de

ZIELE VON DESINFORMATION

Akteure, die Desinformationen verbreiten, wollen

- *die Öffentlichkeit verunsichern*
- *die öffentliche Meinungsbildung beeinflussen*
- *eigene Aktivitäten verschleiern bzw. davon ablenken*
- *kontroverse Debatten emotionalisieren*
- *gesellschaftliche Spannungen verstärken*
- *Misstrauen in staatliche Institutionen und Regierungshandeln schüren*

*Bei einer **Desinformationskampagne** erfolgen Aktionen über einen längeren Zeitraum, wobei sowohl offene als auch verdeckte Mittel genutzt werden. Sie folgt einem definierten strategischen Ziel und soll eine breite Wirkung beim Empfängerkreis entfalten. Urheber sind zumeist staatliche oder staatsnahe Akteure, die geplant und koordiniert zusammenwirken.*

DESINFORMATION IN BEZUG AUF UNTERNEHMEN UND FORSCHUNGSEINRICHTUNGEN

Auch Unternehmen und Forschungseinrichtungen können in Deutschland, aber auch im Ausland, in das Visier staatlich gesteuerter Desinformation geraten.

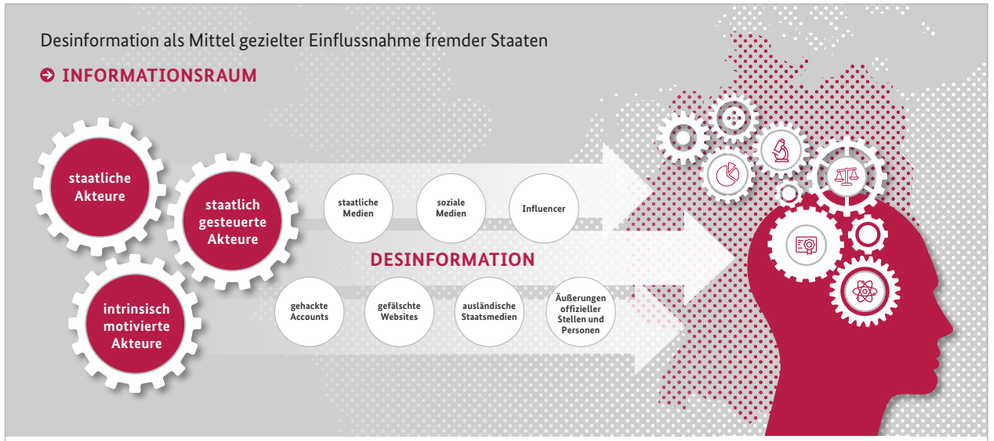
- Schädigung der Reputation als Arbeitgeber
- Abwertung von Produktqualität und Produktsicherheit (z. B. Impfstoffe)
- Verunsicherung in Bezug auf Verlässlichkeit und Unternehmenscompliance
- Diskreditierung einzelner Beschäftigter oder exponierter Schlüssel- und Führungspersonen

Desinformation in einem unternehmerischen Kontext beeinflusst verschiedene Stakeholder: Beschäftigte, sich bewerbende Personen, Kunden und Kundinnen, Analysten, geschäftliche Kontakte. Die öffentliche Meinung, politische Entscheidungen und unternehmerisches Handeln haben wechselseitig aufeinander Einfluss. Desinformation kann hier Kommunikation und Entscheidungen der Handelnden erheblich erschweren.

Info Blatt

2 Wie Desinformationen verbreitet werden.

Die Urheber von Desinformation sind **staatliche**, **staatlich gesteuerte** oder **aus sich heraus motivierte Akteure**. Diese nutzen die Gesamtheit aller ihnen zur Verfügung stehenden **Kommunikationsmittel**, um ihre Desinformation im **Informationsraum** zu verbreiten.



VERBREITUNG VON DESINFORMATION

- **Ausländische staatliche Akteure** nutzen z. B. **offizielle Verlautbarungen, Veröffentlichungen von Staatsmedien oder Einzelbeiträge von Personen** in sozialen Medien, um ihre Desinformation zu verbreiten.
- **Staatlich gesteuerte Akteure**, wie z. B. Nachrichtendienste, greifen diese auf und streuen sie **über ihre eigenen Kanäle** weiter.
- **Soziale Medien** haben eine **besondere Funktion** als Kanäle und Multiplikatoren von Desinformation, da hier schnell und ressourcenarm **viel Aufmerksamkeit** erzeugt werden kann.
- Auch werden zunehmend z. B. **Influencerinnen und Influencer** zur Desinformation eingebunden.
- Akteure nutzen **verschiedene Angriffsvektoren** und **verschränken** diese auch miteinander (HACK AND LEAK / HACK AND PUBLISH).

HACK AND LEAK / HACK AND PUBLISH

Angreifer nutzen verschiedenste Methoden, um Desinformationen zu verbreiten.

Hack and Leak

- *Gezieltes Hacken von Konten in sozialen Medien, legitimen Nachrichtenportalen oder auch Blogs*
- *Ziel: **Erbeutung** von Informationen, um diese – entweder im Original oder verfälscht – zu einem späteren Zeitpunkt zu veröffentlichen*

Hack and Publish

- *Kompromittierung von legitimen Nachrichtenportalen oder Social-Media-Konten sowie Blogs*
- *Ziel: **Verbreitung** von Informationen, manipulierten Inhalten oder anderen Informationen zum Zwecke der Desinformation*

Beispiel-Situationen

- *Ein ranghoher ausländischer Regierungsvertreter beschuldigt ein deutsches Forschungsinstitut, Teil eines geheimen Biowaffenprogramms zu sein. Dabei werden auch – vermutlich gestohlene – interne Dokumente als Beweise herangezogen. Die Anschuldigungen und vermeintlichen Beweise sind haltlos, verbreiten sich jedoch schnell insbesondere in den sozialen Medien.*
- *Über ausländische staatlich gelenkte Medien werden mittels irreführender Forschungsdaten die Wirksamkeit und Sicherheit eines deutschen Impfstoffs infrage gestellt. Auch verschiedene (bezahlte) Influencer berichten. Gleichzeitig wird der eigene Impfstoff beworben, dessen Wirksamkeit jedoch deutlich hinter der des Konkurrenzprodukts zurückliegt.*

3 Wie Sie mit Desinformation umgehen können.

Der Schutz vor Desinformation muss neben anderen Aspekten, wie z. B. Cyber- oder Objektschutz, Teil eines ganzheitlichen Schutzkonzepts sein.

ALLGEMEINE HINWEISE

- Versuchen Sie, **Problemlagen** möglichst frühzeitig zu **erkennen** („Digital Listening“).
- **Bewerten** Sie Bedrohungen nach einem → ***definierten Entscheidungsprozess***.
- Nutzen Sie eine **abgestufte Abwehrreaktion** (Ignorieren > Klarstellung > ***WIDERLEGUNG*** / Anzeige).
- **Warnen** Sie ggf. vor möglichen Falschinformationen und erklären Sie **zugrundeliegende Muster** („Prebunking“).
- Reagieren Sie **schnell** und **kommunizieren** Sie dort, wo der **Angriff stattfand**.
- Passen Sie die **Botschaft an das Zielpublikum** an und nutzen Sie einen **vertrauensvollen Überbringer**.
- Nutzen Sie möglichst Visualisierungen sowie eine **leichte, verständliche Sprache**.
- Verzichten Sie nicht darauf, **Desinformationen zu widerlegen** aus Sorge, diese weiter zu stärken.

→ ***Definierter Entscheidungsprozess***

Interne Abläufe und Zuständigkeiten müssen vorab geklärt sein. Leitfragen für eine Reaktion:

- *Was ist der Fall und wer oder was ist betroffen?*
- *Was ist der Ursprung der Desinformation und wo wurde sie veröffentlicht?*
- *Wie hoch ist das Bedrohungspotential?*

WIDERLEGUNG („DEBUNKING“)

1 *Fakt*

- *Stellen Sie den Fakt an den Anfang – einfach, knapp und einprägsam.*
- *Bieten Sie eine faktengestützte Alternative und schließen sie eine kausale „Lücke“ der Desinformation.*

2 *Irrglaube*

- *Warnen Sie vor der nachfolgenden Desinformation („Ein häufig gehörter Irrglauben ist…“).*
- *Erwähnen Sie einmal vor der Richtigstellung die Desinformation.*

3 *Trugschluss*

- *Erklären Sie, was an der Desinformation falsch ist und zeigen Sie logische Brüche auf.*
- *Nutzen Sie z. B. eine passende Analogie („Das wäre genauso, als ob…“).*

4 *Fakt*

- *Bestätigen Sie zum Schluss den Fakt erneut, ggf. mehrfach.*

GEFAHR

Neue Technologien, wie z. B. Künstliche Intelligenz, Foto-, Voice- oder Video-Deepfakes, erweitern die Möglichkeiten für Desinformationen. Bleiben Sie daher immer auf dem aktuellen technologischen Stand.

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

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

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

*Infoblatt **Schutz vor Desinformation**, Februar 2023*