Beratungsangebot

Der Niedersächsische Verfassungsschutz ist permanent mit Spionagesachverhalten aus der Wirtschaft konfrontiert.

Nehmen Sie das Angebot des Niedersächsischen Verfassungsschutz wahr und sensibilisieren Entscheidungsträger und Mitarbeiter für den Know-how-Schutz.

Wirtschaftsspionage ist Realität!

Ihre Ansprechpartner

Fachbereich Wirtschaftsschutz:

Herr Böger	0511/6709-284
Frau Flemming	0511/6709-247
Herr Peine-Paulsen	0511/6709-244
Herr Schomburg	0511/6709-245

E-Mail: wirtschaftsschutz@
mi.niedersachsen.de

Prävention

Neben diesen Angeboten stellt der Niedersächsische Verfassungsschutz Broschüren und andere Informationsmaterialien zum Extremismus bereit, die Sie bei uns anfordern können.

Bei Wünschen zu Vortrags- und Informationsveranstaltungen sowie inhaltlichen Fragen zum Thema Extremismus erreichen Sie den Verfassungsschutz unter folgenden Kontaktdaten:

Telefon: 0511/6709-215
Telefax: 0511/6709-394
E-Mail: praevention@
mi.niedersachsen.de
www.verfassungsschutz.niedersachsen.de

Niedersächsisches Ministerium
für Inneres und Sport
– Verfassungsschutz –

Wirtschaftsschutz

Information – Prävention – Hilfe
gegen Wirtschaftsspionage

Herausgeber:
Niedersächsisches Ministerium
für Inneres und Sport
Abteilung Verfassungsschutz
Presse- und Öffentlichkeitsarbeit
Büttnerstraße 28, 30165 Hannover
Telefon: 0511 6709-217
Telefax: 0511 6709-394
E-Mail: oeffentlichkeitsarbeit@mi.niedersachsen.de
Internet: www.verfassungsschutz.niedersachsen.de
Facebook: https://www.facebook.com/
Verfassungsschutz.Niedersachsen
Instagram: https://instagram.com/verfassungsschutz.nds
Twitter: https://twitter.com/LfV_NI

Informationen zum
Thema Wirtschaftsschutz
in Niedersachsen

Niedersachsen

Was ist Wirtschaftsspionage?

Die Begriffe Wirtschaftsspionage und Konkurrenzausspähung (Industriespionage) werden häufig undifferenziert bzw. uniform genutzt. Allerdings ist diese Vereinheitlichung nur bei der Betrachtung der Angriffsstrategien und Ziele korrekt. Beide Phänomene nutzen alle vorhanden Ausforschungsmöglichkeiten und haben grundsätzlich Unternehmens-Know-how im Visier.

Der Unterschied besteht darin, dass Wirtschaftsspionage, für deren Abwehr der Verfassungsschutz zuständig ist, staatlich gelenkt ist. Konkurrenzausspähung hingegen wird durch Wettbewerber gesteuert und die Zuständigkeit liegt bei der Polizei.

Im Spionage-Fokus stehen im Besonderen innovative Unternehmen. Überproportional gefährdet sind kleine Unternehmen mit erheblichem Wettbewerbsvorteil. Sowohl die Installation von Informationssicherheitsbeauftragten als auch deren Budget sind dort nicht durch Konzernvorgaben geregelt. Damit ist es schwerer, ein notwendiges Informationssicherheitsmanagementsystem (ISMS) aufzubauen und zu betreiben. Angreifer haben es so leichter.

Bevorzugte Ziele der Ausspähung sind Technologie und Wissenschaft. Die Bereiche Material- und Rüstungstechnik, Computertechnologie, Maschinenbau, Luftfahrt- und Verkehrstechnik, Energie- und Umwelttechnik sowie Biotechnik und Medizin sind in besonderem Maße gefährdet.

In einigen Technologiebereichen besteht darüber hinaus die Gefahr der Proliferation, d. h. die Herstellung bzw. Weiterverbreitung von Massenvernichtungswaffen bzw. dazu verwendbare Produkte, die es gilt abzuwehren. Weitere Informationen hierzu finden Sie auf unserer Webseite: www.verfassungsschutz.niedersachsen.de/

Was bedeutet Wirtschaftsschutz?

Wirtschaftsspionage und Proliferation entgegenzutreten ist Aufgabe der Spionageabwehr. Der Wirtschaftsschutz ist der präventive Anteil der Spionageabwehr, der damit beauftragt ist, Wirtschaftsspionage zu verhindern oder mindestens zu erschweren.

Die Präventionsaufgabe ist ebenso wie die operative Spionageabwehr beim Verfassungsschutz angesiedelt. Bei der Wahrnehmung wird gerade im Bereich der Präventionsarbeit besonderer Wert auf eine vertrauliche sowie vertrauensvolle Zusammenarbeit mit allen Wirtschaftsunternehmen gelegt.

Da sich Wirtschaftsspionage und Konkurrenzausspähung oft nicht deutlich voneinander unterscheiden lassen, sollte der Fachbereich Wirtschaftsschutz des Niedersächsischen Verfassungsschutzes bei Verdachtsmomenten auf jeden Fall kontaktiert werden.

Fallbeispiel: Das Auffinden einer „fremden“ Fritz-Box im Unternehmensnetz kann bereits einen massiven Informationsabfluss offenbaren.

Gemäß Wirtschaftsschutz-Studie 2022 des bitkom ergeben sich 202 Milliarden Euro Schaden pro Jahr im Zusammenhang mit Diebstahl, Industriespionage oder Sabotage.

Gemäß einer Studie des Gesamtverbands der Deutschen Versicherungswirtschaft (GDV) 2019 sind Innentäter für 63% der Fälle von Wirtschaftskriminalität verantwortlich.

Reagieren Sie nicht erst nach dem Schadenereignis!

- Werden Sie sich Ihrer Verantwortung bewusst.
- Nutzen Sie unser kostenloses Informations- und Vortragsangebot.
- Führen Sie eine Informationsinventur durch.
- Definieren sie Ihr spezielles Know-how.
- Erstellen Sie Notfallpläne.
- Testen und üben Sie Ihre Notfallpläne.
- Kontaktieren Sie uns vor verdächtigen Firmenbesuchen oder Joint-Venture-Angeboten bzw. entsprechenden Verhandlungen.
- Beachten Sie unsere Empfehlungen zu Auslandsreisen.
- Achten Sie auf Besonderheiten und Unregelmäßigkeiten.
- Entnetzung: Betrachten Sie Technik nicht als Selbstzweck, sondern als Hilfsmittel. Permanente Internetverbindungen sind große Einfallstore für Schadprogramme.
- Schulen Sie Ihr Personal.
- Verändern Sie Ihre Firmenkultur. Mitarbeitersensibilität ist eine unerlässliche Fähigkeit bei der Abwehr von Spionage.

Die Aufklärung von Wirtschaftsspionage ist Aufgabe der Spionageabwehr des Verfassungsschutzes.

Wie funktioniert Wirtschaftsspionage?

Grundsätzlich ist davon auszugehen, dass Spione alle Möglichkeiten nutzen – von technischen Mitteln bis hin zur Manipulation von Menschen, sogenanntes social engineering!

Fallbeispiel: Umleitung von Waren oder Finanztransaktionen durch manipulierte E-Mails.

Elektronische Angriffe (z.B. über das Internet) sind nur eine neue Dimension in dieser Betrachtung. Sie ersetzen keine Angriffsstrategien, sondern ergänzen diese!

Auch konventionelle Methoden (von Diebstahl über Anbahnung der Kontaktaufnahme bis Erpressung) werden weiterhin genutzt!

Das Problem ist also nicht, sich gegen eine dieser Angriffsmöglichkeiten zu wappnen. Es gilt vielmehr alle Gefahren zu kennen, um diese permanent abwehren zu können. Die Institution eines Informationssicherheitsmanagementsystems ist hierbei behilflich.

Fallbeispiel: Der Chef eines Pharma-Konzerns wird in seinem Dienst-KfZ abgehört.

Kurze Einführungen in die Problembereiche haben wir für Sie in den Bund-Länder-Flyern auf folgender Web-Seite zusammengestellt.

99 % aller erfolgreichen elektronischen Angriffe erfolgen über bekannte Schwachstellen!

(Quelle: Verizon 2015 Data Breach Investigations Report)