

Verfassungsschutz

Wirtschaftsspionage

Risiko für Unternehmen,

Wissenschaft und

Forschung

**Bund
Länder**



Vorwort

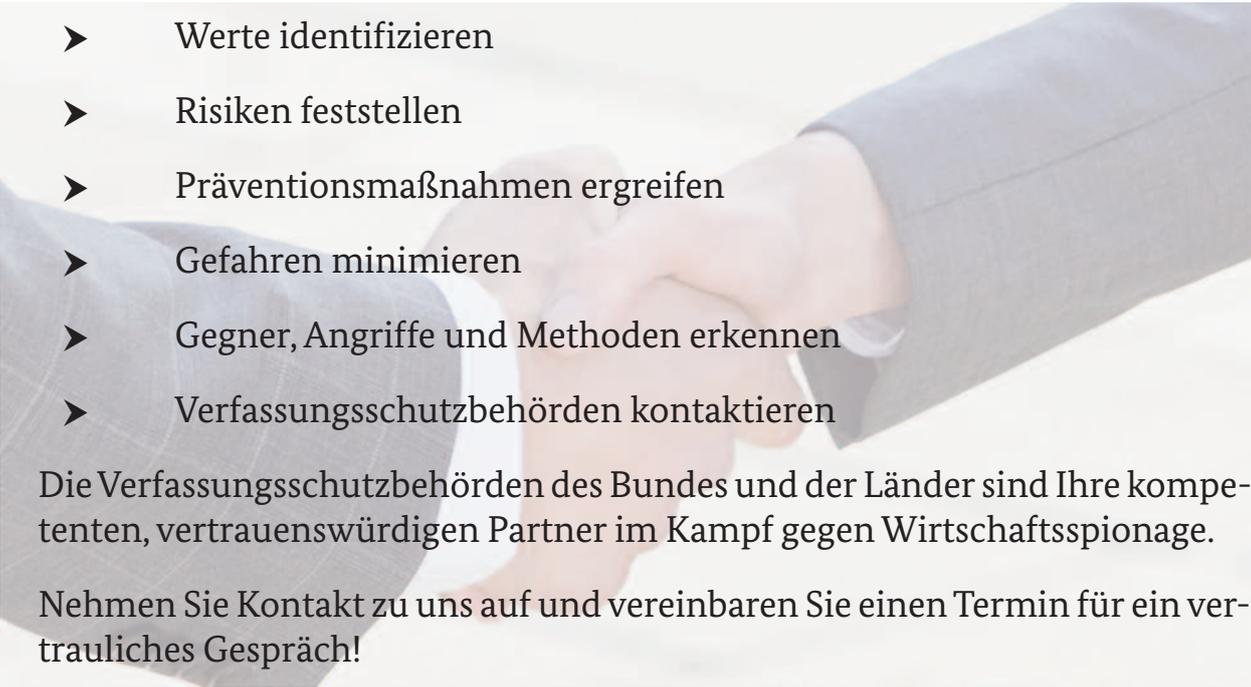
Wirtschaftsspionage ist eine ernstzunehmende und dennoch in der Praxis oft unterschätzte Gefahr in unserer globalisierten, vernetzten Welt.

Spionageaktivitäten fremder Staaten richten sich auch gegen Wirtschaft, Wissenschaft und Forschung. Der potenzielle Schaden ist enorm: Der ungewollte Abfluss von Know-How gefährdet unmittelbar den wirtschaftlichen Erfolg von Unternehmen, aber mittelbar auch die Wettbewerbsfähigkeit und Stabilität unserer Volkswirtschaft.

Deutschland braucht starke Unternehmen, innovative und kreative Wissenschaftler und Forscher. Sie sind die Basis für unseren wirtschaftlichen Erfolg. Know-How-Schutz ist daher essentielle, unabdingbare Voraussetzung für jedes Unternehmen und eine Aufgabe, bei der die Verfassungsschutzbehörden von Bund und Ländern einen wertvollen Beitrag leisten können.

Prävention durch Sensibilisierung ist eine der wichtigsten Maßnahmen gegen Wirtschaftsspionage. Sie hilft, eventuelle Spionageaktivitäten bereits im Vorfeld zu erkennen und abzuwehren. Ein umfassendes Schutzkonzept darf allerdings nicht auf Sensibilisierung beschränkt bleiben. Darüber hinaus müssen auch Vorkehrungen für den Schadensfall getroffen werden.

Diese Broschüre informiert und unterstützt Sie bei den notwendigen Schritten hin zu einem wirksamen Schutzkonzept:

- 
- Werte identifizieren
 - Risiken feststellen
 - Präventionsmaßnahmen ergreifen
 - Gefahren minimieren
 - Gegner, Angriffe und Methoden erkennen
 - Verfassungsschutzbehörden kontaktieren

Die Verfassungsschutzbehörden des Bundes und der Länder sind Ihre kompetenten, vertrauenswürdigen Partner im Kampf gegen Wirtschaftsspionage.

Nehmen Sie Kontakt zu uns auf und vereinbaren Sie einen Termin für ein vertrauliches Gespräch!

Inhalt

1.	Spionageabwehr – Aufgabe des Verfassungsschutzes	5
2.	Im Visier: Know-how „Made in Germany“	6
3.	Fremde Nachrichtendienste	8
3.1	Russische Nachrichtendienste	8
3.2	Nachrichtendienste der Volksrepublik China mit Zielbereichen in Wirtschaft und Wissenschaft	10
3.3	Dienste von Risikostaaten	12
3.4	Wirtschaftsspionage westlicher Dienste	13
4.	Methoden der Wirtschaftsspionage	14
5.	Möglichkeiten des Know-how-Abflusses	15
5.1	Mensch	15
5.2	Einbruchdiebstahl	16
5.3	Technik	17
5.4	Auslandsreisen	20
5.5	Sonstige Methoden	21
6.	Was leistet der Verfassungsschutz?	23
7.	Die zehn goldenen Regeln der Prävention	25
8.	Selbsttest	26
9.	Glossar	27
10.	Kontakt	29

1. Spionageabwehr – Aufgabe des Verfassungsschutzes

Die Abwehr von Spionageaktivitäten anderer Staaten in Deutschland ist eine Schwerpunktaufgabe und Kernkompetenz der Verfassungsschutzbehörden.

Zu den Aufklärungszielen fremder Nachrichtendienste zählt die Informationsbeschaffung aus Politik, Militär, Wirtschaft, Wissenschaft und Forschung. Zudem werden in Deutschland ansässige Gruppierungen, die in Opposition zu ihren Regierungen im Heimatland stehen, ausgespäht und unterwandert.

Nach den Erkenntnissen der Verfassungsschutzbehörden betreiben die oftmals personalstarken Nachrichten- und Sicherheitsdienste anderer Staaten eine intensive und an den politischen Vorgaben ihrer Regierungen oder wirtschaftlichen Prioritäten ihrer Staaten ausgerichtete Aufklärungsarbeit.



Durch die Globalisierung der Märkte und neue weltpolitische Konstellationen hat die Bedeutung der Wirtschaftsspionage seit den neunziger Jahren stetig zugenommen. Im Fokus der Ausforschung steht dabei das Know-how deutscher Wirtschaftsunternehmen und Forschungseinrichtungen.

Eine funktionierende Wirtschaft ist grundlegende Voraussetzung für die innere Stabilität von Staat und Gesellschaft. Es liegt daher im Interesse des Staates, den ungewollten Know-how-Abfluss an unbefugte Dritte zu verhindern.



Im Rahmen der staatlichen Maßnahmen zum Schutz der Wirtschaft kommt der Spionageabwehr eine hohe Bedeutung zu.

Wirtschaftsschutz als der präventive Teil der Spionageabwehr umfasst alle relevanten Maßnahmen, die geeignet sind, einen illegalen Know-how-Transfer durch fremde

Nachrichtendienste aus deutschen Unternehmen und Forschungseinrichtungen zu verhindern oder zumindest zu erschweren sowie jeglichen potenziellen Angriffen bzw. Bedrohungen für die Wirtschaft durch Extremisten und Terroristen möglichst rechtzeitig zu begegnen.

2. Im Visier: Know-how „Made in Germany“

Die deutsche Wirtschaft mit ihren zahlreichen Weltmarktführern steht für technologischen Fortschritt, hohe Qualität sowie Erfolg im internationalen Wettbewerb. Dadurch stellt sie sowohl für fremde Nachrichtendienste als auch für konkurrierende ausländische Unternehmen ein begehrtes Forschungsziel dar.

Im Vordergrund des Ausforschungsinteresses stehen vornehmlich technologieorientierte und innovative deutsche Unternehmen, z.B. aus den Bereichen der Informations- und Kommunikationstechnik (IKT), Biotechnologie, Optoelektronik, Automobil- und Maschinenbau, Luft- und Raumfahrttechnik sowie der Energie- und Umwelttechnologie. Im besonderen Fokus stehen hierbei kleine und mittlere Unternehmen (KMU), das Rückgrat der deutschen Wirtschaft. Diese verfügen – im Gegensatz zu großen Konzernen – oftmals nicht über die personellen oder finanziellen Ressourcen, um ganzheitliche Sicherheitskonzepte umzusetzen.



Der Einsatz moderner IKT ist zum Standard geworden. Diese Entwicklung hat der Spionage und Sabotage neue Möglichkeiten eröffnet. Neben dem Schutz deutscher Spitzentechnologie ist sichere Informationstechnik auch für den Betrieb Kritischer Infrastrukturen zwingend erforderlich.

Wirtschaftsspionage bzw. Konkurrenzausspähung erfolgen nicht nach einheitlichem Muster. Staaten und Unternehmen betreiben sie in Abhängigkeit von ihren spezifischen Bedürfnissen und unter Berücksichtigung der ihnen zur Verfügung stehenden Möglichkeiten. Staaten mit Technologiedefiziten haben es eher auf wirtschaftsnahe Forschungsergebnisse und konkrete Produkte abgesehen, während hoch industrialisierte Länder in erster Linie an wirtschaftlichen und wirtschaftspolitischen Strategien interessiert sind. Die in aller Regel kurzfristiger angelegte Konkurrenzausspähung zielt dagegen eher auf detaillierte Informationen zu Märkten, Technologien und Kunden ab.

Interessen fremder Nachrichtendienste

<p>Technisch und wirtschaftlich hoch entwickelte Staaten</p>	<ul style="list-style-type: none"> ➤ Wirtschaftspolitische Strategien ➤ Sozialökonomische und politische Trends ➤ Unternehmens-, Markt- und Absatzstrategien, Zielrichtungen und Methoden der Forschung ➤ Wettbewerbsstrategien, Preisgestaltung und Konditionen ➤ Zusammenschlüsse und Absprachen von Unternehmen
<p>Staaten mit Technologierückstand</p>	<ul style="list-style-type: none"> ➤ Beschaffung von technischem Know-how, um Kosten für eigene Entwicklungen und Lizenzgebühren zu sparen ➤ Beschaffung von Informationen über Fertigungstechniken, um auf dem Markt mit kostengünstiger gefertigten Nachbauten wettbewerbsfähig zu sein
<p>Interessen bei der ausländischen Konkurrenzausspähung</p>	<ul style="list-style-type: none"> ➤ Informationen über Wettbewerb, Märkte, Technologien, Kunden ➤ Aktuelles Know-how zur Produktentwicklung und Produktionstechnik ➤ Preisinformationen ➤ Kalkulationen ➤ Designstudien

3. Fremde Nachrichtendienste

3.1 Russische Nachrichtendienste

Die russischen Nachrichtendienste sind ein stabiler Faktor der nationalen Sicherheitsarchitektur; sie genießen bei der politischen Führung Rückhalt und hohes Ansehen. Sie tragen zur Erfüllung politischer Vorgaben bei und dienen nicht zuletzt dazu, neben den politischen auch die ökonomischen Interessen Russlands weltweit voranzutreiben. Die russische Wirtschaft profitiert in erheblichem Maße davon, dass alle Dienste gesetzlich verpflichtet sind, Wirtschaftsspionage zu betreiben.



Name:	Slushba Wneschnej Raswedkij (SWR) 
Aufgabe:	Zivile Auslandsaufklärung <ul style="list-style-type: none"> ➤ in den Bereichen Politik, Wirtschaft, Wissenschaft und Technik ➤ Elektronische Fernmeldeaufklärung ➤ Mitwirkung bei der Bekämpfung des internationalen Terrorismus ➤ Bekämpfung der Proliferation ➤ Ausforschung von Zielen/Arbeitsmethoden westlicher Nachrichtendienste
Personalstärke:	~ 13.000 Mitarbeiter

Name:	Glawnoje Raswediwatelnoje Uprawlenije (GRU) 
Aufgabe:	Militärischer Auslandsdienst <ul style="list-style-type: none"> ➤ Aufklärung des gesamten sicherheitspolitischen und militärischen Spektrums, z.B. <ul style="list-style-type: none"> • Bundeswehr • NATO, sonstige westliche Verteidigungsstrukturen • Bereich militärisch nutzbarer Technologie
Personalstärke:	~ 12.000 Mitarbeiter

Name:	Federalnaja Slushba Besopasnosti (FSB) 
Aufgabe:	Inlandsdienst <ul style="list-style-type: none"> ➤ Spionageabwehr (zivil und militärisch) ➤ Extremismus-/Terrorismusbekämpfung ➤ Bekämpfung Organisierter Kriminalität ➤ Sicherung der Staatsgrenze, Grenzkontrolle ➤ Fernmeldesicherheit im Bereich Telekommunikation und Informationstechnik
Personalstärke:	~ 350.000 Mitarbeiter davon ~ 200.000 Grenztruppen

3.2 Nachrichtendienste der Volksrepublik China mit Zielbereichen in Wirtschaft und Wissenschaft

Zur Aufrechterhaltung der inneren Ordnung und der Stabilität des Regimes sowie zur Durchsetzung politischer und ökonomischer Interessen unterhalten Partei und Regierung einen gewaltigen Sicherheitsapparat. Mit dem Ministerium für Staatssicherheit (MSS) verfügt China über einen der weltweit größten Sicherheits- und Aufklärungsdienste.



Name:	Ministry of State Security (MSS) 
Aufgabe:	Ziviler In- und Auslandsdienst <ul style="list-style-type: none"> ➤ Gewährleistung der Inneren Sicherheit (z.B. Terrorismusabwehr aber auch Überwachung von Oppositionellen und separatistischen Bewegungen) ➤ Spionageabwehr ➤ weltweite Auslandsaufklärung, insbesondere in den Bereichen <ul style="list-style-type: none"> • Politik • Wirtschaft • Wissenschaft und Technik • Forschung
Personalstärke:	Vermutlich zahlenmäßig größter ND weltweit

Name:	Second Department (2PLA); auch “Military Intelligence Department (MID)” genannt	
Aufgabe:	Militärischer In- und Auslandsdienst <ul style="list-style-type: none"> ➤ Weltweite Auslandsaufklärung mit menschlichen Quellen ➤ in allen Bereichen mit militärischem Bezug ➤ in den Bereichen Politik und Wirtschaft ➤ Überwachung von Oppositionellen und separatistischen Bewegungen 	
Personalstärke:	unbekannt	

Name:	Third Department (3PLA)	
Aufgabe:	Technische Aufklärung <ul style="list-style-type: none"> ➤ Aufklärung der weltweiten Telekommunikation und Fernmeldesicherheit der nationalen Netze ➤ Kontrolle des diplomatischen Fernmeldeverkehrs der ausländischen Botschaften und Unternehmen im Inland 	
Personalstärke:	unbekannt	

Dienste von Risikostaaten

3.3 Dienste von Risikostaaten

Die sicherheitspolitische Lage auf der Welt hat sich durch mehrere aufstrebende Regionalmächte verändert.

Die klassische Wirtschaftsspionage kann auch Berührungspunkte zum Phänomenbereich Proliferation aufweisen.

Sogenannte Risikostaaten, von denen zu befürchten ist, dass von dort der Einsatz von ABC-Waffen zur Durchsetzung politischer Ziele angedroht wird oder in einem bewaffneten Konflikt eingesetzt werden, bemühen sich, auch auf illegalem Wege in den Besitz solcher Waffen und der für deren Einsatz benötigten Trägertechnologie zu gelangen.

Staaten wie zum Beispiel Iran, Nordkorea, Syrien und Pakistan sehen darin ein geeignetes Mittel, um aus ihrer Sicht bestehende außenpolitische Bedrohungen abzuwehren und politische Forderungen gegenüber Nachbarstaaten oder der internationalen Staatengemeinschaft durchzusetzen.

Unternehmen erkennen die proliferationsrelevanten Absichten ihrer „Geschäftspartner“ oftmals nur schwer, wenn es sich bei dem gehandelten Gut um ein „dual-use“-Produkt handelt, das sowohl für zivile als auch für militärische Zwecke eingesetzt werden kann.



Das Wissen über proliferationsrelevante Zusammenhänge kann daher von Nutzen sein. Informationen dazu sind in der Broschüre der Verfassungsschutzbehörden „Proliferation – Wir haben Verantwortung“ nachzulesen.

3.4 Wirtschaftsspionage westlicher Dienste

Die Verfassungsschutzbehörden haben nach derzeitiger Erkenntnislage keine konkreten Anhaltspunkte, dass Nachrichtendienste verbündeter Staaten systematische Wirtschaftsspionage gegen die Bundesrepublik Deutschland betreiben.

Allerdings verfolgen einige westliche Staaten im Bereich der Wirtschaftsspionage eine andere Sicherheitsphilosophie vor dem Hintergrund ihres strategischen Informationsmanagements und ihrer nationalen Interessen.

So ist nicht auszuschließen, dass z.B. im Rahmen der strategischen Kommunikationsüberwachung durch westliche Dienste sensible Informationen unautorisiert abgeschöpft werden.

Angesichts dieses Risikos ist es daher auch ohne Vorliegen konkreter Erkenntnisse ratsam, bei sensiblen Kommunikationsinhalten entsprechende Sicherheitsvorkehrungen zu treffen.

Die Spionageabwehr der Verfassungsschutzbehörden geht allen Verdachtshinweisen, die sich auf illegale Aktivitäten fremder Nachrichtendienste beziehen, gewissenhaft nach.



4. Methoden der Wirtschaftsspionage

Die Methoden der Wirtschaftsspionage sind variantenreich und werden durch schnell fortschreitende Entwicklungen in der Informations- und Kommunikationstechnik immer vielseitiger. Zu den Arbeitsmethoden fremder Nachrichtendienste gehören sowohl die offene Informationsgewinnung als auch die konspirative Beschaffung vertraulicher Informationen.

Offene Beschaffung	Konspirative Beschaffung
Auswertung von Veröffentlichungen (z.B. im Internet und in Printmedien)	Einschleusung von Agenten
Besuch öffentlicher Veranstaltungen (z.B. Messen, Kongresse)	Erpressung durch Schaffung von Kompromatsituationen
Teilnahme an Studiengängen und wissenschaftlichen Projekten (z.B. Praktikanten und Gastwissenschaftler)	Bestechung
Teilnahme am Wirtschaftsleben (z.B. Aufkauf von Unternehmen und Beteiligung an Joint Ventures)	Observation
Social Engineering (z.B. Gesprächsabschöpfung)	Einbruchdiebstahl
Offenlegungspflichten (z.B. Produktzertifizierung und Visa-Verfahren)	Techn. Abhören von Besprechungsräumen
	Überwachung von Telekommunikation
	Cyberangriffe (z.B. durch den Einsatz von Schadsoftware)

5. Möglichkeiten des Know-how-Abflusses

5.1 Mensch

Der Mitarbeiter im Unternehmen spielt bei der Beschaffung von sensiblen Unternehmensdaten für ausländische Nachrichtendienste auch im Zeitalter des Internets und vernetzter IT-Systeme eine besondere Rolle. Zahlreiche Studien belegen, dass beim Verlust sensibler Informationen die größte Gefahr von den eigenen Mitarbeitern ausgeht. Deshalb sollte bei der Sicherung des unternehmerischen Know-hows der „Faktor Mensch“ besondere Beachtung finden.

Häufig ist Firmenangehörigen gar nicht bewusst, welche Unternehmensdaten schützenswert oder als Betriebs- bzw. Geschäftsgeheimnis eingestuft sind. Gerade Mitarbeiter mit ihrem Insiderwissen können dem Unternehmen großen Schaden zufügen, wenn sie zum „Innentäter“ werden.



Zudem ist der Einsatz von sogenannten „Non-Professionals“ eine nachrichtendienstliche Methode, um an Firmengeheimnisse zu gelangen. Fremde Nachrichtendienste sind darauf spezialisiert, Menschen auch gegen ihren Willen für ihre Zwecke zu benutzen.

Informationen über Zielpersonen werden oft in Sozialen Netzwerken erlangt, da viele Menschen häufig leichtfertig mit beruflichen und persönlichen Informationen umgehen. Details über die Position im Unternehmen oder Aufgabenschwerpunkte, aber auch über Familie oder Hobbys können als Ansatz zur Kontaktaufnahme genutzt werden. In scheinbar unverbindlichen Gesprächen können vertrauliche Informationen abgeschöpft (Social Engineering) oder Abhängigkeiten geschaffen werden.

Das Anwerben kann durch finanzielle Angebote, Vergünstigungen oder Geschenke, aber auch durch Erpressung erfolgen. In der Anfangsphase der „Zusammenarbeit“ werden kleine legale und illegale „Gefälligkeiten“ genutzt, um eine stärkere Abhängigkeit vom Auftraggeber zu erzeugen. Nachrichtendienste gehen bei solchen Operationen sehr sorgfältig, geduldig und vorsichtig vor. Das eigentliche Ziel ist für den Betroffenen meist nicht sofort erkennbar.

Ursachen für eine mögliche Illoyalität bzw. Ansatzmöglichkeiten für Spionageoperationen können u.a. sein:

- Frustration
- Unter- oder Überforderung
- vermeintliche Unterbezahlung
- Schulden oder finanzielle Notsituationen
- Beziehungsschwierigkeiten
- Suchterkrankungen
- übersteigertes Geltungsbedürfnis
- Selbstüberschätzung
- Abenteuerlust

Eine gesunde Unternehmenskultur fördert die Loyalität der Mitarbeiter und kann ungewolltem Informationsverlust entgegenwirken. Das Problem Wirtschaftsspionage sollte im Unternehmen offen angesprochen und die Beschäftigten für diese Thematik sensibilisiert werden.

Die Mitarbeiter sind das wichtigste Potenzial im Unternehmen – als „Innentäter“ können sie zu einer der größten Gefahren für Unternehmen werden, da sie „hinter der Firewall“ agieren. Prävention und Information können dieser Gefahr effektiv entgegenwirken!

5.2 Einbruchdiebstahl

Das Ziel eines Einbruchs muss nicht immer das Entwenden eines Gegenstandes im Sinne von Beschaffungskriminalität sein. Vielmehr kann es der Täter auch auf sensibles Firmen-Know-how abgesehen haben. Heimtückisch sind vor allem die Fälle, in denen augenscheinlich nichts entwendet wurde. Werden lediglich Einbruchspuren festgestellt, besteht die Möglichkeit, dass entweder Abhörtechnik wie Wanzen, Kameras oder Trojaner eingebracht oder unerkannt Daten oder Kopien mitgenommen wurden. Die Beteiligung frem-



der Nachrichtendienste an solchen Sachverhalten ist oft schwierig nachzuweisen, vor allem wenn die Tat einige Zeit zurückliegt. Daher ist es wichtig, auch im Hinblick auf mögliche Innentäter, die Verfassungsschutzbehörden so früh wie möglich zu informieren.

5.3 Technik

Effizientes und erfolgreiches Handeln von Staat und Wirtschaft ist ohne den Einsatz von Informations- und Kommunikationstechnik und der Nutzung des Internets kaum noch realisierbar. Dem hohen Nutzen der Technik stehen jedoch viele Risikofaktoren – z.B. durch Cyberangriffe – gegenüber.

Schadsoftware, Phishing und Social Engineering

Sicherheitslücken in Betriebssystemen und Anwendungen werden gezielt ausgenutzt, um in Netzwerke eindringen zu können. Durch Schadsoftware (z.B. Viren, Würmer und Trojaner) können sich Unbefugte Datenmaterial zugänglich machen bzw. Anmelde- und Netzwerkinformationen sammeln, manipulieren und sabotieren.



Über professionell gestaltete E-Mails mit infizierten Anhängen die zum Beispiel das berufliche Interessensfeld des Opfers ansprechen, wird Schadsoftware eingeschleust und somit ein unberechtigter Zugang zum Firmennetzwerk ermöglicht.

Eine weitere für Nachrichtendienste und Cyberkriminelle Erfolg versprechende Methode an die persönlichen Daten eines Internet-Benutzers zu kommen, ist Phishing. Benutzer sollen dazu gebracht werden, auf einer gefälschten Internetseite ihren Benutzernamen und ihr Passwort einzugeben. Ein vorgeschaltetes Social Engineering kann dafür sorgen, dass beim Opfer kein Misstrauen erzeugt wird und ungewollt sensible Informationen preisgegeben werden.

Der Einsatz von Schadsoftware ermöglicht die Sabotage bzw. die Übernahme von Produktions- bzw. Steuerungseinrichtungen. Der Fall Stuxnet macht deutlich, dass Kritische Infrastrukturen durch elektronische Angriffe besonders stark



gefährdet sind. So muss mit dem potentiellen Missbrauch moderner Technologien, wie Smart Grids oder Smart Meter (intelligente steuerbare Stromnetze bzw. Zähler für Energie), die den Alltag in Wirtschaft und Privathaushalten erheblich effizienter gestalten sollen, gerechnet werden.

Zudem bewies Stuxnet, welche verheerenden Folgen mit unkontrollierten, offenen Schnittstellen (z.B. USB) in IT-Systemen einhergehen können.

DDoS-Attacken und Botnetze

Unternehmen sind darauf angewiesen, dass ihre Onlinedienste wie Webshops, Cloud-Services und E-Mail-Dienste erreichbar sind. Um bereitgestellte Dienste arbeitsunfähig zu machen, werden in der Regel DDoS-Attacken (Distributed Denial of Service) durchgeführt. Koordinierte DDoS-Attacken werden über eine Vielzahl infizierter Rechner ausgeführt, die ein Botnetz bilden. Die Folge eines solchen Angriffs ist die Überlastung von Infrastruktursystemen.

Telekommunikationsanlagen und Smartphones

Neben Firmennetzwerken und Produktionsanlagen sind auch Telekommunikationsanlagen für Spionagezwecke manipulierbar. Leistungsmerkmale, wie z.B. Konferenzschaltungen oder Rückruf-Funktionen lassen sich zum heimlichen Abhören von Gesprächen und zur Raumüberwachung einsetzen.



Smartphones bieten unbefugten Dritten nicht zuletzt durch unzureichende Konfiguration der Sicherheitseinstellungen (beispielsweise über WLAN oder Bluetooth-Schnittstellen) die Möglichkeit des Datenzu-

Fall Stuxnet:

Einer der spektakulärsten Cyberangriffe der letzten Zeit. Die Verursacher nutzten eine Schadsoftware, die gezielt Siemens SCADA-Systeme (Supervisory Control and Data Acquisition) angriff. Es handelte sich um einen in der Komplexität der Funktionen noch nie aufgetretenen Computerwurm, der sich per USB-Schnittstellen weiterverbreitete. Aufgrund des Kommunikationsverhaltens von Stuxnet musste davon ausgegangen werden, dass der Iran bzw. eine dort betriebene Atomanlage Ziel des Angriffs war.

Der Onlineshop eines Elektronikhändlers ist Opfer eines DDoS-Angriffs geworden. Mehrere Tage war das Portal im wichtigen Weihnachtsgeschäft nicht erreichbar.

griffs. Hinzu kommt, dass ungeschützte mobile Geräte die Möglichkeit bieten, im Abgleich mit dem Unternehmensnetzwerk Daten auszutauschen und somit die Funktionalität eines mobilen Büros übernehmen. Bei einem Angriff ermöglichen sie einen Zugriff auf das gesamte Firmen-Know-how. Die Nutzung öffentlicher Hot-Spots stellt ebenso eine Gefahr für einen unerwünschten Systemzugriff und Datenabfluss oder -manipulation dar.

Bring Your Own Device

Insbesondere im Top-Management und bei jungen Arbeitnehmern wächst der Wunsch, persönliche IT-Präferenzen ins Arbeitsleben zu übernehmen. Dieser Trend wird als „Bring Your Own Device“ (BYOD) bezeichnet. Die Vorteile für Unternehmen liegen in erster Linie darin, dass keine Kosten für die Beschaffung der Geräte anfallen und der Wartungsaufwand reduziert wird. Ein großer Nachteil ist die mögliche Bildung einer Schatten-IT, die nicht mehr kontrollierbar ist. Weiterhin können unbekannte Softwarestände und Konfigurationen der Endgeräte zu erheblichen Sicherheitsrisiken führen.

Beruflich genutzte Geräte sollten zur besseren Kontrolle zentral administriert und das wahllose Herunterladen von Apps oder sonstiger Software nach Möglichkeit unterbunden werden. Hierbei müssen die Mitarbeiter für diese Einschränkungen besonders sensibilisiert werden, da andernfalls durch das Umgehen der Maßnahme, zum Beispiel durch sogenanntes „Jailbreaking“ (unberechtigtes Überwinden der Nutzereinschränkungen), unerwünschte Einfallstore für den Angreifer geöffnet werden.

Cloud Computing

Viele Unternehmen folgen dem Trend, Rechenkapazität, Datenspeicher, Netzwerkkapazitäten oder ganze Softwarepakete aus einem externen Netzwerk zu beziehen. Dieser als Cloud Computing bezeichnete Ansatz ermöglicht es, neue IT-Services und Geschäftsmodelle umzusetzen und diese dynamisch an den jeweiligen Bedarf anzupassen. Neben den vielen Vorteilen bestehen bei der Verwendung von Cloud-Diensten für Unternehmen Sicherheits- und Verfügbarkeitsrisiken. Durch Kompromittierung der Datenverbindung zum Cloud-Server, kann es zu einem Kontrollverlust über sensible Daten kommen.

Während des „Arabischen Frühlings“ wurde nahezu der gesamte Internetverkehr in Ägypten abgeschaltet. Ägyptische Unternehmer, die ihre Daten bei ausländischen Cloud-Anbietern ausgelagert hatten, konnten nicht mehr auf diese zugreifen.

Nachrichtendienste können Zugriff auf sensible Daten ausländischer Unternehmen bekommen, sobald diese Daten im Herrschaftsbereich des jeweiligen Staates gespeichert werden. Auch ein Ausfall der Internetverbindung

kann dazu führen, dass die Geschäftsaktivitäten zum Erliegen kommen, da Cloud Computing eine Standleitung zu den ausgelagerten IT-Strukturen erfordert. Welche Daten in die Cloud gegeben bzw. welche Services aus der Cloud angefordert werden, bedarf einer kritischen Betrachtung.



5.4 Auslandsreisen



Im Zuge der Globalisierung gehören häufige Geschäftsreisen und Auslandsaufenthalte zum Unternehmensalltag. Insofern spielt auch der Faktor Sicherheit auf Reisen eine große Rolle. Hierzu sollten insbesondere die Reisehinweise des Auswärtigen Amtes beachtet werden.

Jedoch sollte auch die Gefahr der Spionage durch fremde Nachrichtendienste nicht unterschätzt werden.

Unternehmen, die in Ländern mit besonderen Sicherheitsrisiken (siehe Staatenliste im Anhang) geschäftlich tätig sind, sollten hierbei verschiedene Punkte berücksichtigen:

Visa

Viele Länder verlangen bei Einreise von Staatsbürgern anderer Nationen außer einem gültigen Reisepass ein Einreisevisum. Für die Beantragung eines Visums sind umfangreiche persönliche und berufliche Angaben erforderlich. Die Fülle dieser Informationen erleichtert eine Überwachung im Reiseland und kann für nachrichtendienstliche Zwecke missbraucht werden.



Empfehlungen:

- ✓ Visa- und Meldebestimmungen einhalten
- ✓ Visa-Anträge gründlich und korrekt ausfüllen
- ✓ Missverständliche und abweichende Angaben zur Person oder zum Arbeitgeber vermeiden
- ✓ Bei Kontakten mit ausländischen Konsulaten möglichst wenig firmenspezifische Informationen angeben

Hotel

Hotelzimmer und Hotelsafes sind keine sicheren Aufbewahrungsorte für vertrauliche Informationen. Auch hier ist die Gefahr der Spionage gegeben. Es muss damit gerechnet werden, dass Hotelzimmer und Gepäck heimlich durchsucht werden. In einigen Ländern werden in erstklassigen Hotels durch die dortigen Nachrichtendienste Video- und Aufzeichnungsgeräte zur Überwachung eingesetzt. Des Weiteren sollte für eine sichere Telekommunikation auf die Nutzung des hoteleigenen WLAN bzw. Telefonnetzes verzichtet werden.

Empfehlungen:

- ✓ Hotelzimmer im Ausland unter dem Namen des Reisenden buchen, nicht aber unter Angabe des Firmennamens und der Funktion (z.B. Vorstandsmitglied, Geschäftsführer)
- ✓ Bei längeren Aufenthalten ggf. verschiedene Hotels benutzen
- ✓ Sensible Firmenunterlagen stets mit sich führen

5.5 Sonstige Methoden

Erpressbarkeit

Geheimdienste versuchen über die Schaffung kompromittierender Situationen, Druckmittel zu finden, um die betreffende Person zur Zusammenarbeit zu nötigen. Hierbei werden vielfältige Methoden eingesetzt. Verleitung zu verpflichtenden Gefälligkeiten, Besuche im Rotlichtmilieu oder der Einsatz attraktiver Lockvögel werden bevorzugt genutzt. Aber auch persönliche Schwierigkeiten wie Überschuldung oder Alkohol- und andere Suchtprobleme sind ein willkommenes Mittel Menschen gefügig zu machen.

Zertifizierungsverfahren

Wenn Produkte im Ausland hergestellt oder vertrieben werden sollen, besteht oft eine amtliche Zertifizierungspflicht. Mit Zertifizierungsverfahren sind detaillierte Produktprüfungen nach Normen und regelmäßige Inspektionen der Fertigungsstätten verbunden. Hier sind vor allem das chinesische CCC-Verfahren und das russische GOST-Verfahren zu nennen. Im Rahmen des CCC-Verfahrens, müssen Exporteure ihre Waren



mit dem Ziel China bei einer staatlich anerkannten und akkreditierten Stelle in China überprüfen lassen. Auch die Kontrolle der Fertigungsstätten durch chinesische Inspektoren ist Teil dieses Verfahrens. Dies schließt eine intensive

Begutachtung bei der Offenlegung von Bauplänen, internen Akten und Mustergeräten ein. Die Gefahr ist groß, dass es auf diesem Wege zu ungewolltem Wissensabfluss kommt.

Internetüberwachung

In einigen Staaten erfolgt eine umfangreiche Überwachung des E-Mail- und Internet-Verkehrs. Seit 1998 kontrolliert zum Beispiel der russische Inlandsgeheimdienst FSB mit dem Überwachungsprogramm SORM II (System für operative Untersuchungsmaßnahmen) offiziell den gesamten inländischen Netzwerk-Verkehr. Russische Internet-



provider sind verpflichtet, auf eigene Kosten eine Überwachungsschnittstelle mit einer Verbindung zum FSB einzurichten. Durch Erweiterung von SORM II mittels Deep Packet Inspection (DPI) wird dem Dienst seit 2012 ein direkter Zugriff auf den Datenverkehr in Echtzeit ermöglicht.

Kryptierungsverbot

Vertrauliche Informationen können mittels Verschlüsselung vor unbefugtem Zugriff geschützt werden. So werden beispielsweise Kommunikationsverbindungen mit VPN-Tunnel abgesichert. Festplatten von mobilen Geräten lassen sich mittels Software verschlüsseln und Kryptotelefone dienen der sicheren Sprachkommunikation. Allerdings ist der Gebrauch von Verschlüsselungstechnik in einigen Ländern aufgrund politischer Gegebenheiten eingeschränkt oder verboten. Unterschiedliche länderspezifische Regelungen bei Ein-, Ausfuhr und Verwendung von kryptographischen Produkten können dazu führen, dass Unternehmen gesetzwidrig handeln und mit rechtlichen Konsequenzen zu rechnen ist.

6. Was leistet der Verfassungsschutz?

Der Verfassungsschutz ist Ihr kompetenter Ansprechpartner, wenn es um den Schutz Ihres Firmen-Know-hows vor Wirtschaftsspionage geht. Er informiert vertraulich, kostenfrei und leistet praxisgerechte und fachkundige Unterstützung bei der Klärung von Spionageverdachtsfällen.

Zudem unterstützt der Verfassungsschutz Unternehmen, Forschungseinrichtungen sowie Verbände konkret durch Sensibilisierung und Aufklärung über die Gefahren durch Wirtschaftsspionage.



1. Präventions- und Informationsangebot

- Vorträge und Veranstaltungen zu ausgewählten Themen des Wirtschaftsschutzes (z.B. Know-how-Schutz, Geschäftsreisen)
- Vertrauliche themen- und risikobezogene Informationsgespräche mit Unternehmen und Forschungseinrichtungen
- Aktuelle Informationen auf den Webseiten der Verfassungsschutzbehörden unter der Rubrik Wirtschaftsspionage/Wirtschaftsschutz
- Herausgabe von Newslettern, themenbezogenen Faltblättern, Broschüren und Tagungsbänden
- Zusammenarbeit mit Verbänden, Kammern, Arbeitskreisen und Institutionen sowie in Sicherheitspartnerschaften
- Unterstützung bei der Einführung eines individuellen Sicherheitskonzepts

2. Unterstützung im Verdachtsfall

- Zentraler Ansprechpartner bei Verdacht auf Wirtschaftsspionage und unerklärlichem Informationsabfluss
- Kompetente Beratung und Unterstützung bei dem Verdacht auf Wirtschaftsspionage auf der Grundlage der vertraulichen Behandlung aller Informationen
- Unterstützung von forensischen Untersuchungen bei technischen Angriffen in Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI), ggf. auch mit dem Nationalen Cyber-Abwehrzentrum der Bundesrepublik Deutschland
- Bearbeitung von Verdachtsfällen mit nachrichtendienstlichen Mitteln
- Ermittlungen

Die Mitarbeiter des Verfassungsschutzes sind gerne bereit, Sie in einem persönlichen Gespräch über Ziele und Vorgehensweisen von Wirtschaftsspionen zu informieren und Sie ggf. bei der Initiierung geeigneter Sicherheitsmaßnahmen zu unterstützen.

7. Die zehn goldenen Regeln der Prävention

Deutsche Unternehmen sind häufig Vorreiter des technologischen Fortschritts. Ihre Innovationskraft gilt als Schlüssel für den wirtschaftlichen Erfolg unseres Landes. Damit dies so bleibt, müssen Know-how und sensible Daten vor Spionage geschützt werden. Prävention ist immer der beste Schutz! Oft ist nur ein geringer Aufwand notwendig, um interne Informationen effektiv gegen unbefugten Zugriff zu schützen.



Die nachfolgenden Merksätze fassen kurz und prägnant die wesentlichen Aspekte des Informationsschutzes zusammen. Bei Bedarf können sie durch unternehmensspezifische Gesichtspunkte ergänzt werden.

1. Nicht warten, bis der Spionagefall eingetreten ist!
2. Informationsinventur – „Kronjuwelen“ identifizieren!
3. Sicherheit muss Chefsache sein!
4. Ganzheitliches Sicherheitskonzept entwickeln (personell, materiell und IT-Sicherheit), die Umsetzung kontrollieren und permanent fortschreiben!
5. Informationsschutz als strategischen Erfolgsfaktor nutzen!
6. Know-how-Schutz auch bei Auslandsreisen!
7. Gutes Betriebsklima schaffen – zufriedene Mitarbeiter sind loyal!
8. Auffälligkeiten und konkrete Hinweise konsequent verfolgen; im Verdachtsfall an den Verfassungsschutz wenden!
9. Arbeitsvertragliche Regelungen zu klar definierten Geheimhaltungsvereinbarungen, Verstöße sanktionieren!
10. Zugriffsberechtigungen nach dem Prinzip „Kenntnis nur wenn nötig“!

Selbsttest

8. Selbsttest

Wie sicher ist Ihr Unternehmen?
 Nehmen Sie sich die Zeit für einen kurzen Selbsttest.

		Ja	Nein
1.	Ist das Thema „Sicherheit“ in Ihrem Betrieb „Chefsache“?		
2.	Haben Sie Ihr schützenswertes Know-how (Kronjuwelen) identifiziert?		
3.	Gibt es in Ihrer Firma ein Sicherheits- bzw. Informationsschutzkonzept?		
4.	Findet eine regelmäßige Mitarbeiter-Sensibilisierung zu Sicherheitsthemen in Ihrem Unternehmen statt?		
5.	Werden Hinweise auf Know-how-Verluste erfasst und analysiert?		
6.	Kontaktieren Sie Sicherheitsbehörden bei Verdacht auf illegalen Informationsabfluss?		

Sollte Ihre Antwort in nur einem Fall NEIN lauten, empfiehlt sich eine Beratung durch den Verfassungsschutz.

9. Glossar

Informationssicherheit:

Schutz sensibler Informationen vor Verlust und unbefugtem Zugriff.

Konkurrenzausspähung/Industriespionage:

Ausforschung eines Unternehmens durch einen Wettbewerber. Der Verfassungsschutz hat keine gesetzliche Zuständigkeit.

Konspiration:

Getarntes, heimliches oder verdecktes Vorgehen.

Kompromat:

Schaffung und Nutzung von Druckmitteln, um Personen zu einer Zusammenarbeit mit Geheimdiensten zu bewegen.

Kritische Infrastrukturen:

Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe oder andere dramatische Folgen eintreten würden.

Legalitätsprinzip:

Verpflichtung der Strafverfolgungsbehörden (Staatsanwaltschaft und Polizei), bei Kenntnis einer Straftat tätig zu werden – „Strafverfolgungszwang“. → Opportunitätsprinzip

Legalresidenturen:

Getarnte Stützpunkte fremder Nachrichtendienste, insbesondere in den offiziellen (Botschaften, Generalkonsulate) und halboffiziellen (z.B. Presseagenturen, Fluggesellschaften) Vertretungen ihrer Länder in einem Gastland.

Nachrichtendienstliche Mittel des Verfassungsschutzes:

Sammelbegriff für Mittel zur heimlichen Informationsbeschaffung durch den Verfassungsschutz (vgl. § 8 Abs. 2 BVerfSchG).

Non-Professionals:

Ausländische Studenten, Praktikanten, Wissenschaftler, Professoren u.ä. die auf Zeit in Deutschland leben und zum Zwecke der Wirtschaftsspionage genutzt werden.

Opportunitätsprinzip:

Das in den Verfassungsschutzbehörden grundsätzlich geltende Opportunitätsprinzip erlaubt innerhalb enger Grenzen das Handeln nach Zweckmäßigkeitsgesichtspunkten. Daher besteht für diese Behörden nicht die grundle-

gende Pflicht, z.B. bei Vorliegen von Anhaltspunkten für geringere Straftaten sofort die Strafverfolgungsbehörden zu benachrichtigen. Das Opportunitätsprinzip stellt das Gegenstück zu dem bei den Strafverfolgungsbehörden geltenden → Legalitätsprinzip dar.

Phishing:

Abfangen der Daten von Internetnutzern beispielsweise über gefälschte Internetadressen oder SMS.

Proliferation:

Beschaffung bzw. Weiterverbreitung von Produkten, Technologien und deren Know-how zum Auf- und Ausbau von Massenvernichtungswaffen bzw. deren Trägertechnologien.

SCADA:

Netzleitsystem mit Schaltwerken in einer Netzleitstelle für elektrische Netze.

Smart Grids/Smart Meter:

Intelligentes Stromnetz/-Energiezähler, das dem Anschlussnutzer den tatsächlichen Energieverbrauch und die tatsächliche Nutzungszeit anzeigt.

Social Engineering:

Methode, um unberechtigten Zugang zu sensiblen Informationen durch „Aushorchen“ von Personen zu erlangen. Ausgenutzt werden menschliche Eigenschaften wie beispielsweise Vertrauen, Eitelkeit, Hilfsbereitschaft, Habgier, Angst oder Respekt vor Autorität.

Spionage:

Beschaffung geschützter Informationen aus den Bereichen Politik, Militär, Wirtschaft und Wissenschaft. Spionage ist der Oberbegriff für die gemäß §§ 98 ff StGB strafbewehrten Handlungen.

Wirtschaftsschutz:

Beinhaltet im engeren Sinne alle relevanten Maßnahmen des Verfassungsschutzes, die geeignet sind, einen illegalen Know-how-Transfer durch fremde Nachrichtendienste aus deutschen Unternehmen und Forschungseinrichtungen zu verhindern oder zumeist zu erschweren.

Wirtschaftsspionage:

Staatlich gelenkte oder gestützte, von Nachrichtendiensten fremder Staaten ausgehende Ausforschung von Wirtschaftsunternehmen und Forschungseinrichtungen.

10. Kontakt

Bundesamt für Verfassungsschutz
Merianstraße 100, 50765 Köln
Tel: 02 21 - 792 0 • Fax: 02 21 - 792 29 15
E-Mail: wirtschaftsschutz@bfv.bund.de
<http://www.verfassungsschutz.de>



Landesamt für Verfassungsschutz Baden-Württemberg
Taubenheimstraße 85 a, 70372 Stuttgart
Tel: 07 11 - 954 43 01 • Fax: 07 11 - 954 44 44
E-Mail: info@verfassungsschutz-bw.de
<http://www.verfassungsschutz-bw.de>

Bayerisches Landesamt für Verfassungsschutz
Knorrstraße 139, 80937 München
Tel: 089 - 31 20 15 00 • Fax: 089 - 31 20 15 85
E-Mail: wirtschaftsschutz@lfv.bayern.de
<http://www.verfassungsschutz.bayern.de>

Senatsverwaltung für Inneres und Sport –Abteilung II–
Klosterstraße 47, 10179 Berlin
Tel: 030 - 901 29 - 470 • Fax: 030 - 901 29 - 466
E-Mail: wirtschaftsschutz@verfassungsschutz-berlin.de
<http://www.verfassungsschutz-berlin.de>

Ministerium des Innern des Landes Brandenburg –Abteilung 5–
Henning-von-Tresckow-Straße 9-13, 14467 Potsdam
Tel: 03 31 - 866 25 00 • Fax: 03 31 - 866 25 99
E-Mail: info-wirtschaftsschutz@verfassungsschutz-brandenburg.de
<http://www.verfassungsschutz-brandenburg.de>

Der Senator für Inneres und Sport,
Abteilung 4 - Landesamt für Verfassungsschutz Bremen
Flughafenallee 23, 28199 Bremen
Tel: 04 21 - 537 70 • Fax: 04 21 - 537 71 95
E-Mail: office@lfv.bremen.de
<http://www.verfassungsschutz.bremen.de>

Freie und Hansestadt Hamburg
Behörde für Inneres, Landesamt für Verfassungsschutz
Johanniswall 4/III, 20095 Hamburg
Tel: 040 - 24 44 43 • Fax: 040 - 33 83 60
E-Mail: poststelle@verfassungsschutz.hamburg.de
<http://www.hamburg.de/verfassungsschutz>

Landesamt für Verfassungsschutz Hessen
Konrad-Adenauer-Ring 49, 65187 Wiesbaden
Tel: 06 11 - 72 04 04 • Fax: 06 11 - 72 01 79
E-Mail: poststelle@lfv.hessen.de
<http://www.verfassungsschutz.hessen.de>

Innenministerium des Landes Mecklenburg-Vorpommern –Abteilung 5–
Johannes-Stelling-Straße 21, 19053 Schwerin
Tel: 03 85 - 742 00 • Fax: 03 85 - 71 44 38
E-Mail: info@verfassungsschutz-mv.de
<http://www.verfassungsschutz-mv.de>

Niedersächsisches Ministerium für Inneres und Sport –Abteilung 6–
Büttnerstraße 28, 30165 Hannover
Tel: 05 11 - 670 90 • Fax: 05 11 - 670 93 93
E-Mail: wirtschaftsschutz@abt6.mi.niedersachsen.de
<http://www.verfassungsschutz.niedersachsen.de>

Ministerium für Inneres und Kommunales des Landes Nordrhein-Westfalen
–Abteilung 6–
Haroldstraße 5, 40213 Düsseldorf
Tel: 02 11 - 871 28 21 • Fax: 02 11 - 871 29 80
E-Mail: wirtschaftsspionage.verfassungsschutz@mik.nrw.de
<http://www.mik.nrw.de/verfassungsschutz>

Ministerium des Innern und für Sport Rheinland-Pfalz –Abteilung 6–
Schillerplatz 3-5, 55116 Mainz
Tel: 061 31 - 16 37 73 • Fax: 061 31 - 16 36 88
E-Mail: wirtschaftsschutz@ism.rlp.de
<http://www.verfassungsschutz.rlp.de>

Landesamt für Verfassungsschutz Saarland
Neugrabenweg 2, 66123 Saarbrücken
Tel: 06 81 - 303 80 • Fax: 06 81 - 303 81 09
E-Mail: info@lfv.saarland.de
<http://www.saarland.de/verfassungsschutz.htm>

Landesamt für Verfassungsschutz Sachsen
Neuländer Straße 60, 01129 Dresden
Tel: 03 51 - 858 50 • Fax: 03 51 - 858 55 00
E-Mail: wirtschaftsschutz@lfv.smi.sachsen.de
<http://www.verfassungsschutz.sachsen.de>

Ministerium für Inneres und Sport des Landes Sachsen-Anhalt
–Abteilung 4–
Zuckerbusch 15, 39114 Magdeburg
Tel: 03 91 - 567 39 00 • Fax: 03 91 - 567 59 43
E-Mail: abwehr@mi.sachsen-anhalt.de
<http://www.mi.sachsen-anhalt.de/verfassungsschutz>

Innenministerium des Landes Schleswig-Holstein –Abteilung IV / 7–
Düsternbrooker Weg 92, 24105 Kiel
Tel: 04 31 - 988 35 00 • Fax: 04 31 - 988 35 03
E-Mail: IV7-zentrale@im.landsh.de
<http://www.verfassungsschutz.schleswig-holstein.de>

Thüringer Landesamt für Verfassungsschutz
Haarbergstraße 61, 99097 Erfurt
Tel: 03 61 - 440 60 • Fax: 03 61 - 440 62 51
E-Mail: kontakt@tlfv.thueringen.de
<http://www.thueringen.de/th3/verfassungsschutz>

Impressum

Herausgeber

Bundesamt für Verfassungsschutz
für die Verfassungsschutzbehörden
des Bundes und der Länder

Gestaltung

Bundesamt für Verfassungsschutz
Print- und MedienCenter

Druck

INFOX GmbH&Co.
Informationslogistik KG, Troisdorf

Bildnachweis

ccvision.de

© bofotolux - Fotolia.com

© yellowj - Fotolia.com

© Chepko Danil - Fotolia.com

© Benjamin Haas - Fotolia.com

© Parris Cope - Fotolia.com

© Minerva Studio - Fotolia.com

© Eva Kahlmann - Fotolia.com

© Photosani - Fotolia.com

© Nmedia - Fotolia.com

© Scanrail - Fotolia.com

© buchachon - Fotolia.com

© 3d brained - Fotolia.com

© stockWERK - Fotolia.com

© Brian Jackson - Fotolia.com

© Nikolai Sorokin - Fotolia.com

Stand

April 2014

Diese Broschüre ist Teil der Öffentlichkeitsarbeit der Verfassungsschutzbehörden des Bundes und der Länder. Sie wird kostenlos abgegeben und ist nicht zum Verkauf bestimmt. Sie darf weder von Parteien noch von Wahlwerbern und Wahlhelfern während eines Wahlkampfes zum Zwecke der Wahlwerbung verwandt werden.

