Wirtschaftsschutz

9. Wirtschaftsschutz

9.1 Einleitung

Deutschland ist als technologie- und exportorientierte Nation abhängig von auf Forschung und Erfahrung beruhendem Wissen (Know-how) und Innovation als wertvollste Ressourcen der Volkswirtschaft. Dieses Wissen und diese Informationen sind sowohl für fremde Nachrichtendienste (Wirtschaftsspionage) als auch konkurrierende Unternehmen (Konkurrenzausspähung), die gezielt und professionell Ausspähung betreiben, von höchstem Interesse. Effektive Forschung und Entwicklung zu betreiben ist zeitaufwändig und teuer, zudem bedarf es hervorragend ausgebildeten Personals. Mangelt es einem Staat oder einem Unternehmen an einer der genannten Ressourcen, kann versucht werden, sich die fehlenden Erkenntnisse über eine gezielte Ausspähung anzueignen. Insbesondere durch die Entwicklungen im Rahmen der Digitalisierung sowie die besonderen wirtschaftlichen Herausforderungen der vergangenen Jahre erhöht sich der Druck auf Unternehmen, schneller und besser produzieren zu können, bzw. neue Produkte auf den Markt zu bringen.

Potenziell betroffen sind innovative und technologieorientierte Branchen, besonders Bereiche der Informations- und Kommunikationstechnik, der Luft- und Raumfahrt, der Automobilindustrie, der Werkstoff- und Produktionstechnik, der Biotechnik und Medizin, der Nanotechnologie sowie der Energie- und Umwelttechnik. Von Interesse sind insbesondere Produktinnovationen und Marktstrategien. Aber auch auf den ersten Blick weniger innovative oder sensible Daten und Informationen können für Spionageaktivitäten attraktiv sein. Die fortschreitende Entwicklung KI-basierter Systeme (Künstliche Intelligenz) stellt in dem Zusammenhang eine besondere Herausforderung dar. Das Erlangen von Informationen über technologische Fortschritte kann einerseits Gegenstand von Spionageaktivitäten sein, andererseits können solche Systeme bei der Spionage an sich eingesetzt werden, was deren Aufdeckung weitaus schwieriger machen kann.

Insbesondere seit Beginn des russischen Angriffskrieges gegen die Ukraine sind einerseits Unternehmen der Rüstungsindustrie sowie

deren Zulieferer, andererseits aber auch Unternehmen, die als Kritische Infrastruktur (KRITIS) gelten, in den Fokus geraten. Hier stehen weniger Aspekte der Spionage als solche der Sabotage im Vordergrund.

Niedersächsische Unternehmen verzeichnen mit ihren Spitzentechnologien große Erfolge, z. B. im Bereich der Automobil- und Schifffahrtsbranche, der Laser- und Sensortechnik, der Windenergieanlagen und Landmaschinen sowie der Hörgeräteakustik und können damit Ziel fremder Nachrichtendienste und von Konkurrenzfirmen sein.
Vor diesem Hintergrund wurde im Jahr 2000 beim Niedersächsischen Verfassungsschutz aus der Spionageabwehr heraus der Fachbereich Wirtschaftsschutz geschaffen. Dieser Fachbereich des Niedersächsischen Verfassungsschutzes versteht sich als Partner der Wirtschaft.
Die Verfassungsschutzbehörden von Bund und Ländern haben sich auf folgendes gemeinsames Aufgabenverständnis der Fachbereiche Wirtschaftsschutz geeinigt:

„Die Verfassungsschutzbehörden informieren im Rahmen des präventiven Wirtschaftsschutzes über eigene Erkenntnisse und Analysen, die dazu beitragen, dass Wirtschaft und Wissenschaft sich eigenverantwortlich effektiv gegen Ausforschung (insbes. Wirtschaftsspionage), Sabotage und Bedrohungen durch Extremismus und Terrorismus schützen können."

Das Beratungsangebot des Niedersächsischen Verfassungsschutzes zu den Themen Wirtschafts- und Industriespionage, Cybersicherheit[220], Know-how-Schutz, Sicherheit in der Informations- und Kommunikationstechnologie, Geheimschutz in der Wirtschaft, Sicherheit auf Geschäftsreisen im Ausland, Innentäterproblematik und Social Engineering[221] wird stark nachgefragt. Es sind bereits

220 Cybersicherheit erweitert das Aktionsfeld der klassischen IT-Sicherheit auf den gesamten Cyber-Raum. Dieser umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik und schließt darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein. Damit wird praktisch die gesamte moderne Informations- und Kommunikationstechnik zu einem Teil des Cyber-Raumes (siehe Bundesamt für Sicherheit in der Informationstechnik, www.bsi.bund.de).

221 Social Engineering bezeichnet eine Methodik zur Verhaltensmanipulation. Social Engineers spionieren das persönliche Umfeld ihres Opfers aus, täuschen Identitäten vor oder nutzen Verhaltensweisen wie Autoritätshörigkeit aus, um geheime Informationen oder unbezahlte Dienstleistungen zu erlangen.

zahlreiche Unternehmen bei Vortragsveranstaltungen mit sicherheitsrelevanten Informationen erreicht worden.

Im Sinne eines verlässlichen Partners ist der Fachbereich Wirtschaftsschutz single Point of Contact (SPOC) für die Wirtschaft und damit auch Ansprechpartner bei fachlichen Fragen über die genannten Themengebiete hinaus. So können z. B. auch Fragen zum Extremismus in Absprache mit den jeweiligen Fachbereichen in den Beratungsgesprächen thematisiert werden.

9.2 Aufgaben und Arbeitsweise

Im vergangenen Jahr wurden durch Veranstaltungen des Fachbereiches Wirtschaftsschutz im Niedersächsischen Verfassungsschutz eine Vielzahl von Unternehmen erreicht.

Beratungen

Zum Kerngeschäft des Fachbereiches Wirtschaftsschutz zählen individuelle Sensibilisierungs- und Informationsgespräche bei den Unternehmen vor Ort. Insgesamt wurden im Jahr 2023 69 Beratungen aufgrund spezieller Anfragen durchgeführt (2022 waren es 75).

Der Verfassungsschutz unterliegt nicht dem Legalitätsprinzip. Das ermöglicht es, gegenüber den in den Unternehmen verantwortlich handelnden Personen Vertraulichkeit zuzusagen, ohne dass Gesprächsinhalte ggf. eine strafrechtliche Bearbeitung nach sich ziehen.
Sind Unternehmen von einem Sicherheitsvorfall betroffen, befürchten sie unter Umständen einen Imageverlust, sofern der Vorfall öffentlich bekannt wird. Dadurch bedingt ist auch von einem großen Dunkelfeld vorhandener, aber nicht mitgeteilter oder angezeigter Sicherheitsvorfälle auszugehen.
Im Jahr 2023 war bei Sicherheitsvorfällen häufig die Informationstechnologie von Unternehmen betroffen. In den meisten Fällen waren Firmennetzwerke durch Schadsoftware manipuliert. Eine nachrichtendienstliche Steuerung dieser Angriffe war nicht auszuschließen.

Wie verschiedene Meldungen an den Verfassungsschutz zeigen, werden Unternehmen nach wie vor häufig Opfer von Verschlüsselungstrojanern. In den überwiegenden Fällen werden diese per E-Mail eingeschleust. Entweder befindet sich in der E-Mail eine Verlinkung, die auf eine schadhafte Internetseite verweist oder es wird eine Schadsoftware in einem manipulierten Anhang mitgeschickt.

Moderne Schadsoftware ist z. B. in der Lage, eine bestehende E-Mail-Kommunikation auszulesen und so eine schadhafte E-Mail zu generieren, die sich von der vorherigen Kommunikation kaum unterscheidet. Die Gefahr, auf den Anhang einer so generierten E-Mail zu klicken, ist damit sehr hoch. Entwicklungen der KI können in diesem Zusammenhang ebenfalls für Angriffe genutzt werden.

Eine Vielzahl von Cyberangriffen wird durch intensives Social Engineering vorbereitet bzw. begleitet. Je mehr im Vorfeld über Adressaten einer (maliziösen) E-Mail bekannt ist, umso besser kann diese formuliert und angepasst werden, womit sich die Wahrscheinlichkeit, für authentisch gehalten und geöffnet zu werden, entsprechend erhöht.

Soweit ein Unternehmen Opfer eines solchen Angriffs wird, erfolgt in den meisten Fällen keine sofortige Verschlüsselung. Stattdessen wird zunächst versucht, das infiltrierte Netzwerk genauer zu untersuchen und nach Möglichkeit Unternehmensdaten auszuleiten. Die Verschlüsselung der Daten erfolgt erst im letzten Schritt und ist meist verbunden mit der Aufforderung einer Lösegeldzahlung. Der Schaden für das betroffene Unternehmen ist so erheblich höher. Oft liegt die Infektion mit der Schadsoftware schon längere Zeit zurück, wird aber erst mit Eintreten der Verschlüsselung bemerkt. Dies erschwert die forensische Analyse enorm.

In den Fällen, die dem Niedersächsischen Verfassungsschutz mitgeteilt wurden, konnte nach eingehender Prüfung der Verdacht einer nachrichtendienstlichen Tätigkeit nicht begründet werden. Es handelte sich eher um Fälle von Wirtschaftskriminalität.

Vor den im Informationsverbund der Verfassungsschutzbehörden im Verlauf des Jahres 2023 bekannt gewordenen Risiken (meist Cyberangriffe) wurden die betreuten Unternehmen in Niedersachsen

in zahlreichen Newslettern des Fachbereiches Wirtschaftsschutz gewarnt. Die Newsletter dienen in erster Linie der Sensibilisierung in den Unternehmen.
Nach wie vor ist davon auszugehen, dass soziale Netzwerke (Xing, Facebook, LinkedIn o. a.) genutzt werden, um im Rahmen von Social Engineering Informationen zu beschaffen, um diese im späteren Verlauf für Cyberangriffe zu verwenden.

Vortragstätigkeit

Im Jahr 2023 hielten Mitarbeitende des Fachbereiches Wirtschaftsschutz 81 Vorträge bei unterschiedlichen Veranstaltungen (2022 waren es 91). Neben Industrie- und Handelskammern, Wirtschaftsverbänden, Universitäten und kommunalen Wirtschaftsförderungen werden die Vorträge des Niedersächsischen Verfassungsschutzes stark von Unternehmen für ihre Mitarbeiterinnen und Mitarbeiter sowie insbesondere auch für Führungskräfte nachgefragt, um für ein sicheres Verhalten zu sensibilisieren.

Netzwerkarbeit

Ein bedeutsamer Aspekt der Arbeit des Niedersächsischen Verfassungsschutzes im Bereich des Wirtschaftsschutzes ist die Netzwerkarbeit. Ein wichtiger Partner, auch für den Informationsaustausch, ist die niedersächsische Polizei, die oft Hinweisgeber für mögliche Wirtschaftsspionagefälle ist. Häufig arbeitet der Verfassungsschutz mit dem Landeskriminalamt Niedersachsen (LKA NI) und der dortigen „Zentralen Ansprechstelle Cybercrime für die niedersächsische Wirtschaft“ (ZAC) zusammen.
Mit der fortschreitenden Digitalisierung sowie zunehmender Bedeutung von Industrie 4.0, der Verzahnung von Produktion mit modernster Informations- und Kommunikationstechnik und damit verbunden der Cybersicherheit, haben sich Netzwerke gebildet, die für Unternehmen Hilfestellungen und Lösungen bieten. Seit vielen Jahren ist das Netzwerk „niedersachsen.digital e. V.“ ein fester Partner des Niedersächsischen Verfassungsschutzes. Der Fachbereich Wirtschaftsschutz ist regelmäßig bei der dort ansässigen Fokusgruppe Cybersicherheit vertreten. Darüber hinaus wirkt der Fachbereich Wirtschaftsschutz im IT-Gesprächskreis der Industrie- und Handelskammer Hannover und bei der interdisziplinären Expertengruppe „Indy4“ mit

und ist mit einem Mitglied im Außenwirtschaftsausschuss vertreten. Außerdem ist er Multiplikator in der Allianz für Cybersicherheit beim Bundesamt für Sicherheit in der Informationstechnik (BSI).

9.3 Unternehmen der Kritischen Infrastruktur (KRITIS)

Eine besonders herausfordernde Aufgabe ist gerade in unsicheren Zeiten die Aufrechterhaltung des Gemeinwohls. Deren sehr wichtige Bestandteile sind Unternehmen, die als Kritische Infrastruktur (KRITIS) gelten, da deren Produktionsanlagen bzw. -systeme von wesentlicher Bedeutung für die Produktion lebensnotwendiger Güter oder Dienstleistungen sind. Ein umfangreicher Lieferausfall dieser Produkte kann i. d. R. nicht durch andere Akteure aufgefangen oder ausgeglichen werden.
Mögliche Konsequenzen daraus wären, dass die Bevölkerung entsprechende Waren bzw. Leistungen nicht mehr beziehen kann und in nächster Konsequenz Hunger, Durst, mangelhafte Gesundheits- und/oder Energieversorgung etc. folgen können. Der Schutz Kritischer Infrastrukturen ist somit eine immens wichtige Aufgabe, die insbesondere mit Beginn des russischen Angriffskrieges gegen die Ukraine stärker in den Fokus geraten ist.
Der Fachbereich Wirtschaftsschutz pflegt sehr gute Kontakte zu allen dem Niedersächsischen Verfassungsschutz bekannten Betreibern Kritischer Infrastrukturen in Niedersachsen, um diese bestmöglich zu unterstützen. Er berät in Fragen der Spionage- und Sabotageabwehr, um die Versorgungssicherheit möglichst umfassend zu gewährleisten. Die ganzheitliche Sicht „Steigerung der inneren Sicherheit für Niedersachsen" durch Erhöhung der Resilienz in KRITIS-Unternehmen ist hier der treibende Faktor, welchem auch durch Mitarbeit in verschiedenen Gremien Rechnung getragen wird.

In Zusammenarbeit mit anderen Abteilungen des Niedersächsischen Ministeriums für Inneres und Sport und dem Landeskriminalamt Niedersachsen wurde am 21.03.2023 die dritte Tagung für Sicherheitsverantwortliche der KRITIS-Unternehmen durchgeführt.

Teilgenommen haben daran circa 80 Personen, überwiegend Security Officer der unterschiedlichen KRITIS-Sektoren. Die Vortragenden aus verschiedenen Bereichen der Bundes- und Landesverwaltung (u. a. auch des Bundesamtes für Sicherheit in der Informationstechnik, BSI) sowie der Stiftung Wissenschaft und Politik (SWP), des Deutschen Institutes für Normung (DIN), des Helmholtz Centers for Information Security (CISPA), des Brandenburgischen Institutes für Gesellschaft und Sicherheit gGmbH (BIGS) und T-Systems International GmbH boten ein für alle KRITIS-Sektoren nützliches Programm. Ein Schwerpunkt der Tagung lag darin, die unterschiedlichen behördlichen Akteure sowie deren Aufgaben und Möglichkeiten der Zusammenarbeit im Themenfeld KRITIS kennenzulernen. Ein zweiter Schwerpunkt war der Austausch über Herausforderungen hiesiger KRITIS-Unternehmen nach Beginn des russischen Angriffskrieges gegen die Ukraine.

9.4 Hannover Messe

Der Niedersächsische Verfassungsschutz beteiligte sich vom 19. bis 21.04.2023 am Gemeinschaftsstand „Digitalisierung" des Landes Niedersachsen auf der Hannover Messe. Das Angebot diente dem Austausch der ausstellenden Institutionen mit den Besucherinnen und Besuchern, die sich über aktuelle Trends und Entwicklungen (z. B. Digitalisierung, Cybersecurity oder allgemeine Awareness in Unternehmen) informieren wollten. Einer der Messetage stand unter dem Motto „Cybersicherheit und Wirtschaftsschutz", in dessen Kontext Vorträge und Diskussionen zu Spionageabwehr und Cyberangriffen angeboten wurden, an denen auch der Fachbereich Wirtschaftsschutz beteiligt war.

9.5 Best practice meeting

Das „best practice meeting" ist ein Veranstaltungsformat des Niedersächsischen Verfassungsschutzes für maximal 25 Personen je Veranstaltung. Jede Veranstaltung setzt einen thematischen Schwerpunkt zu dem nach einem einleitenden Kurzvortrag in einer

moderierten Diskussionsrunde verschiedene Standpunkte und Erfahrungen ausgetauscht werden. Aufgrund des überschaubaren Teilnehmerkreises hat sich dieses Format als äußerst zielorientiert für die jeweils vertretenen Unternehmen erwiesen.

Am 09. und 10.03.2023 fanden zwei Veranstaltungen zum Thema „Cyberangriff - und dann?" in Osnabrück statt. Inhaltlich beschäftigten sich beide Veranstaltungen mit bestmöglichen Abwehrmaßnahmen sowie mit dem Umgang und den Folgen eines solchen Angriffs.

Das dritte „best practice meeting" fand am 09.06.2023 zum Thema „Zero-Trust" in der Region Hannover statt. Kennzeichnend für den Zero-Trust-Ansatz ist, dass prinzipiell keinem Dienst, Nutzer oder Gerät in der Informationstechnik vertraut wird. Damit soll das Risiko für Unternehmensnetzwerke und -applikationen auf ein Minimum reduziert und sowohl externe Bedrohungen als auch interne Gefahrenquellen ausgeschaltet werden. Die Tatsache, dass die Implementierung eines solchen Ansatzes mit unterschiedlichen Herausforderungen verbunden ist, bildete die Grundlage für eine umfangreiche Diskussion.

9.6 Sicherheitstagung für geheimschutzbetreute Unternehmen

Vom 10. bis 11.05.2023 fand die jährliche Sicherheitstagung für geheimschutzbetreute Unternehmen des Niedersächsischen Verfassungsschutzes mit etwa 70 Sicherheitsbevollmächtigten sowie Vertreterinnen und Vertretern einzelner Sicherheitsbehörden in Wildeshausen statt. Zu Beginn informierte Christian Krebs vom Bundesministerium für Wirtschaft und Klimaschutz als dortiger Betreuer für geheimschutzbetreute Unternehmen über aktuelle Entwicklungen im Bereich der Geheimschutzbetreuung sowie anstehende Veränderungen für die betroffenen Unternehmen.

Anschließend referierte ein Vertreter des österreichischen Abwehramtes über Gemeinsamkeiten und Unterschiede in der Geheimschutzbetreuung der deutschen bzw. österreichischen Behörden. Er klärte auch über Besonderheiten auf, die relevant für geheimschutzbetreute Unternehmen sind, die sowohl in Deutschland als auch in Österreich tätig sind.

Stefan Lukas, Nahost-Analyst und Gastdozent an der Führungsakademie der Bundeswehr in Hamburg, referierte über die sicherheitspolitische Lage im Iran. Er gab einen Überblick über die derzeit herrschenden Machtverhältnisse im Iran und die weiterhin anhaltende Autorität der Pasdaran. Zudem verdeutlichte er die oft unterschätzte Position des Irans als Dreh- und Angelpunkt der Weltwirtschaft sowie die Auswirkungen des Klimawandels auf zukünftige Konflikte im und um das Land.

Dominik Johannes von der Deutschen Telekom Security GmbH stellte verschiedene Mittel der Lauschabwehr vor, mit deren Hilfe Räume auf ihre Abhörsicherheit geprüft werden. So kommen u. a. Hochfrequenzmessungen und Thermografiedetektion, aber auch die visuelle Überprüfung eines Raumes und seiner Einrichtungsgegenstände zum Einsatz.

Anschließend charakterisierte Michael Willer von der Human Risk Consulting GmbH verschiedene Angriffskanäle des Social Engineerings, also dem Manipulieren von Menschen durch psychologische Techniken, um ein bestimmtes Verhalten hervorzurufen. Er veranschaulichte, mit welchen Mitteln er in seiner Arbeit Unternehmen auf ihren „Sicherheitsfaktor Mensch“ testet, z. B. mit Phishing-Mails oder durch legendierte Telefonanrufe.

Ergänzt wurde die Tagung um zwei Fachvorträge des Verfassungsschutzes: zum einen mit einem Überblick über Aktivitäten der verfassungsschutzrelevanten Delegitimierung des Staates und zum anderen über aktuelle Entwicklungen in Bezug auf staatlich gesteuerte Cyberangriffe.

Zum Abschluss der Tagung stellte Lena Bennefeld vom geschäftsführenden Vorstand des Laserzentrum Hannover e. V. die aktuelle Forschung und Arbeit des Laserzentrums vor, darunter z. B. die Erforschung von Produktionstechnik auf dem Mond oder von innovativer Agrartechnik.

9.7 22. Wirtschaftsschutztagung des Niedersächsischen Verfassungsschutzes

An der Wirtschaftsschutztagung am 06.11.2023 in Hannover nahmen etwa 255 Teilnehmerinnen und Teilnehmer aus Wirtschaft, Wissenschaft und von staatlichen Institutionen teil.

Die Niedersächsische Innenministerin Daniela Behrens eröffnete die Tagung und gab u. a. einen kurzen Ausblick zur Entwicklung der nicht abschwellenden Desinformationskampagnen im Zusammenhang mit dem russischen Angriffskrieg in der Ukraine sowie den Angriffen der HAMAS auf Israel.

Michael Kaspar, Islamwissenschaftler beim Niedersächsischen Verfassungsschutz, informierte über den Nahost-Konflikt und gab Einblicke in die Ziele und Vorgehensweise der terroristischen Organisationen „HAMAS“ und „Hizb Allah“. Die Auswirkungen des Krieges auf Deutschland und Niedersachsen zeigten sich aktuell virtuell hauptsächlich durch Sympathie- bzw. Antipathiebekundungen sowie aufgeheizte Diskussionen und Desinformationskampagnen, in der Realwelt allerdings auch in einem gesteigerten Demonstrationsgeschehen mit ansteigendem Aggressionspotenzial.

Stefan Wöhlken von der TELCAT MULTIKOM GmbH und Markus Dietz von der GRASS-MERKUR GmbH stellten Möglichkeiten dar, wie sich Unternehmen sowohl in der (Festnetz-)Telefonie als auch in der allgemeinen Informationstechnik krisenfester aufstellen und Bedrohungen im Vorfeld durch ein Schwachstellenmanagement rechtzeitig erkennen können.

Die Referenten wiesen u. a. auf wichtige Leitlinien des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sowie die Richtlinie der Europäischen Union zur Netzwerk- und Informationssicherheit (NIS2-Richlinie) hin, deren Ziel die Stärkung der Cyberresilienz in der Europäischen Union ist.

Dr. Kristin Masuch, als Vertreterin für das Projekt „ITS.Kompetent“, ergänzte das Thema durch Ausführungen zur Human Firewall und

appellierte an die Unternehmen, auf maßgeschneiderte Cybersicherheitsmaßnahmen zu setzen. So sollten die Trainingsmaterialien und Awareness-Maßnahmen anhand der individuell vorhandenen IT-Kompetenz ganz gezielt ausgewählt werden.

David Richter, Mitarbeiter des Auswärtigen Amtes, berichtete über die internationale Vorgehensweise bei Cyberangriffen durch ausländische Akteure und machte das Ziel der gemeinsamen Bemühungen deutlich: Resilienz-Erhöhung, und somit der Schutz einer „gemeinsamen digitalen Welt".

Ein zweiter Themenblock setzte sich mit den Risiken durch unseren „Partner, Konkurrenten und systemischen Rivalen", wie es in der China-Strategie der Bundesregierung heißt, auseinander und beleuchtete die Umgangsweise von Wissenschaft und Wirtschaft mit dem Handelspartner China.

Sophia Stahl von der paper trail GmbH berichtete gemeinsam mit Till Eckert von der Investigativ-Redaktion CORRECTIV über wissenschaftliche Kooperationen zwischen chinesischen und deutschen Universitäten. Thomas König von der Deutschen Industrie- und Handelskammer referierte über Inhalte und Verbesserungsansätze der im Juli 2023 veröffentlichten China-Strategie der Bundesregierung.

Flankierend erhielt das Auditorium Einblicke in die Rüstungsindustrie, vorgetragen von Peter Kunkel, Chief Security Officer (CSO) der Rheinmetall AG. Das Thema „Rüstung im Fokus" griff die aktuellen Entwicklungen, aber auch die Herausforderungen eines lokalen Rüstungsunternehmens mit weltweiten Standorten und Produktionsstätten in Kriegszeiten auf.

Der Niedersächsische Verfassungsschutzpräsident, Dirk Pejril, schloss die thematische Klammer um die Wirtschaftsschutztagung mit Ausführungen über die erstarkende Verbreitung von Verschwörungstheorien und das Weltbild von „Reichsbürgerinnen" und „Reichsbürgern". Insgesamt spiele der Faktor Sicherheit eine entscheidende Rolle bei der Bewertung der Attraktivität eines Landes, so Pejril, und sei damit ein wichtiger Faktor auch für die Ansiedlung und den Bestand von Wirtschaftsunternehmen. Daher seien die Vernetzung, der Austausch und die vertrauensvolle Zusammenarbeit zwischen Sicherheitsbehörden und Unternehmensvertreterinnen und -vertretern immens wichtig.

9.8 Kontaktdaten

Für Fragen steht der Fachbereich Wirtschaftsschutz des Niedersächsischen Verfassungsschutzes unter folgenden Kontaktdaten zur Verfügung:

Telefon: 0511 6709-284
Telefax: 0511 6709-393
E-Mail: wirtschaftsschutz@mi.niedersachsen.de
Internet: www.verfassungsschutz.niedersachsen.de