Wirtschaftsschutz

10. Wirtschaftsschutz

10.1 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 für fremde Nachrichtendienste (Wirtschaftsspionage) und konkurrierende Unternehmen (Konkurrenzausspähung), die gezielt und professionell Ausspähung betreiben, von höchstem Interesse.

Von diesen Aktivitäten 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 Energie- und Umwelttechnik. Von Interesse sind Produktinnovationen und Marktstrategien.

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 Arbeitsbereich Wirtschaftsschutz geschaffen. Dieser Arbeitsbereich des Niedersächsischen Verfassungsschutzes ist ein Partner für die Wirtschaft.

Die Verfassungsschutzbehörden von Bund und Ländern haben sich auf folgendes gemeinsames Aufgabenverständnis der Arbeitsbereiche 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[138], Know-how-Schutz, Sicherheit in der Informations- und Kommunikationstechnologie, Geheimschutz in der Wirtschaft, Sicherheit auf Geschäftsreisen im Ausland, Innentäterproblematik und Social Engineering[139] wird stark nachgefragt, wie aus den folgenden Abschnitten deutlich wird. So wurden u. a. bereits zahlreiche Unternehmen bei Vortragsveranstaltungen mit sicherheitsrelevanten Informationen erreicht.

10.2 Zahlen und Fakten

Mittlerweile werden vom Niedersächsischen Verfassungsschutz im Geheim- und Wirtschaftsschutz 1.117 Unternehmen betreut.

Beratungen

Zum Kerngeschäft des Arbeitsbereiches Wirtschaftsschutz zählen individuelle Sensibilisierungs- und Informationsgespräche bei den Unternehmen vor Ort. Insgesamt gab es im Jahr 2019 98 speziell angefragte Beratungen von Firmen.

Für die Unternehmen ist hilfreich, dass der Verfassungsschutz nicht dem Legalitätsprinzip unterliegt, also Sachverhalte mit strafrechtlich relevantem Hintergrund nicht zwingend der Staatsanwaltschaft bzw. der Polizei melden muss. Denn im Falle eines Strafprozesses könnte ein Sicherheitsvorfall öffentlich werden und die betroffenen Firmen müssten Imageschäden befürchten.

Häufig war die Informationstechnologie von Unternehmen betroffen, denn in mehreren Fällen waren Firmennetzwerke durch Schadsoftware manipuliert. Eine nachrichtendienstliche Steuerung dieser Angriffe war nicht auszuschließen.

138 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 Information 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).

139 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.

In starkem Maße werden Unternehmen Opfer von Verschlüsselungstrojanern, wie verschiedene Meldungen an den Verfassungsschutz zeigen. Nach wie vor ist das entscheidende Einfallstor in den Unternehmen die E-Mail, deren Inhalt meistens eine Verlinkung aufweist. Dort ist dann die Schadsoftware, ein Verschlüsselungstrojaner hinterlegt.
Eine weitere Betrugsart, die nach wie vor und häufig bei Unternehmen auftritt, ist der sogenannte Fake-Boss-Angriff oder auch CEO-Fraud. Angreifer nehmen in der Regel per E-Mail mit einem zeichnungsbefugten Firmenangehörigen Kontakt auf und täuschen vor, die E-Mail sei vom Vorstand des Unternehmens. Unter der Vorgabe, es handele sich zum Beispiel um einen geheim zu haltenden Firmenaufkauf, wird die Mitarbeiterin oder der Mitarbeiter aufgefordert, eine Überweisung häufig in sechsstelliger Höhe in Euro vorzunehmen. In vielen Fällen sind Unternehmen erhebliche Schäden entstanden, weil mangelnde Sensibilität und fehlendes Vieraugenprinzip zu einer Überweisung geführt haben.
In den Fällen, die dem Arbeitsbereich Wirtschaftsschutz zu den beiden vorgenannten Varianten mitgeteilt wurden, konnte nach eingehender Prüfung kein Verdacht einer nachrichtendienstlichen Tätigkeit begründet werden. Es handelte sich dann wohl eher um Fälle von Wirtschaftskriminalität.
Über den Newsletter des Arbeitsbereiches Wirtschaftsschutz an seine betreuten Unternehmen in Niedersachsen wurden zahlreiche Warnungen vor elektronischen Angriffen herausgegeben, die im Informationsverbund der Verfassungsschutzbehörden im Verlauf des Jahres 2019 bekannt geworden sind.
Nach wie vor ist davon auszugehen, dass vermehrt soziale Netzwerke (Xing, Facebook o. a.) genutzt werden, um für elektronische Angriffe Informationsbeschaffung im Rahmen von Social Engineering zu betreiben.

Vortragstätigkeit

Im Jahr 2019 hielten Mitarbeiter des Arbeitsbereiches Wirtschaftsschutz 129 Vorträge bei unterschiedlichen Veranstaltungen. Neben Industrie- und Handelskammern, Universitäten und kommunalen Wirtschaftsförderungen werden die Vorträge des Niedersächsischen Verfassungsschutzes stark von Unternehmen für ihre Mitarbeiterinnen und Mitarbeiter und Führungskräfte nachgefragt, um für eine Sensibilisierung zu sorgen.

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 und dort mit der Zentralen Ansprechstelle Cybercrime (ZAC) zusammen.
Durch die zunehmende 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. Der Arbeitsbereich Wirtschaftsschutz wirkt dabei in der Fokusgruppe Informations- und Cybersicherheit von Hannover IT e. V., im IT-Gesprächskreis der Industrie- und Handelskammer Hannover und bei der interdisziplinären Expertengruppe „Indy4" mit. Außerdem ist er Multiplikator in der Allianz für Cybersicherheit[140] beim Bundesamt für Sicherheit in der Informationstechnik.

Der Niedersächsische Verfassungsschutz führte im Rahmen seiner Netzwerkarbeit im Jahr 2019 folgende Veranstaltungen durch:

10.3 „Best practice meeting – security2share"

Das Veranstaltungsformat des Business-Frühstücks „Best practice meeting – security2share" wurde im Jahr 2019 fortgeführt.
Die Teilnehmerzahl pro Veranstaltung ist begrenzt und so waren die Termine mit Unternehmensvertreterinnen und Unternehmensvertretern unterschiedlicher Branchen schnell ausgebucht.

Etwa ab dem 6. Jhd. vor Christus begannen die Menschen damit, Texte zu verschlüsseln. Sowohl die Beweggründe, wie auch die da-

140 Die Allianz für Cybersicherheit wurde 2012 vom Bundesamt für Sicherheit in der Informationstechnik (BSI) gegründet und verfolgt das Ziel, die Widerstandsfähigkeit des Standortes Deutschland gegenüber Cyber-Angriffen zu stärken. Aktuell gehören ihr 4.088 Unternehmen, 122 Partner und 97 Multiplikatoren an.

für verwendeten Techniken haben sich im Laufe der Epochen geändert. Die Notwendigkeit aber, Informationen und Nachrichten zu verschlüsseln, hat nicht abgenommen, sondern erfährt gerade in der heutigen Zeit eine hohe Bedeutung.
In zwei Veranstaltungen am 23.01.2019 in Hannover und am 19.03.2019 in Osnabrück beschäftigten sich insgesamt 50 Unternehmensvertreterinnen und -vertreter näher mit dem Thema Verschlüsselung von Daten. Darunter fallen auch Fragestellungen nach unterschiedlichen Verschlüsselungsmethoden sowie konkreten Umsetzungsmöglichkeiten.

Im Zeitalter der Digitalisierung erwarten wir als Gesellschaft, dass Informationen ständig und überall verfügbar sind. Andererseits haben Informationen aber auch einen erheblichen Wert und müssen geschützt werden. Dieses Spannungsfeld gilt es entsprechend auszufüllen, um Verschlüsselungsmethoden sinnvoll einzusetzen.

Bei beiden Veranstaltungen gab ein Vertreter des Bundesamtes für Sicherheit in der Informationstechnik (BSI) einige grundlegende Informationen zum Thema Leitungsverschlüsselung. Der zweite Programmpunkt setzte den Schwerpunkt auf E-Mail-Verschlüsselung. Zum Abschluss wurde noch ein neuromathematischer Ansatz dargestellt, wie eine Verschlüsselung in Zukunft aussehen könnte.

Die Veranstaltungsreihe „Best practice meeting“ wird 2020 zu unterschiedlichen Themen fortgesetzt.

10.4 23. Sicherheitstagung für geheimschutzbetreute Unternehmen

Vom 14. bis zum 15.05.2019 fand in Hildesheim die Tagung des Niedersächsischen Verfassungsschutzes für Sicherheitsbevollmächtigte der geheimschutzbetreuten Unternehmen statt. Es nahmen etwa 70 Vertreterinnen und Vertreter von Wirtschaftsunternehmen sowie einige von Bundes- und Landesbehörden daran teil.

Inhaltlich lag der Schwerpunkt in diesem Jahr auf Beiträgen über die Arbeitsbereiche des Verfassungsschutzes. Vorgestellt wurde der Bereich der Investitionsprüfungen, dessen Aufgabe es ist, ausländische Direktinvestitionen auf nachrichtendienstliche Sicherheitsbedenken hin zu überprüfen. Diese Aufgabe wird vom Bundesamt für Verfassungsschutz wahrgenommen. Außerdem wurde Aktion Neustart vorgestellt, das Aussteigerprogramm des Niedersächsischen Verfassungsschutzes für Rechtsextremismus und Islamismus. Ergänzend erläuterte ein Vertreter der Volkswagen AG, wie in einem konkreten Fall mit Mitarbeitern aus dem salafistischen Umfeld umgegangen wurde und welchen Herausforderungen das Unternehmen gegenüberstand. Weitere Programmpunkte waren die Novellierung des Geheimschutzhandbuches sowie die Vorstellung der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS). ZITiS ist Dienstleister für die Sicherheitsbehörden in Deutschland und erforscht und entwickelt in deren Auftrag technische Lösungen und Methoden, die die innere Sicherheit verbessern (www.zitis.bund.de).

10.5 Verfassungsschutz unterstützt KRITIS-Tagung

Am 04.09.2019 wurde in Hannover die erste Niedersächsische KRITIS-Tagung unter maßgeblicher Beteiligung des Fachbereichs Wirtschaftsschutz des Niedersächsischen Verfassungsschutzes durchgeführt.

Das Niedersächsische Ministerium für Inneres und Sport hatte die Betreiber von Kritischen Infrastrukturen (KRITIS)[141] in Niedersachsen zu einem Dialog nach Hannover eingeladen. KRITIS sind Betriebe und Anlagen, die für die Versorgung der Menschen und die Entsorgung von Abwässern und Abfällen elementar wichtig sind. Dabei handelt es sich z. B. um Kraft- oder Wasserwerke, Krankenhäuser, aber auch um Unternehmen des Finanzwesens, Transports und Verkehrs.

In der Keynote sagte Staatssekretär Stephan Manke aus dem Niedersächsischen Ministerium für Inneres und Sport:

„Mehr als jemals zuvor ist unsere Gesellschaft heute von solchen technischen Systemen abhängig. Ohne Strom steht die industrielle Produktion still, ohne die reibungslose Versorgung mit Trinkwasser und Nahrung ist das gesellschaftliche Leben kaum vorstellbar. Bei Ausfällen dieser Infrastrukturen würde der gesellschaftliche Alltag vollständig zum Erliegen kommen. Wir haben deshalb diverse Betreiber aus diesen Bereichen zu einem umfassenden Austausch eingeladen, denn insbesondere Cyberangriffe auf unsere Kritischen Infrastrukturen sind keine Science-Fiction, sondern realistische Szenarien, denen wir uns gemeinsam stellen und worauf wir uns im Verbund vorbereiten müssen. … Unser Ziel muss es sein, auf hohem Niveau die Sicherheit Kritischer Infrastrukturen gegenüber Angriffen sicherzustellen."

An der Veranstaltung in Hannover nahmen rund 60 Gäste teil, hauptsächlich Vertreterinnen und Vertreter von KRITIS-Unternehmen sowie Behördenvertreterinnen und -vertreter und Fachexpertinnen und -experten. Auch das Verbindungsbüro des Bundesamtes für Sicherheit in der Informationstechnik (BSI) war vertreten. Spezifische Themen der Vorträge und Workshops waren u. a. analoge und digitale Risiken, wie große Betriebsstörungen, Cyberangriffe auf solche Anlagen und mögliche Domino-Effekte.

Meldungen über kritische Zustände in IT-Anlagen von KRITIS sind momentan über das IT-Sicherheitsgesetz dem BSI zugeordnet. Allerdings sind die realen bzw. „analogen" Gefahren, welche von ihnen im Falle des Ausfalles ausgehen, eher im jeweiligen Bundesland verortet. Den im Bereich des Katastrophenschutzes tätigen

141 Siehe auch Fußnote 131, Kapitel 8.3.

Organisationen und der Polizei stellen sich hier u. U. weitere ggf. neue Aufgaben.
Mit den Aufgaben der Spionage- und Sabotageabwehr in Bezug auf Wirtschaftsunternehmen gibt es aber auch die Zuständigkeit für die Verfassungsschutzbehörden.

10.6 Tagung zum Thema „Drohnen als Risiko für Unternehmen“

In der Vergangenheit vermehrten sich Meldungen aus Wirtschaftsunternehmen, die Drohnenüberflüge in teils sensiblen Bereichen feststellten. In einigen Fällen musste davon ausgegangen werden, dass während der Überflüge auch Fotos gefertigt worden sind.
Der Fachbereich Wirtschaftsschutz hat dies zum Anlass genommen, eine separate Veranstaltung zu dieser Thematik durchzuführen und die damit verbundenen Schwierigkeiten und Probleme anzusprechen sowie mögliche Lösungsansätze aufzuzeigen.

Insgesamt waren etwa 80 Teilnehmende der Einladung am 18.09.2019 gefolgt. In diversen Vorträgen von der Volkswagen AG, T-Systems International GmbH, Rheinmetall Air Defence AG, Dreger Group und Stein Maritime Consulting wurden die unterschiedlichsten Anforderungen und Einsatzkonzepte der Drohnendetektion und -abwehr dargestellt.
Abschließend gab es noch einen Ausblick, welche künftigen Entwicklungen und die damit verbundenen Bedrohungen in Zukunft zu erwarten sind und wie der sinnvolle Einsatz von Drohnen zum Beispiel für den Schutz Kritischer Infrastrukturen aussehen kann.

Zusammenfassend kann festgehalten werden, dass die Drohnentechnologie mit all ihren Möglichkeiten einen vielfältigen Nutzen bieten kann, darüber hinaus aber auch bei einer missbräuchlichen Nutzung ein großes Gefährdungspotenzial für Unternehmen und Gesellschaft besteht.

10.7 18. Wirtschaftsschutztagung des Niedersächsischen Verfassungsschutzes

Am 04.11.2019 fand die Wirtschaftsschutztagung des Niedersächsischen Verfassungsschutzes statt. Insgesamt waren etwa 220 Vertreterinnen und Vertreter größtenteils niedersächsischer Unternehmen der Einladung des Verfassungsschutzes gefolgt, um sich über die aktuelle Bedrohungslage zu informieren. Begrüßt werden konnten außerdem einige Teilnehmende anderer Sicherheitsbehörden aus Bund und Ländern.

Der Niedersächsische Minister für Inneres und Sport, Boris Pistorius, betonte in einer Keynote die Bedeutung von Zusammenarbeit und gegenseitiger Unterstützung sowie des Austausches in Sicherheitsfragen.

Auch in diesem Jahr fand sich das Thema Digitalisierung auf der Tagesordnung wieder, so gab es gleich zu Beginn eine Diskussionsrunde zum Thema „Digitalisierung und Sicherheit – geht das?". Vertreten waren dabei das Mittelstand 4.0-Kompetenzzentrum Hannover, die Digitalagentur Niedersachsen, Hannover IT e.V. sowie die Herfurth & Partner Rechtsanwaltsgesellschaft mbH.

Nach einem Beitrag des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zu aktuellen Gefahren in der Digitalisierung wurde das CyberRange-e von Innogy SE als erstes Trainingszentrum gegen Bedrohungen für den Energiesektor vorgestellt. Durch War-Gaming[142] werden die Teilnehmenden auf konkrete Situationen vorbereitet, um im Ernstfall richtig reagieren zu können.

142 Beim War-Gaming geht es darum, mögliche Angriffsszenarien spielerisch nachzustellen. Aufgeteilt in zwei Teams versuchen die Teilnehmenden in ein fremdes Netzwerk einzudringen, bzw. diesen Angriff zu erkennen und abzuwehren.

Bedingt durch die eigene Betroffenheit schilderte die Schlütersche Verlagsgesellschaft mbH, wie sie mit der Schadsoftware EMOTET im eigenen Unternehmen von der Infektion des Netzwerks bis hin zur Beseitigung umgegangen ist.

Abschließend stand noch einmal das Risiko durch fehlerhaftes Verhalten von Mitarbeiterinnen und Mitarbeitern im Mittelpunkt. Aktuelle Angriffsmethoden durch Social Engineering wurden von Human Risk Consulting GmbH sehr anschaulich erläutert.

Viele der Teilnehmenden nutzten nicht nur die Fachvorträge, um sich über die aktuellen Themen zu informieren, sondern schätzten darüber hinaus die Möglichkeit, sich untereinander zu vernetzen und den Kontakt zu Vertreterinnen und Vertretern des Verfassungsschutzes zu suchen. Der hohe Stellenwert der Wirtschaftsschutztagung als Kommunikations- und Informationsforum für Wirtschaftsunternehmen wurde dadurch mehr als deutlich.

10.8 Messen

Hannover Messe

Der Niedersächsische Verfassungsschutz beteiligte sich vom 01. bis zum 05.04.2019 an dem Gemeinschaftsstand des Landes Niedersachsen auf der Hannover Messe und informierte über das Beratungs- und Dienstleistungsangebot des Fachbereiches Wirtschaftsschutz.
Nachgefragt waren insbesondere Informationen über Wirtschafts- und Industriespionage, Know-how-Schutz und Cybersicherheit im industriellen Umfeld. Viele Besucherinnen und Besucher wünschten eine Sensibilisierung ihrer Mitarbeiterinnen und Mitarbeiter durch die Fachleute des Verfassungsschutzes.
Über den eigenen Messestand hinaus beteiligte sich der Niedersächsische Verfassungsschutz an folgenden Veranstaltungen des Rahmenprogramms:

- Moderation einer Podiumsdiskussion zum Thema „Produktion secure gestalten – Auf dem Weg zu

einer sicheren Industrie 4.0“, an der u. a. auch Stefan Muhle, Staatssekretär im Niedersächsischen Ministerium für Wirtschaft, Arbeit, Verkehr und Digitalisierung teilgenommen hat,
- Vortrag bei der Indy4-Konferenz „Digitale Perspektiven“,
- Vortrag bei einer Tagung der Gesellschaft für Datenschutz und Datensicherheit (GDD) und
- Sitzung des Ausschusses für Außenwirtschaft der Industrie- und Handelskammer (IHK) Hannover

10.9 Kontaktdaten

Für Fragen steht der Arbeitsbereich Wirtschaftsschutz beim Verfassungsschutz unter folgenden Kontaktdaten zur Verfügung:

Telefon: 0511/6709-247 oder -248
Telefax: 0511/6709-393
E-Mail: wirtschaftsschutz@verfassungsschutz.niedersachsen.de
Internet: www.verfassungsschutz.niedersachsen.de