Wirtschaftsschutz

10. Wirtschaftsschutz

10.1 Einleitung

Deutschland ist als technologie- und exportorientierte Nation abhängig von Wissen (Know-how) und Innovation. Beides sind wertvolle Ressourcen der Volkswirtschaft und basieren auf Forschung und Erfahrungen. 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, besteht hohes Interesse an der Aneignung dieses Wissens durch gezielte Ausspähung. Insbesondere durch die Entwicklungen im Rahmen der Digitalisierung und die besonderen wirtschaftlichen Herausforderungen der vergangenen Jahre erhöht sich der Druck auf Unternehmen, schneller und besser produzieren zu können und neue Produkte auf den Markt zu bringen.

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 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 von Systemen, die auf Künstlicher Intelligenz (KI) basieren, stellt in dem Zusammenhang eine besondere Herausforderung dar. Das Erlangen von Informationen über technologische Fortschritte kann einerseits Gegenstand von Spionage sein, andererseits können KI-basierte Tools auch für Spionagezwecke eingesetzt werden.

Insbesondere seit Beginn des russischen Angriffskrieges gegen die Ukraine sind Unternehmen der Rüstungsindustrie und deren Zulieferer sowie Unternehmen, die als Kritische Infrastruktur (KRITIS)

gelten, in den Fokus geraten. Hier steht weniger die Spionage als vielmehr die Sabotage im Vordergrund.

Niedersächsische Unternehmen verzeichnen mit ihren Spitzentechnologien große Erfolge 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, der als Ansprechpartner für die Wirtschaft zur Verfügung steht.
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 umfasst die Themen Wirtschafts- und Industriespionage, Cybersicherheit[191], Know-how-Schutz, Sicherheit in der Informations- und Kommunikationstechnologie, Geheimschutz in der Wirtschaft, Sicherheit auf Geschäftsreisen im Ausland, Innentäterproblematik und Social Engineering[192]. Zahlreiche Unternehmen sind bereits im Rahmen von Vortragsveranstaltungen mit sicherheitsrelevanten Informationen erreicht worden.

191 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).

192 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.

Der Fachbereich Wirtschaftsschutz des Niedersächsischen Verfassungsschutzes ist auch zentrale Ansprechstelle für die Wirtschaft, z. B. bei Fragen des Extremismus und arbeitet eng mit den dafür zuständigen Fachbereichen zusammen.

10.2 Aufgaben und Arbeitsweise

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 dies öffentlich bekannt würde. Dadurch ist auch von einem großen Dunkelfeld von nicht mitgeteilten oder angezeigten Sicherheitsvorfällen auszugehen. Im Jahr 2024 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.

Der Newsletter des Fachbereiches Wirtschaftsschutz informiert die Unternehmen regelmäßig über aktuelle Erkenntnisse, die im Verbund der Verfassungsschutzbehörden gewonnen wurden. Diese Newsletter dienen in erster Linie der Sensibilisierung, aber auch der Weitergabe von Informationen und Hinweisen auf Veranstaltungen.

Nach wie vor ist davon auszugehen, dass soziale Netzwerke wie z. B. Xing, Facebook oder LinkedIn genutzt werden, um im Rahmen von Social Engineering Informationen zu beschaffen, und diese für Cyberangriffe oder Anbahnungen im Bereich der Spionage (HUMINT) zu verwenden. Je mehr im Vorfeld über Adressaten einer (maliziösen) E-Mail bekannt ist, umso besser kann diese formuliert und angepasst werden. Damit

erhöht sich die Wahrscheinlichkeit, dass eine E -Mail für authentisch gehalten und geöffnet wird.

Beratungen, Vorträge, Netzwerkarbeit

Die Arbeit des Fachbereiches Wirtschaftsschutz des Niedersächsischen Verfassungsschutzes umfasst im Wesentlichen Vorträge, gezielte Firmenberatungen sowie eine intensive Netzwerkarbeit. Vorträge werden häufig von den Industrie- und Handelskammern, Wirtschaftsverbänden, Universitäten und kommunalen Wirtschaftsförderungen und von Unternehmen für ihre Mitarbeiterinnen und Mitarbeiter und Führungskräfte nachgefragt. Dabei wird über die Tätigkeit des Verfassungsschutzes berichtet, auf aktuelle Risiken hingewiesen und mögliche Abwehrmaßnahmen aufgezeigt. Es wird generell versucht, für sicherere Abläufe in Unternehmen zu sensibilisieren, z. B. bei organisatorischen Regularien oder baulichen Maßnahmen.

Bei gezielten Firmenberatungen können einzelne Fragestellungen intensiver erörtert und anhand konkreter Situationen und Begebenheiten Lösungsansätze aufgezeigt werden.

Wichtige Netzwerkpartner im Bereich des Wirtschaftsschutzes sind Polizeibehörden, insbesondere die „Zentrale Ansprechstelle Cybercrime für die niedersächsische Wirtschaft“ (ZAC) des Landeskriminalamtes Niedersachsen (LKA NI), das Netzwerk „niedersachsen.digital e. V.“ sowie verschiedene IT-Gesprächskreise der Industrie- und Handelskammern und die Allianz für Cybersicherheit beim Bundesamt für Sicherheit in der Informationstechnik (BSI).

10.3 Unternehmen der Kritischen Infrastruktur (KRITIS)

Eine besonders herausfordernde Aufgabe stellt gerade in unsicheren Zeiten die Aufrechterhaltung des Gemeinwohls dar. Wichtige Bestandteile dafür sind Unternehmen, die als Kritische Infrastruktur (KRITIS) gelten, da deren Anlagen und 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 Konsequenz daraus wäre, dass die Bevölkerung entsprechende Waren bzw. Leistungen nicht mehr beziehen kann und Hunger, Durst, mangelhafte Gesundheits- und/oder Energieversorgung etc. folgt. Der Schutz von KRITIS ist somit eine immens wichtige Aufgabe, die insbesondere mit Beginn des russischen Angriffskrieges gegen die Ukraine stärker in den Fokus geraten ist.
Der Niedersächsische Verfassungsschutz unterstützt die Betreiber von KRITIS in Niedersachsen, indem er in Fragen der Spionage- und Sabotageabwehr berät, um die Versorgungssicherheit möglichst umfassend zu gewährleisten. Die Verbesserung der Inneren Sicherheit für Niedersachsen durch Stärkung der Resilienz in KRITIS-Unternehmen, ist der treibende Faktor, dem auch durch die Mitwirkung in verschiedenen Gremien Rechnung getragen wird.

10.4 Best practice meeting

Das „best practice meeting“ ist ein Veranstaltungsformat für maximal 30 Personen mit einem thematischen Schwerpunkt. Im Anschluss an einen einleitenden Kurzvortrag werden in einer moderierten Diskussionsrunde verschiedene Standpunkte und Erfahrungen ausgetauscht. Aufgrund des bewusst reduzierten Teilnehmerkreises hat sich dieses Format als äußerst effektiv für die Unternehmen erwiesen, weil sich aus den Diskussionen z. B. konkrete Ansätze für umsetzbare Maßnahmen entwickeln können.
Am 15.03.2024 war das Thema „Pre-Employment Screening (PES)“. Darunter sind (Sicherheits-)Überprüfungen zu verstehen, die bereits

während des Bewerbungsprozesses und vor Eintritt der Person in das Unternehmen durchgeführt werden. Das Ziel ist, Personen, die möglicherweise einen Unsicherheitsfaktor darstellen könnten, vorbeugend vom Unternehmen fernzuhalten.
Viele Unternehmen konstatierten den Bedarf, ein PES bei der Besetzung von Schlüsselpositionen zu etablieren und rechtssicher einzusetzen. Mehrere Praktiker berichteten unter verschiedenen Blickwinkeln über ihre Erfahrungen mit der Implementierung eines PES.

10.5 Geheimschutztagung

Vom 10. bis zum 11.04.2024 fand die jährliche Geheimschutztagung des Niedersächsischen Verfassungsschutzes mit etwa 75 Sicherheitsbevollmächtigten der geheimschutzbetreuten Unternehmen sowie Vertreterinnen und Vertretern einzelner Sicherheitsbehörden in Aurich statt.
Im Mittelpunkt der Tagung standen die Themen Wissenstransfer, Vernetzung und der Austausch zwischen am Geheimschutzverfahren beteiligten Behörden, wie dem Bundesministerium für Wirtschaft und Klimaschutz (BMWK), dem Verfassungsschutz und den jeweiligen Unternehmen.

Verfassungsschutzpräsident Dirk Pejril gab einen Überblick über die derzeitige Sicherheitslage und betonte die Herausforderungen im Kontext hybrider Bedrohungen und die damit einhergehenden Desinformationskampagnen.
U. a. berichtete der Geschäftsführer eines von einem Cyberangriff betroffenen weltweit agierenden Unternehmens, wie dieser erfolgreich aufgearbeitet wurde. Der Aufbau einer Notinfrastruktur und die professionelle Betreuung eines externen Cyber-Security-Partners seien wegweisend gewesen.
Weitere Themen waren u. a. Internationaler Geheimschutz, Spionage, Datenschutz und abhörsichere Kommunikation.

10.6 Geheimschutztag

Ergänzend zur zweitägigen Geheimschutztagung fand am 26.11.2024 zum ersten Mal ein Geheimschutztag in Bad Zwischenahn statt, an dem etwa 60 Sicherheitsbevollmächtigte geheimschutzbetreuter Unternehmen teilnahmen.

Zielgruppe sind speziell Vertreterinnen und Vertreter von Unternehmen, die neu mit dieser Thematik konfrontiert sind und umfangreich mit den Grundlagen des Geheimschutzes vertraut gemacht werden. Ergänzt wurde die Informationsveranstaltung mit Beiträgen des Fachbereichs Geheimschutz im Niedersächsischen Verfassungsschutz, des Bundesamtes für den Militärischen Abschirmdienst (BAMAD) sowie eines Unternehmens der Rüstungsindustrie, das über langjährige Erfahrungen im Umgang mit Verschlusssachen verfügt. Zudem hat sich der Fachbereich Prävention vorgestellt und dabei seine Aufgaben sowie Angebote dargestellt, basierend auf der Frage „Was kann ich als Sicherheitsbevollmächtigter eines Unternehmens tun, wenn sich Mitarbeitende des Unternehmens radikalisieren?“

10.7 23. Wirtschaftsschutztagung des Niedersächsischen Verfassungsschutzes

An der 23. Wirtschaftsschutztagung am 11.11.2024 in Hannover nahmen etwa 280 Personen aus Wirtschaft, Wissenschaft und von staatlichen Institutionen teil. Verfassungsschutzpräsident Dirk Pejril eröffnete die Vortragsreihe u. a. mit einem Überblick über hybride Bedrohungen, Desinformationskampagnen sowie Chancen und Gefahren von Künstlicher Intelligenz (KI) und warnte vor der Zunahme russischer Cyber- und Spionageangriffe.

Beim Themenschwerpunkt KI ging es um deren Anwendungsbereiche in der Arbeitswelt und rechtliche Fragestellungen. Weitere Vorträge beschäftigten sich mit Deepfakes und Desinformationen, die den gesellschaftlichen Zusammenhalt erheblich gefährden können, den möglichen Auswirkungen der Präsidentschaftswahl in den USA auf die hiesige Wirtschaft sowie aktuellen Spionagefällen aus Mediensicht.

10.8 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