Wirtschaftsschutz

9. Wirtschaftsschutz

9.1 Einleitung 334
9.2 Aufgaben und Arbeitsweise 336
9.3 Sicherheitstagung für geheimschutzbetreute Unternehmen 339
9.4 Veranstaltung „Desinformation ist falsch“ 340
9.5 Kontaktdaten 341

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 zeitaufwendig 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 den 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.

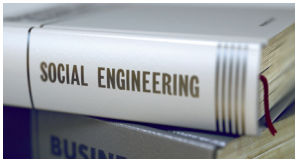
Von diesen Aktivitäten betroffen sind innovative und technologieorientierte Branchen, besonders Bereiche der Informations- und Kommunikationstechnik, der Luft- und Raumfahrt, der Automobilindustrie, der Werkstoff- und Produktionstechnik, der Biotechnik und Medizin, der Nanotechnologie sowie Energie- und Umwelttechnik. Von Interesse sind Produktinnovationen und Marktstrategien. Im Zusammenhang mit der Entwicklung bzw. Anpassung von COVID-19-Impfstoffen ist die Pharmaindustrie inklusive deren Zulieferer derzeit besonderen Risiken ausgesetzt.

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 ist ein Partner für die Wirtschaft.

Die Verfassungsschutzbehörden von Bund und Ländern haben sich auf folgendes gemeinsame 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[153], Know-how-Schutz, Sicherheit in der Informations- und Kommunikationstechnologie, Geheimschutz in der Wirtschaft, Sicherheit auf Geschäftsreisen im Ausland, Innentäterproblematik und Social Engineering[154] wird stark nachgefragt, wie aus den folgenden Abschnitten deutlich wird. So wurden u. a. bereits zahlreiche Unternehmen bei Vortragsveranstaltungen mit sicherheitsrelevanten Informationen erreicht. Im Sinne eines verlässlichen Partners ist der Fachbereich Wirtschaftsschutz single point of contact (SPOC) für die Wirtschaft und damit auch Ansprechpartner bei fachlichen Fragestellungen über die genannten Themengebiete hinaus. So werden z. B. auch Fragestellungen des Extremismus in Absprache mit den jeweiligen Fachbereichen immer wieder in den Beratungsgesprächen thematisiert.



153 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).

154 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.

9.2 Aufgaben und Arbeitsweise

Mittlerweile werden vom Niedersächsischen Verfassungsschutz in den Fachbereichen Geheim- und Wirtschaftsschutz 1.256 Unternehmen betreut.

Beratungen

Zum Kerngeschäft des Fachbereiches Wirtschaftsschutz zählen individuelle Sensibilisierungs- und Informationsgespräche bei den Unternehmen vor Ort, die im Jahr 2021 aufgrund der nach wie vor anhaltenden Corona-Pandemie nur in begrenztem Maße stattfinden konnten. Die Flexibilisierung der Arbeitsmodelle in den Unternehmen führten dazu, dass Beratungen vor Ort und Mitarbeiterschulungen, die zuvor regelmäßig als Mittel zur Sensibilisierung genutzt worden sind, seltener angefragt wurden. Anhand einiger angebotenen Online- oder Hybrid-Veranstaltungen war auch zu erkennen, dass der Fokus in der Hochphase der Pandemie oft nicht auf Fortbildung der Mitarbeiterinnen und Mitarbeiter lag, sondern die Pandemie und die Bewältigung ihrer wirtschaftlichen Auswirkungen die Konzerne dominierte. Insgesamt wurden 56 Beratungen aufgrund spezieller Anfragen durchgeführt (2020 waren es 45, 2019 98).

Insbesondere bei der Sachverhaltsbearbeitung ist es für die Unternehmen hilfreich, dass der Verfassungsschutz nicht dem Legalitätsprinzip unterliegt, also Sachverhalte mit strafrechtlich relevantem Hintergrund nicht zwingend der Staatsanwaltschaft bzw. der Polizei gemeldet werden müssen. Denn im Falle eines Strafprozesses könnte ein Sicherheitsvorfall öffentlich werden und die betroffenen Firmen müssten Imageschäden befürchten.

Häufig war die Informationstechnologie von Unternehmen betroffen. In den meisten Fällen waren Firmennetzwerke durch Schadsoftware manipuliert. Eine nachrichtendienstliche Steuerung dieser Angriffe war nicht auszuschließen.

Noch immer werden Unternehmen in starkem Maße Opfer von Verschlüsselungstrojanern, wie verschiedene Meldungen an den Verfassungsschutz zeigen. In den überwiegenden Fällen geschieht dies per E-Mail. Entweder befindet sich in der E-Mail eine

Verlinkung, die auf eine auf einer Internetseite hinterlegte Schadsoftware führt, oder es wird eine Schadsoftware in einem manipulierten Anhang mitgeschickt. Der als „König der Schadsoftware" (Zitat Arne Schönbohm, Präsident des Bundesamtes für Sicherheit in der Informationstechnik, BSI) bezeichnete Schädling EMOTET wurde dabei in den allermeisten Fällen verwendet.
EMOTET ist z. B. in der Lage, eine bestehende E-Mail-Kommunikation auszulesen und somit 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.
Wurden bis vor einigen Jahren noch sofort nach erfolgter Infektion die Rechner verschlüsselt, so kommt es inzwischen immer häufiger vor, dass vor der Verschlüsselung Unternehmensdaten ausgeleitet werden. Der Schaden für das betroffene Unternehmen ist damit erheblich höher.[155]

Nach wie vor tritt bei Unternehmen häufig der sogenannte Fake-Boss-Angriff oder auch CEO-Fraud auf. Angreifer nehmen in der Regel per E-Mail mit einem zeichnungsbefugten Firmenangehörigen Kontakt auf und täuschen vor, die E-Mail sei vom Vorstand oder aus der Geschäftsführung des Unternehmens. Unter der Vorgabe, es handele sich zum Beispiel um einen geheim zu haltenden Firmenaufkauf oder eine dringend zu tätigende Investition, wird die Mitarbeiterin oder der Mitarbeiter aufgefordert, eine Überweisung – häufig in bis zu sechsstelliger Höhe – in Euro vorzunehmen. In vielen Fällen sind Unternehmen erhebliche Schäden entstanden, weil mangelnde Sensibilität und fehlendes Vieraugenprinzip zu einer Überweisung geführt haben. Nicht unüblich ist auch, dass zusätzlich telefonisch Kontakt zu der angeschriebenen Person aufgenommen wird, um den vermeintlichen Wahrheitsgehalt zu erhöhen. Anrufer ist dann z. B. eine Person, die sich als Rechtsanwalt des Unternehmens ausgibt.
In den Fällen, die dem Fachbereich Wirtschaftsschutz zu den beiden vorgenannten Varianten mitgeteilt wurden, konnte nach eingehender Prüfung kein Verdacht einer nachrichtendienstlichen Tätigkeit

155 Die Serverstruktur hinter EMOTET wurde Anfang 2021 nach umfangreichen Ermittlungen von den Sicherheitsbehörden zerschlagen. Ende 2021 soll die Software allerdings bereits wieder aktiv gewesen sein.

begründet werden. Es handelte sich dann eher um Fälle von Wirtschaftskriminalität.
Über den Newsletter des Fachbereiches Wirtschaftsschutz an seine betreuten Unternehmen in Niedersachsen wurden zahlreiche Warnungen (meist vor elektronischen Angriffen) herausgegeben, die im Informationsverbund der Verfassungsschutzbehörden im Verlauf des Jahres 2021 bekannt geworden sind. Diese Newsletter dienen in erster Linie der Sensibilisierung in den Unternehmen.
Nach wie vor ist davon auszugehen, dass vermehrt soziale Netzwerke (Xing, Facebook, LinkedIn o. a.) genutzt werden, um im Rahmen von Social Engineering Informationen zu beschaffen, und diese im späteren Verlauf für elektronische Angriffe zu verwenden.

Vortragstätigkeit

Im Jahr 2021 hielten Mitarbeitende des Fachbereiches Wirtschaftsschutz 53 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 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 und dort mit der Zentralen Ansprechstelle Cybercrime (ZAC) zusammen.
Durch die fortschreitende Digitalisierung sowie 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. Seit vielen Jahren ist das Netzwerk niedersachsen.digital e.V. (früher Hannover IT 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 Ausschussmitglied im Außenwirtschaftsausschuss vertreten. Außerdem ist er Multiplikator in der Allianz für Cybersicherheit[156] beim „Bundesamt für Sicherheit in der Informationstechnik“.
Eigene Veranstaltungen konnten im Jahr 2021 aufgrund der Corona-Pandemie weiterhin nur sehr begrenzt stattfinden.

9.3 Sicherheitstagung für geheimschutzbetreute Unternehmen

Die für das Frühjahr 2021 geplante jährliche Sicherheitstagung für geheimschutzbetreute Unternehmen wurde in den Herbst des Jahres verschoben und fand vom 05. bis zum 06.10.2021 in Braunlage statt. Etwa 40 Vertreterinnen und Vertreter von Wirtschaftsunternehmen sowie aus Bundes- und Landesbehörden nahmen an der Tagung teil.
Inhaltlich standen die Themen Krisenmanagement (Axel Springer SE), Cybercrime (BMVg) sowie staatlich verantwortete Cyberoperationen (Stiftung Neue Verantwortung e. V.) im Mittelpunkt der Veranstaltung. Darüber hinaus wurde seitens der European Space Agency (ESA) das europäische Satellitennavigationssystem Galileo und seitens der Zentralen Kriminalinspektion Göttingen der Ermittlungskomplex „Krawum“ vorgestellt, infolge dessen ein Online-Netzwerk für den Vertrieb von Sprengstoffen abgeschaltet werden konnte.
Abgerundet wurde die Veranstaltung durch die Darstellung einer Studie des Kriminologischen Forschungsinstituts Niedersachsen (KFN) in Zusammenarbeit mit PricewaterhouseCoopers (PwC) zu Cyberangriffen gegen Unternehmen sowie Ausführungen des BMWi über aktuelle Entwicklungen im Geheimschutz.

156 Siehe Fußnote 151, Kapitel 7.3.

9.4 Veranstaltung „Desinformation ist falsch“

„Was ist Desinformation und wann werden falsche Nachrichten zu einer Gefahr?“ war die zentrale Fragestellung der Veranstaltung am 16.11.2021 in Hannover unter dem Titel „Desinformation ist falsch“. Das Ziel von staatlichen Desinformationskampagnen besteht stets darin, Länder zu destabilisieren und dadurch angreifbar zu machen. Die Basis der Demokratie ist der freie Zugang zu Informationen und die Überprüfbarkeit der Fakten. Die Veranstaltung fand hybrid statt. Während etwa 90 Personen vor Ort teilnahmen, verfolgten sie etwa 200 Personen über den Livestream.

Im ersten Teil der Veranstaltung wurden die technischen Möglichkeiten mittels Deep Fake (Axel Springer Academy of Journalism and Technology), der Einfluss staatlicher Desinformationskampagnen (BMVg) sowie gegen Unternehmen gerichtete Falschinformationen (Complexium GmbH) thematisiert und in einer anschließenden Runde vertiefend diskutiert.

Im zweiten Teil lag der Schwerpunkt auf rechtlichen Vorgaben und Möglichkeiten des Gesetzgebers, gegen Desinformation vorzugehen (Leibniz-Institut für Medienforschung) sowie der Erlangung von Informationskompetenz als Schlüsselqualifikation im Umgang mit Nachrichten und Informationen (Institut für Informationswissenschaft und Sprachtechnologie der Universität Hildesheim). Abschließend wurden auch diese Vorträge in einer Diskussionsrunde zusammengefasst, bei der sowohl Teilnehmerinnen und Teilnehmer vor Ort als auch online die Möglichkeit der Beteiligung gegeben wurde.

9.5 Kontaktdaten

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

Telefon: 0511 6709-284 oder -248
Telefax: 0511 6709-393
E-Mail: wirtschaftsschutz@mi.niedersachsen.de
Internet: www.verfassungsschutz.niedersachsen.de