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 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 und Anpassung eines COVID-19-Impfstoffes ist die Pharmaindustrie inklusive deren Zulieferer besonderen Risiken ausgesetzt.

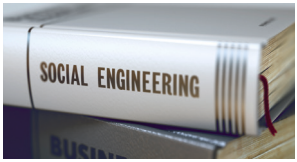
Insbesondere seit Beginn des russischen Angriffskrieges auf die Ukraine sind einerseits Unternehmen der Rüstungsindustrie sowie deren Zulieferer, andererseits aber auch Unternehmen, die als Kritische Infrastruktur (KRITIS) gelten, in den Fokus geraten. Hier stehen weniger Aspekte der Spionage als solche 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 ist ein Partner für die 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[134], Know-how-Schutz, Sicherheit in der Informations- und Kommunikationstechnologie, Geheimschutz in der Wirtschaft, Sicherheit auf Geschäftsreisen im Ausland, Innentäterproblematik und Social Engineering[135] 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.



134 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).

135 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 fast 1.300 Unternehmen betreut.

Beratungen

Zum Kerngeschäft des Fachbereiches Wirtschaftsschutz zählen individuelle Sensibilisierungs- und Informationsgespräche bei den Unternehmen vor Ort. Nachdem diese Gespräche aufgrund der Corona-Pandemie in den Jahren zuvor zurückgegangen waren, wurden diese im Jahr 2022 wieder möglich und von den Unternehmen auch abgefordert. Insgesamt wurden 75 Beratungen aufgrund spezieller Anfragen durchgeführt (2021 waren es 56).

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.

Unternehmen befürchten oftmals einen Imageverlust, wenn die eigene Betroffenheit eines Sicherheitsvorfalls öffentlich bekannt wird. Dadurch bedingt ist auch von einem großen Dunkelfeld vorhandener, aber nicht mitgeteilter/angezeigter Sicherheitsvorfälle auszugehen.

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

Nach wie vor 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 Webseite hinterlegte Schadsoftware 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

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.
Oftmals liegt auch die Infektion mit der Schadsoftware schon längere Zeit zurück, wird aber erst mit Eintreten der Verschlüsselung bemerkt. Dies erschwert die forensische Analyse enorm.
Eine Vielzahl von Cyberangriffen wird durch intensives Social Engineering vorbereitet bzw. begleitet. Je mehr im Vorfeld über den 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.
In den Fällen, die dem Niedersächsischen Verfassungsschutz mitgeteilt wurden, erfolgt zunächst eine Prüfung der möglichen Urheberschaft. Bei einem Verdacht einer nachrichtendienstlichen Tätigkeit erfolgt die weitere Bearbeitung durch den Arbeitsbereich Cyberabwehr des Fachbereiches Spionageabwehr.
Über den Newsletter des Fachbereiches Wirtschaftsschutz wurden zahlreiche Warnungen (meist vor Cyberangriffen) an seine betreuten Unternehmen in Niedersachsen herausgegeben, die im Informationsverbund der Verfassungsschutzbehörden im Verlauf des Jahres 2022 bekannt geworden sind. Diese 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, und diese im späteren Verlauf für Cyberangriffe zu verwenden.

Vortragstätigkeit

Im Jahr 2022 hielten Mitarbeitende des Fachbereiches Wirtschaftsschutz 91 Vorträge bei unterschiedlichen Veranstaltungen (2021 waren es 53). 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 (LKA NI) 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. 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 beim „Bundesamt für Sicherheit in der Informationstechnik (BSI)".

9.3 Unternehmen der Kritischen Infrastruktur (KRITIS)

Die Aufrechterhaltung des Gemeinwohls ist gerade in unsicheren Zeiten eine besonders herausfordernde Aufgabe. Deren sehr wichtige Bestandteile sind Unternehmen, die als Kritische Infrastruktur (KRITIS) gelten, da deren Produktionsanlagen bzw. -systeme von

wesentlicher Bedeutung für die Produktion notwendiger Güter oder Dienstleistungen sind. Ein umfangreicher Lieferausfall dieser Produkte kann in der Regel nicht durch andere Akteure aufgefangen oder ausgeglichen werden.
Mögliche Konsequenzen daraus wären, dass die Bevölkerung entsprechende Waren bzw. Leistungen nicht mehr beziehen können und in nächster Konsequenz Hunger, Durst, mangelhafte Gesundheits- oder/und Energieversorgung etc. folgen können. Der Schutz Kritischer Infrastrukturen ist somit eine immens wichtige Aufgabe, die mit Beginn des russischen Angriffskrieges auf die Ukraine stärker in den Fokus geraten ist. Der Verfassungsschutz leistet seinen Beitrag, um Betreiber Kritischer Infrastrukturen bestmöglich zu unterstützen und die Versorgungssicherheit möglichst umfassend zu gewährleisten.
Der Fachbereich Wirtschaftsschutz pflegt aus o. a. Gründen sehr gute Kontakte zu allen dem Niedersächsischen Verfassungsschutz bekannten KRITIS-Unternehmen in Niedersachsen und berät diese in Fragestellungen zu Spionage- und Sabotageabwehr. 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 hat der Niedersächsische Verfassungsschutz in der Vergangenheit bereits zwei Tagungen für Sicherheitsverantwortliche der KRITIS-Unternehmen durchgeführt, eine dritte Tagung ist für die erste Hälfte 2023 geplant.

9.4 Sicherheitstagung für geheimschutzbetreute Unternehmen

Vom 18. bis zum 19.05.2022 fand die jährliche Sicherheitstagung für geheimschutzbetreute Unternehmen in Garrel statt. Etwa 60 Vertreterinnen und Vertreter von Wirtschaftsunternehmen sowie aus Bundes- und Landesbehörden nahmen an der Tagung teil.

Die Tagung begann mit einem Bericht von Frau Dr. Verena Peters, die stellvertretend für das Bundesministerium für Wirtschaft und Klimaschutz (BMWK) über die neuesten Änderungen und aktuellen Entwicklungen im Bereich der Bearbeitung der geheimschutzbetreuten Unternehmen referierte.

Im Anschluss gab Raoul Classen, beschäftigt bei der DETEK AG, einen Einblick in die Ermittlungsarbeit der Detektei und berichtete über einen Fall, welcher zwischen Hassplattformen und Troll-Communities stattgefunden habe. Seine Schilderungen brachten den Zuhörerinnen und Zuhörern eindrucksvoll nahe, wie schnell im Internet Mobbing, Hass und Verleumdung an Fahrt aufnehmen und Einzelpersonen wie auch Unternehmen das Leben erschweren können.

Frau Prof. Dr. Annika Schach von der Hochschule Hannover (Medien, Information und Design, Abteilung Information und Kommunikation) gab wertvolle Tipps zum Thema Kommunikation in Unternehmen. So führte sie anhand diverser Beispiele den Gästen vor Augen, wie wichtig eine gute Vorbereitung auf verschiedene Störszenarien in der internen Kommunikation und im Umgang mit der Presse sei.

Der Mitarbeiter des Fachbereiches Wirtschaftsschutz beim Verfassungsschutz, Jörg Peine-Paulsen, referierte über die Entwicklungen, die für Unternehmen, Wissenschaft und Politik in den letzten Jahren relevant waren. Von Cyberangriffen über die Lieferkettenproblematik und die Pandemie, die Finanzkrise bis hin zum Angriffskrieg Russlands gegen die Ukraine wurde deutlich: nach der Krise ist vor der Krise. Hier bliebe bzgl. der allgemeinen Unternehmenssicherheit somit nur der Aufruf zur Wachsam- und Betriebsamkeit.

Der Bundesnachrichtendienst (BND) gewährte den Teilnehmerinnen und Teilnehmern Einblicke in ein fremdes Land in schwieriger Lage: Afghanistan. Obwohl die Sicherheitslage dort unter den Eindrücken des Ukraine-Krieges zuletzt etwas aus dem Blick der Berichterstattung gedrängt wurde, sei die Lage dort nicht minder brisant. Der BND berichtete über die aktuelle Lage vor Ort, über Entwicklungen in der Vergangenheit und wagte einen vorsichtigen Blick in eine weiterhin unsichere Zukunft.

Als weitere Referentin des Verfassungsschutzes stellte Nicole Rügenhagen als Leiterin des Referatsteils Spionageabwehr die aktuellen Herausforderungen in ihrem Arbeitsbereich dar. So machte sie beispielsweise deutlich, dass der Bereich der Cyberabwehr im Verfassungsschutz ausgebaut werde und hier eine hohe fachliche Expertise vorhanden und auch von Nöten sei.
Wolfgang Richter von der Stiftung Wissenschaft und Politik, dort der Forschungsgruppe Sicherheitspolitik angehörend, legte Hintergründe zu Russland, der Ukraine und der NATO dar und berichtete über aktuelle Entwicklungen im Kriegsgebiet.
Abschließend rundete Ingo Peters von der Zentralen Kriminalinspektion Oldenburg (Taskforce Cybercrime) die Tagung mit einem Vortrag über den Cyberbunker in Traben-Trarbach ab. Die polizeiliche Bearbeitung des Dark-Market-Verfahrens ziehe ihre Kreise bis in den niedersächsischen Norden. Der Bericht über ein solch umfangreiches Verfahren lieferte einen besonderen Einblick in das Zusammenwirken der jeweils beteiligten Behörden.

9.5 20. Wirtschaftsschutztagung des Niedersächsischen Verfassungsschutzes

Nach einer Schwerpunktveranstaltung zum Thema „Desinformation“ im letzten Jahr fand am 07.11.2022 wieder die alljährliche Wirtschaftsschutztagung statt. Etwa 180 Vertreterinnen und Vertreter größtenteils niedersächsischer Unternehmen nahmen an der Präsenzveranstaltung teil.
Der damalige Niedersächsische Minister für Inneres und Sport, Boris Pistorius betonte in seiner Keynote, dass die Zahl der digitalen Attacken auf niedersächsische Firmen stetig ansteige. Neben Angriffen auf Firmennetzwerke aus kriminellem Antrieb und der daraus resultierenden Erpressung könnten auch politische Motive dahinterstehen. Der Krieg Russlands gegen die Ukraine erfordere bereits eine erhöhte Wachsamkeit,

hinzu käme die Unsicherheit aufgrund des steigenden Einflusses aus China.

Im ersten Teil der Veranstaltung stellte Frau Dr. Diana Kisro-Warnecke von der Nippon Telegraph and Telephone Group (NTT) in ihrem Vortrag „China: Partner, Konkurrent oder systemischer Rivale?" die Chancen und Risiken dar, die der wachsende Handel mit China mit sich bringt. Online dazugeschaltet wurde Frau Sophia Stahl vom Recherchezentrum CORRECTIV, die in ihrem Vortrag „Chinesisches Militär made in Germany" die Zusammenarbeit deutscher Hochschulen und Universitäten mit chinesischen Forschungseinrichtungen darlegte und auf die Gefahr hinwies, dass das Wissen, welches an hiesigen Hochschulen geteilt wird, in China auch in militärische Einrichtungen fließen könne. Dr. Tim Stuchtey, Direktor des Brandenburgischen Instituts für Gesellschaft und Sicherheit (BIGS) schilderte Erkenntnisse des Instituts aus der Studie „Der hohe Preis des Zauderns: Handel unter russischer Aggression", worin die viel diskutierten Kosten des Embargos gegen Russland den Kosten einer eher russlandfreundlichen Politik gegenübergestellt wurden. In einer sich anschließenden Podiumsdiskussion wurden die ineinandergreifenden Themen diskutiert und Fragen aus dem Plenum aufgegriffen.

Im zweiten Teil der Veranstaltung ging es um die „Sicherheit von morgen mit Hilfe von Künstlicher Intelligenz". In diesem Vortrag gab Prof. Dr. Marco Barenkamp von der LMIS AG („Let's make it smarter") einen Einblick über die Möglichkeiten, die in der Nutzung Künstlicher Intelligenz (KI) liegen und wie diese für die Cybersecurity nutzbar gemacht werden können.

Der letzte Fachvortrag kombinierte die Themen KI und Desinformation. Caroline Lindekamp als Head of „noFake" erläuterte die Ansätze des vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Projektes „noFake", das mit Hilfe von KI Falschmeldungen erkennen und zu widerlegen versucht.

9.6 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