Wirtschaftsschutz

10. Wirtschaftsschutz

10.1 Einleitung

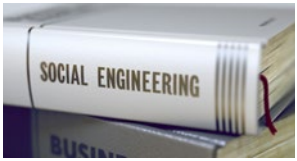
Deutschland ist als technologie- und exportorientierte Nation abhängig von auf Forschung und Erfahrung beruhendem Wissen (Know-how) und Innovation als wertvollste Ressourcen der Volkswirtschaft. Dieses Wissen und diese Informationen sind sowohl für fremde Nachrichtendienste (Wirtschaftsspionage) als auch konkurrierende Unternehmen (Konkurrenzausspähung), die gezielt und professionell Ausspähung betreiben, von höchstem Interesse. Um effektiv Forschung und Entwicklung zu betreiben, bedarf es hervorragend ausgebildeten Personals, zudem sind sie zeitaufwändig und teuer. Mangelt es einem Staat oder einem Unternehmen an einer der genannten Ressourcen, kann versucht werden, sich die fehlenden Erkenntnisse über eine gezielte Ausspähung anzueignen.

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 eines COVID-19-Impfstoffes ist die Pharmaindustrie 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[162], Know-how-Schutz, Sicherheit in der Informations- und Kommunikationstechnologie, Geheimschutz in der Wirtschaft, Sicherheit auf Geschäftsreisen im Ausland, Innentäterproblematik und Social Engineering[163] 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 Aufgaben und Arbeitsweise

Mittlerweile werden vom Niedersächsischen Verfassungsschutz in den Fachbereichen Geheim- und Wirtschaftsschutz 1.238 Unternehmen betreut.

Beratungen

Zum Kerngeschäft des Fachbereiches Wirtschaftsschutz zählen individuelle Sensibilisierungs- und Informationsgespräche bei den Unternehmen vor Ort, die im Jahr 2020 aufgrund der Corona-Pandemie allerdings stark zurückgefahren werden mussten. Insgesamt wurden 45 Beratungen aufgrund spezieller Anfragen durchgeführt (2019 waren es 98).

Für die Unternehmen ist hilfreich, dass der Verfassungsschutz nicht dem Legalitätsprinzip unterliegt, also Sachverhalte mit strafrecht-

162 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).

163 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.

lich 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 mehreren Fällen waren Firmennetzwerke durch Schadsoftware manipuliert. Eine nachrichtendienstliche Steuerung dieser Angriffe war nicht auszuschließen.

In starkem Maße werden Unternehmen 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. Als besondere Schadsoftware ist EMOTET herauszustellen. Einerseits sind von dieser Schadsoftware etliche sich ständig weiter entwickelnde Varianten im Umlauf, andererseits ist EMOTET 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.

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 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 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 vor elektronischen Angriffen herausgegeben, die im Informationsverbund der Verfassungsschutzbehörden im Verlauf des Jahres 2020 bekannt geworden sind.
Nach wie vor ist davon auszugehen, dass vermehrt soziale Netzwerke (Xing, Facebook, LinkedIn o. a.) genutzt werden, um Informationen für elektronische Angriffe im Rahmen von Social Engineering zu beschaffen.

Vortragstätigkeit

Im Jahr 2020 hielten Mitarbeitende des Fachbereiches Wirtschaftsschutz 41 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. Die seit vielen Jahren vom Niedersächsischen Verfassungsschutz begleitete Fokusgruppe Cybersicherheit von Hanno-

ver IT e.V. wurde in diesem Jahr mit dem Arbeitskreis Cybersicherheit der Digitalagentur Niedersachsen zusammengelegt und über die Region Hannover hinaus auf ganz Niedersachsen ausgeweitet. Eine Umfirmierung zum neuen „niedersachsen.digital" e.V. hat in diesem Jahr ebenfalls stattgefunden. Darüber hinaus wirkt der Fachbereich Wirtschaftsschutz im IT-Gesprächskreis der Industrie- und Handelskammer Hannover und bei der interdisziplinären Expertengruppe „Indy4" mit. Außerdem ist er Multiplikator in der Allianz für Cybersicherheit[164] beim „Bundesamt für Sicherheit in der Informationstechnik".

Die Anzahl eigener Veranstaltungen musste im Jahr 2020 aufgrund der Corona-Pandemie ebenfalls stark reduziert werden. Ein für das Frühjahr 2020 geplantes Business-Frühstück des Veranstaltungsformates „Best practice meeting – security2share" konnte nicht durchgeführt werden. Auch die jährlich stattfindende Sicherheitstagung für geheimschutzbetreute Unternehmen musste abgesagt werden.

10.3 19. Wirtschaftsschutztagung des Niedersächsischen Verfassungsschutzes

Die alljährliche Wirtschaftsschutztagung fand am 02.11.2020 virtuell statt. Insgesamt verfolgten 500 Vertreterinnen und Vertreter größtenteils niedersächsischer Unternehmen den Livestream. Im Vergleich zur Vorjahresveranstaltung haben somit mehr als doppelt so viele Interessierte an dieser Wirtschaftsschutztagung teilgenommen. Inhaltlich orientierte sich die Veranstaltung sehr stark an den veränderten Arbeitsbedingungen vor dem Hintergrund der Corona-Pandemie und den daraus resultierenden Herausforderungen.

Der Niedersächsische Minister für Inneres und Sport, Boris Pistorius, betonte in seiner Keynote, wie wichtig es ist, die Gefahren durch

164 Siehe Fußnote 156, Kapitel 8.3.

Cyberkriminalität und die große Bedeutung von IT-Sicherheit und Digitaler Souveränität immer wieder öffentlich zu thematisieren. Denn Cyberkriminelle versuchten mit unzähligen Angriffen und Strategien, die Pandemie und die damit einhergehende Verunsicherung für ihre Zwecke zu nutzen. Bei allen Möglichkeiten, die die Digitalisierung bietet, müsse sie vor allem sicher sein, um bestmöglich vor jeder Art von Angriffen und Spionage zu schützen.

Dr. Jan-Oliver Wagner, CEO Greenbone Networks GmbH, stellte in seinem Vortrag „Digitale Souveränität – Die zunehmende Bedeutung nachhaltiger Widerstandsfähigkeit" heraus, dass die Angreifbarkeit digitaler Netzwerke stetig zunehme, die digitale Widerstandsfähigkeit dabei aber sinke. Dies werde durch vermehrtes Arbeiten im Homeoffice noch verstärkt, wenn vielfach aus Zeitgründen Security-Aspekte bei der Einrichtung dieser Arbeitsplätze außer Acht gelassen werden. Ansprüche an die Sicherheit dürften auch künftig nicht in den Hintergrund geraten.

Johannes Wiggen, Referent für Cybersicherheit, Analyse und Beratung der Konrad-Adenauer-Stiftung e. V., referierte anschließend über „Die Auswirkungen von COVID-19 auf Cyberkriminalität und staatliche Cyberaktivitäten". Die Corona-Pandemie illustriere durch die gestiegene Nutzung digitaler Angebote und den Einsatz weniger geschützter, privater IT-Geräte im Homeoffice digitale Sicherheitsrisiken und verdeutliche die Notwendigkeit adäquater Maßnahmen zum Schutz von IT-Systemen im unternehmerischen Umfeld, besonders aber auch in Kritischen Infrastrukturen[165].

Die anschließende Podiumsdiskussion zum Thema „Videokonferenzen – Menschen sicher miteinander vernetzen?!" bildete den inhaltlichen Schwerpunkt der diesjährigen Tagung. Neben Dr. Jan-Oliver Wagner beteiligten sich Christian Rommert (Digitalunternehmer LeitungsKunst), Klaus Marwede (Datenschutzbeauftragter und CEO niedersachsen.digital Service GmbH) und Andreas Ebert (Leiter Know-how- und Prototypenschutz Volkswagen AG) an dem Panel. Um unter den aktuell geltenden Einschränkungen weiterhin effek-

165 Siehe Fußnote 154, Kapitel 8.3.

tiv arbeiten zu können, sind Unternehmen darauf angewiesen, dass sich Mitarbeiter untereinander austauschen können. Videokonferenzen sind dafür seit Monaten das Mittel der Wahl, allerdings bergen sie einige Gefahren. Sowohl datenschutzrechtliche Aspekte als auch Aspekte des Know-how-Schutzes wurden thematisiert.

Während der gesamten Veranstaltung bestand für die Teilnehmenden die Möglichkeit, online Fragen zu stellen, auf die besonders in der Podiumsdiskussion eingegangen werden konnte. Der rege Zuspruch zu diesem digitalen Veranstaltungsformat zeigt, wie etabliert die Wirtschaftsschutztagung als Informationsforum für Unternehmen ist, allerdings ließ die Online-Veranstaltung die Möglichkeit zum persönlichen Gespräch und besonders den vertraulichen Austausch vermissen.

10.4 Kontaktdaten

Für Fragen steht der Fachbereich 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