Spionageabwehr / Proliferation / Elektronische Angriffe

8. Spionageabwehr / Proliferation / Elektronische Angriffe

8.1 Spionageaufkommen in Niedersachsen

Als Teil der jeweiligen Sicherheitsarchitektur verfügen zahlreiche Staaten über Nachrichtendienste, die Informationen auch mit nachrichtendienstlichen Mitteln sammeln und auswerten. Insbesondere totalitäre Staaten verfügen über Geheimdienste, die auch aktiv Maßnahmen ergreifen, z. B. politisch Einfluss nehmen, Sabotage betreiben oder Attentate verüben. Bei manchen Geheimdiensten kommen auch paramilitärische Abteilungen zur Durchführung von geheimen Kommandounternehmungen zum Einsatz. Bis vor wenigen Jahren wurde die klassische Spionage als Phänomen aus vergangenen Zeiten betrachtet, aber auch im digitalen Zeitalter mit weltweiter Datenvernetzung und rasant voranschreitenden technischen Entwicklungen werben ausländische Nachrichtendienste menschliche Quellen an.

In der Bundesrepublik Deutschland sind der Auslandsnachrichtendienst (Bundesnachrichtendienst [BND]), der Inlandsnachrichtendienst (Verfassungsschutz) sowie der militärische Nachrichtendienst (Bundesamt für den Militärischen Abschirmdienst [BAMAD]) mit der Informationsbeschaffung betraut.

Nachrichtendienste unterliegen in Rechtsstaaten einer Fach- und Rechtsaufsicht durch die vorgesetzten Dienststellen, weil Nachrichtendienste, wie alle staatliche Gewalt, an Recht und Gesetz gebunden sind. Infolge ihrer verdeckten Arbeitsweise und des Interesses von Regierungsstellen an der Informationsgewinnung und Analyseergebnissen wird eine Aufsicht durch Exekutivbehörden selbst oft nicht als hinreichend erachtet. Die Kontrolle wird daher durch parlamentarische Gremien ergänzt. Diese kann durch Debatten, Aktuelle Stunden oder durch parlamentarische Anfragen in und aus den jeweiligen Parlamenten erfolgen.[176]

Das Sachgebiet Spionageabwehr im Niedersächsischen Verfassungsschutz hat den gesetzlichen Auftrag, alle Informationen über sicherheitsgefährdende oder geheimdienstliche Aktivitäten

176 Siehe dazu auch Kapitel 1.6.

zu erheben, zu analysieren und Spionage sowie Proliferation[177] möglichst zu verhindern. Da Niedersachsen als erfolgreicher Wirtschaftsstandort potenzielles Ziel von Spionageaktivitäten fremder Geheim- oder Nachrichtendienste[178] ist, gilt es ihn vor derartigen Aktivitäten zu bewahren. Zudem geht es darum, den Schutz der in Niedersachsen lebenden Bürgerinnen und Bürger zu gewährleisten.

360-Grad-Blick der Verfassungsschutzbehörden

Hauptakteure der klassischen Spionageaktivitäten in der Bundesrepublik Deutschland sind nach wie vor die Russische Föderation, die Volksrepublik China und der Iran. Die Schwerpunkte der Interessen dieser Länder orientieren sich an den politischen Vorgaben und wirtschaftlichen Prioritäten.

Aufgrund desolater Sicherheitslagen in ihren Heimatländern und damit verbundener existenzieller Bedrohungen sucht eine große Zahl von Menschen Zuflucht und Schutz in Europa. Insbesondere Deutschland ist Ziel von Flüchtlingsbewegungen, die ihren Ursprung vor allem in Afghanistan, im Irak, in Syrien sowie in der Ukraine, aber auch in den Ländern Zentral- und Westafrikas haben. Mit der sich vergrößernden Exilgemeinde ist die Ausforschung oppositioneller Aktivitäten zur wichtigen Zielvorgabe für fremde Dienste in Deutschland geworden.

Fremde Geheim- oder Nachrichtendienste sind in unterschiedlicher Personalstärke u. a. an den jeweiligen amtlichen Vertretungen (z. B. Botschaften, Generalkonsulate = Legalresidenturen) in Deutschland präsent und unterhalten dort Stützpunkte. Geheim- und Nachrichtendienstmitarbeitende können dort, als Diplomatinnen und Diplomaten getarnt, tätig werden und Informationen beschaffen oder sie leisten Unterstützung bei geheimdienstlichen Operationen ihrer Zentralen. Außenpolitische Spannungen haben im vergangenen Jahr dazu

177 Proliferation ist die Weiterverbreitung von ABC-Waffen und Trägersystemen; siehe auch Kapitel 8.2.

178 Im Gegensatz zu Geheimdiensten unterliegen Nachrichtendienste einer rechtsstaatlichen Kontrolle und haben keine polizeilichen Befugnisse. Die deutschen Verfassungsschutzbehörden sind demnach Nachrichtendienste. Siehe dazu auch Kapitel 1.7.

geführt, dass Russland vier seiner ehemals fünf Generalkonsulate in Deutschland schließen musste. Als Reaktion auf die Hinrichtung des Deutsch-Iraners Jamshid Sharmahd wurde im Oktober 2024 auch der Iran aufgefordert, seine drei Generalkonsulate in Deutschland zu schließen, was dann ca. vier Wochen später auch erfolgte.

Eine Vielzahl von Informationen, die für fremde Geheim- oder Nachrichtendienste interessant erscheinen und früher nur mit klassischen Spionagetätigkeiten zu erheben waren, sind heutzutage mit relativ geringem technischen Aufwand und fast ohne Aufdeckungsrisiko auf virtuellem Wege zu erlangen. Zum Teil ist aufgrund bestimmter Parameter auch von einer geheim- oder nachrichtendienstlichen bzw. staatlichen Beteiligung auszugehen. Durch die regelmäßige Nutzung identischer Infrastrukturen und der gleichen Vorgehensweisen bei verschiedenen Angriffen, können Angreifer häufig identifiziert werden.
Exemplarisch sind im Folgenden einige Bearbeitungsschwerpunkte der Spionageabwehr des Niedersächsischen Verfassungsschutzes dargestellt.


Logo des SWR

Russland

Der russische Auslandsnachrichtendienst nennt sich Sluschba wneschnei raswedki (SWR, auch SVR, Dienst der Außenaufklärung der Russischen Föderation). Seine Aufgabe ist es, Informationen in den Bereichen Politik, Technologie, Wirtschaft und Wissenschaft zu

beschaffen, um sie sowohl für die Politik als auch die Wirtschaft in Russland nutzbar zu machen.

Einflussnahme und Desinformation

Über seine Spionageaktivitäten hinaus ist Russland bestrebt, Einfluss auf die öffentliche Meinungsbildung und den politischen Diskurs in Deutschland auszuüben. Die Einflussnahme erfolgt sowohl durch staatliche Stellen wie auch durch Einzelpersonen über soziale Netzwerke, Institute, Organisationen und russische Staatsmedien. Oft wird versucht, die wahren Urheber durch Fake-Profile und Social Bots zu verschleiern.

Jede Zielgruppe wird gezielt angesprochen. Dafür werden ganz unterschiedliche Instrumente und Kanäle benutzt. Die Verbreitung russlandfreundlicher Narrative findet über die offiziellen Kanäle statt, dazu gehören z. B. auch Verlautbarungen des Präsidenten selbst oder des Außenministeriums, über die Staatsmedien, die staatsnahen Informationsportale sowie über soziale Medien. Über diese Kanäle verfolgt Russland das Ziel, Ängste und Sorgen z. B. vor Lebensmittel- und Energieknappheit der deutschen Bevölkerung zu schüren und anzuheizen.

Diese Aktivitäten zielen u. a. darauf ab, das Vertrauen in die Stabilität und Handlungsfähigkeit der demokratischen Institutionen und Mechanismen grundsätzlich zu untergraben, die westliche Wertegemeinschaft zu diskreditieren und Bündnisse wie EU sowie NATO zu schwächen.

Die öffentliche Meinung soll im Sinne Russlands beeinflusst und die eigene Machtposition gestärkt werden. Dafür werden auch aktuelle politische und gesellschaftliche Ereignisse sowie Entwicklungen aufgegriffen. So berichten russische Staatsmedien immer wieder einseitig über Demonstrationsgeschehen z. B. in Deutschland. Insbesondere bei der Berichterstattung über Demonstrationen gegen den Ukraine-Krieg versucht Russland über die Verbreitung von Narrativen sein Handeln gegenüber seiner eigenen Bevölkerung und der russischsprachigen Diaspora im Ausland zu rechtfertigen, aber auch, um in der deutschen Bevölkerung Zweifel an der Regierungsfähigkeit der Bundesregierung zu schüren. Auf diese Weise kann mittelbar auf die Meinungsbildung und möglicherweise auf das Wahlverhalten der Bevölkerung in Deutschland Einfluss genommen werden. Nicht

Kreml-genehme Berichterstattung wird in Russland unter Strafe gestellt.
Die massive und anhaltende politische, militärische und wirtschaftliche Unterstützung der Ukraine durch die europäischen Staaten und die USA hat in Russland Reaktionen hervorgerufen, die zu erheblichen Veränderungen der Sicherheitslage in den Unterstützerländern geführt hat.
Die Vorgangsbearbeitung in der Spionageabwehr war im Jahr 2024 im Wesentlichen durch die weltpolitischen Ereignisse, insbesondere durch den russischen Angriffskrieg gegen die Ukraine, geprägt.
Nicht zuletzt deshalb bleibt Russland auch weiterhin ein Schwerpunkt im Fachbereich Spionageabwehr.
Alle deutschen Sicherheitsbehörden stellen sich kontinuierlich aktiv auf die sich stets verändernde Sicherheitslage und die mit dem Russland-Ukraine-Krieg zusammenhängenden Herausforderungen ein. Neben den Aspekten und Auswirkungen „Hybrider Bedrohungen", waren im Wesentlichen die Fachbereiche Rechtsextremismus, Wirtschaftsschutz und Spionageabwehr in diesem Zusammenhang gefordert.

Weitere Ausführungen speziell zum Russland-Ukraine-Krieg finden Sie im Kapitel 2.2, Brennpunktthema „Der Krieg Russlands gegen die Ukraine: Auswirkungen auf Niedersachsen".

China

Um ihren Machtanspruch zu sichern und die eigenen wirtschaftlichen Ziele erreichen zu können, setzt die Volksrepublik China Geheimdienste ein. Von den vier chinesischen Geheimdiensten ist insbesondere das chinesische „Ministerium für Staatssicherheit" (MSS) für die Auslandsaufklärung zuständig. Es gilt als weltweit größter ziviler Geheimdienst.

Die Volksrepublik China bedient sich ihrer Geheimdienste als Mittel zum Regimeerhalt. Übergeordnetes Ziel allen geheimdienstlichen Handelns ist die Aufrechterhaltung des Machtanspruchs der Kommunistischen Partei Chinas (KPCh). China strebt eine aktive Gestaltung der internationalen Ordnung an und propagiert offen das Ziel, im Jahr 2049, dem 100. Gründungsjahr der Volksrepublik,

wirtschaftlich wie militärisch global führend zu sein. Um dieses Ziel zu erreichen, besteht ein allumfassender Informationsbedarf, den China offensiv auch mit geheimdienstlichen Mitteln deckt. Zu den wesentlichen geheimdienstlichen Akteuren zählen der nichtmilitärische In- und Auslandsgeheimdienst MSS[179], der militärische Geheimdienst MID[180], das MÖS[181] sowie der technisch-militärische Geheimdienst NSD[182].

Logo des MSS

China hat sich in Bezug auf den Ukraine-Krieg diplomatisch an die Seite Russlands gestellt. Das Land hat jedoch betont, dass es eine neutrale Position einnehme und sich für eine friedliche Lösung des Konflikts einsetze. Die Weigerung Chinas, den Angriffskrieg Russlands zu verurteilen, hatte bisher keine erkennbaren wirtschaftlichen Nachteile für die Volksrepublik zur Folge.

Gegenwärtig räumen chinesische Geheimdienste, neben den Themen um die Belt-and-Road-Initiative[183] – insbesondere den Entwicklungen im Sektor der Informationstechnologie (Cloud, Internet of Things, Quantentechnologien, Robotik sowie der 5G-Technologie) höchste Priorität ein. Dabei setzen die Dienste auch ausgeklügelte und technologisch anspruchsvolle Cyberoperationen zur Gewinnung von technologischem Know-how, auch für den eigenen Entwicklungsbedarf, ein.
Die Ziele chinesischer Spionage werden nach einer Nutzenkalkulation ausgewählt. Beabsichtigt ist vor allem der Profit für die eigene Nation durch die Informationsbeschaffung. Die Schädigung des Gegners wird von den chinesischen Diensten als zweckdienliches

179 Ministerium für Staatssicherheit = In- und Auslandsgeheimdienst mit Exekutivbefugnissen, Schwerpunkt: Beobachtung oppositioneller Bestrebungen.

180 Militärischer In- und Auslandsgeheimdienst = Abschirmung gegen Aufklärungsversuche, Informationsgewinnung zu ausländischen Streitkräften.

181 Ministerium für öffentliche Sicherheit = Dem Polizeiministerium unterstellt, Bereitstellung geheimdienstlicher Spezialeinheiten.

182 Technisch-militärischer Geheimdienst = Spezialisiert auf Satellitenaufklärung und hochentwickelte Cyberoperationen gegen kritische Infrastrukturen.

183 Der Begriff bezeichnet die Neue Seidenstraße. Sie ist ein langfristiges Projekt der Kommunistischen Partei Chinas zum Aufbau von Infrastrukturen für Transport, Versorgung und Handel. Vorbild sind historische Routen zwischen China und dem Westen, die man erweitert und verändert.

Mittel in Kauf genommen, ist aber oft selbst nicht Ziel des geheimdienstlichen Handelns.

Iran

Die Geheimdienste der Islamischen Republik Iran sind eine wichtige Stütze für das dortige Regime. Das Ministerium für Nachrichtenwesen der Islamischen Republik Iran (MOIS oder VAJA) ist der zivile Auslandsgeheimdienst der Islamischen Republik Iran.

Logo des VAJA

Die Ausspähung der Oppositionellengemeinde ist ein wesentlicher Aufgabenbereich der iranischen Geheimdienste. Die Hinweise erstreckten sich über die Beobachtung irankritischer Demonstrationen bis hin zur konkreten Gefährdung von Einzelpersonen. Der Niedersächsische Verfassungsschutz leitet in diesen Fällen in Zusammenarbeit mit verschiedenen Sicherheitsbehörden entsprechende Aufklärungsmaßnahmen ein.

8.2 Proliferation

Der Begriff Proliferation bezeichnet die Verbreitung atomarer, biologischer und chemischer Waffensysteme sowie deren zugehörige Trägersysteme. Ein zentrales Merkmal der Proliferation ist, dass sie in der Regel nicht von Einzelpersonen, sondern von Staaten betrieben wird, oft unter Einbeziehung ihrer Geheim- oder Nachrichtendienste. Es handelt sich dabei um Länder, von denen zu befürchten ist, dass sie ABC-Waffen in einem bewaffneten Konflikt einsetzen oder deren Einsatz zur Durchsetzung politischer Ziele androhen. Die derzeitigen dynamischen Entwicklungen in regionalen Krisen- und Konfliktgebieten sowie die geopolitischen Machtspiele autoritärer Regime verdeutlichen das wachsende Risiko für die globale sicherheitspolitische Lage.

Broschüre des Bundesamtes für Verfassungsschutz

Die Bundesrepublik Deutschland hat sich, ebenso wie viele andere Staaten, international dazu verpflichtet, den Einsatz und die Verbreitung von

Massenvernichtungswaffen zu verhindern, um das friedliche Zusammenleben der Völker zu sichern. Da Massenvernichtungswaffen und deren Trägersysteme nicht in Gänze auf dem Weltmarkt erhältlich sind, konzentrieren sich proliferationsrelevante Staaten auf den Erwerb einzelner Komponenten.
Im Fokus stehen sogenannte Dual-Use-Güter, also Produkte, Technologien, Software und Know-how, die sowohl zivil als auch militärisch genutzt werden können. Ziel der proliferationsrelevanten Staaten ist es, die militärische Verwendung solcher Güter durch die Vortäuschung eines zivilen Verwendungszwecks zu verschleiern. Durch den Einsatz von Tarnfirmen sowie falsche Angaben zu Ware, Bestimmungsort und Verwendungszweck ist es häufig äußerst schwierig, durch Geheim- oder Nachrichtendienste gesteuerte Beschaffungsaktivitäten zu erkennen.
In den vergangenen Jahren wurde das Aufgabenspektrum der Proliferationsabwehr um den Bereich der sogenannten Emerging Technologies (EMT) erweitert. Hierbei handelt es sich um innovative Entwicklungen und Hochtechnologien, die militärische Konflikte in einem Ausmaß beeinflussen können, das den Auswirkungen von Massenvernichtungswaffen ähnelt. Da die geltenden Exportkontrollgesetze im Bereich EMT oft begrenzt sind, hat der Niedersächsische Verfassungsschutz es sich zur Aufgabe gemacht, durch gezielte Sensibilisierung präventiv tätig zu werden.

Niedersachsen ist ein erfolgreicher Standort von zahlreichen innovativen Unternehmen und Forschungseinrichtungen. Die hier entwickelten und produzierten Güter und Technologien könnten potenziell zur Herstellung oder Weiterentwicklung von Massenvernichtungswaffen genutzt werden. Bei der Beschaffung proliferationsrelevanter Güter gehen die Länder häufig mit großer Kreativität vor, um die geltenden Exportbestimmungen zu umgehen. Unter Nutzung geheim- oder nachrichtendienstlicher Strukturen und bestehender Unternehmensnetzwerke wird versucht, die mit der Lieferung beauftragten deutschen Unternehmen zu täuschen. Um den tatsächlichen Endempfänger zu verschleiern, werden zudem Umweglieferungen über befreundete Nachbarstaaten organisiert. Es hat sich gezeigt, dass proliferationsrelevante Absichten von deutschen Unternehmen und Forschungseinrichtungen als solche oft nicht erkannt werden.

Abgesehen von der Gefahr, die von Massenvernichtungswaffen ausgeht, stellt die Verletzung von Exportbestimmungen eine Ordnungswidrigkeit oder sogar eine Straftat gemäß dem Außenwirtschaftsgesetz, der Außenwirtschaftsverordnung und gegebenenfalls dem Kriegswaffenkontrollgesetz dar.

In den vergangenen Jahren wurde ein solides Netzwerk zu niedersächsischen Unternehmen und Forschungseinrichtungen aufgebaut und kontinuierlich erweitert. Das Netzwerk aus Wissenschaftlern, Exportbeauftragten und den Geheimschutzbevollmächtigten in niedersächsischen Unternehmen tauscht Fachinformationen aus und baut so Hemmschwellen ab. Die vertrauensvolle Zusammenarbeit führte zu einer hohen Sensibilität bei den Gesprächspartnerinnen und Gesprächspartnern und trägt zur Steigerung des Hinweisaufkommens bei.

Die meisten Hinweise betrafen 2024 Russland, China und den Iran.[184]

Das Bestreben der Volksrepublik China im Bereich nach Massenvernichtungswaffen unterscheidet sich grundlegend von anderen Staaten mit ähnlichen Zielen. In Deutschland gibt es weniger relevante Hinweise darauf, dass China gezielt versucht, sich Güter im Zusammenhang mit ABC-Waffen und Trägersystemen zu beschaffen. Aufgrund seines technologischen Fortschritts ist China in diesem Bereich vermutlich weitgehend unabhängig. Im Bereich der sogenannten EMT verfolgt China hingegen mit großem Engagement das Ziel, eine globale Führungsposition zu erreichen. Dafür wird gezielt der deutsche Markt sowie die deutsche Wissenschaftslandschaft genutzt.

China verfolgt ambitionierte Ziele, um die größte Wirtschaftsmacht der Welt zu werden. Um das hierfür notwendige Know-how zu erlangen, macht die Volksrepublik häufig durch den Erwerb vollständiger Unternehmen, durch ein besonderes Engagement im Rahmen wissenschaftlicher Kooperationen und auch durch die gezielte Suche nach sozialer Nähe zu politischen und wirtschaftlichen Entscheidungsträgern auf ihr Interesse aufmerksam. Die

184 Zu den Auswirkungen des Russland-Ukraine-Krieges siehe Kapitel 2.2.

Vorgehensweisen sind vielfältig und unterliegen häufig weder internationalen Sanktionen noch nationalen Exportkontrollen. Dies macht Deutschland besonders anfällig für den Abfluss von Hochtechnologie. Die Problematik wird durch den zivil-militärischen Dual-Use-Charakter vieler sogenannter EMT zusätzlich verschärft.
Der Iran entsendet zahlreiche Gastwissenschaftler an deutsche und auch niedersächsische Universitäten und Forschungseinrichtungen. Es ist jeweils im Einzelfall zu prüfen, ob dies vor dem Hintergrund der Informationsbeschaffung für Massenvernichtungswaffenprogramme erfolgt. Die Sensibilisierung für die Proliferationsproblematik der betreuenden Wissenschaftler erfolgt bei Bedarf und wird regelmäßig vom Niedersächsischen Verfassungsschutz aktualisiert.

Der Niedersächsische Verfassungsschutz leistet Präventionsarbeit durch gezielte Aufklärung und steht als vertraulicher Ansprechpartner zur Verfügung. Durch die enge Zusammenarbeit mit anderen Sicherheitsbehörden trägt er aktiv zur Aufdeckung und Verhinderung proliferationsrelevanter Aktivitäten bei und leistet so auf lokaler Ebene einen bedeutenden Beitrag zur internationalen Sicherheit.

8.3 Cyberabwehr

Die Abhängigkeit unserer Gesellschaft von Informations- und Kommunikationstechnologien steigt. Die dadurch verursachte Verwundbarkeit moderner Gesellschaften stellt eine große sicherheitspolitische Herausforderung dar, denn der mögliche Schaden für Staaten, ihre Bevölkerung und ihre Volkswirtschaften im Falle der Beeinträchtigung von Informations- und Kommunikationsinfrastrukturen ist immens. Staat, Kritische Infrastrukturen[185], Wirtschaft, Wissenschaft und Bevölkerung sind auf das verlässliche Funktionieren dieser Technologien, insbesondere des

185 Kritische Infrastrukturen (KRITIS) sind Organisationen und Einrichtungen von essenzieller Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden (siehe Internetseite des Bundesamtes für Sicherheit in der Informationstechnik, www.bsi.bund.de).

Broschüre des Bundesamtes für Verfassungsschutz

Internets, angewiesen. Cyberangriffe werden zahlreicher, komplexer und professioneller. Häufig kann bei Angriffen weder auf die Identität noch auf die Motivation des Angreifers geschlossen werden; kriminelle, terroristische, militärische und/oder geheim- bzw. nachrichtendienstliche Hintergründe sind denkbar. Die für solche Angriffe häufig genutzten hoch entwickelten Schadprogramme abzuwehren und zurückzuverfolgen, erfordert eine enge Kooperation der Sicherheitsbehörden. Fremde Staaten bedienen sich gezielter Cyberangriffe, um Informationen zu erlangen und das erworbene Wissen zu ihrem Vorteil zu nutzen. Täglich gibt es bundesweit eine Vielzahl an Cyberangriffen, mit dem Ziel der Verschlüsselung und der anschließenden Erpressung der Betroffenen[186]. Auf den einschlägigen Seiten für die Internetsicherheit, wie z. B. auf der Internetseite des Bundesamtes für Sicherheit in der Informationstechnik (https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html) werden die Angriffe statistisch dargestellt. Neben den auch im Jahr 2024 fortgesetzten Angriffen auf Großunternehmen waren in Niedersachsen diverse kleinere und mittelständische Unternehmen, politische Parteien oder auch Privatpersonen betroffen. Das verdeutlicht, welch hohen Stellenwert die IT-Sicherheit in jedem Bereich hat.

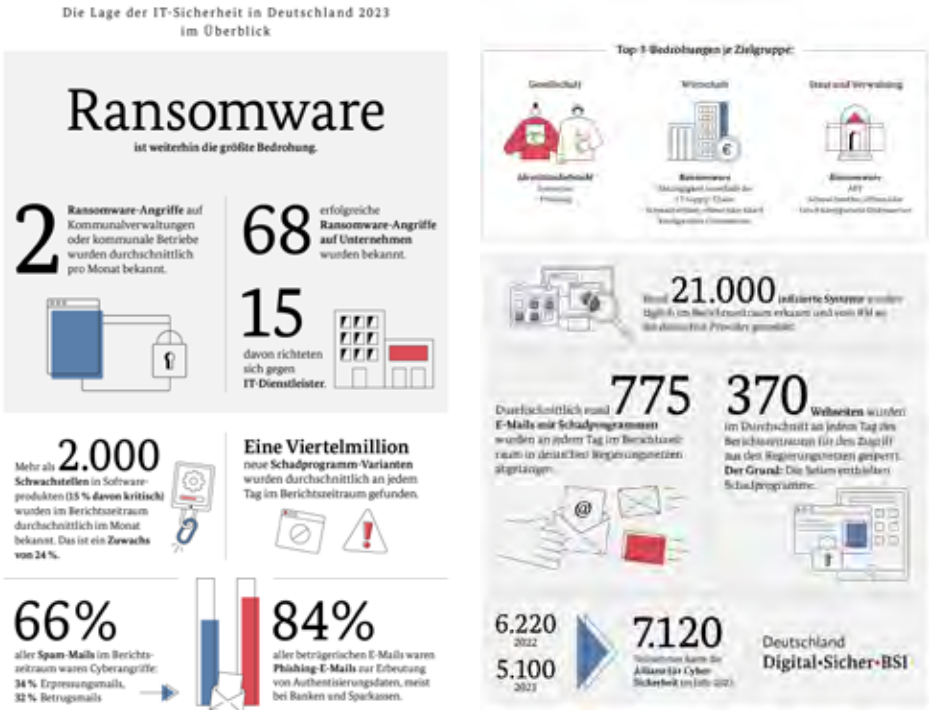
Eine große Gefahr für Unternehmen und Behörden stellen nach wie vor „Advanced Persistant Threats“[187] dar. Diese zielgerichteten Cyberangriffe durch gut organisierte und professionell ausgestattete Hacker, die Anweisungen und Unterstützung in der Regel von Regierungen erhalten könnten, verlaufen typischerweise in mehreren Phasen und sind sehr komplex in der Vorbereitung

186 Auch bekannt als Einsatz von Ransomware (aus dem englischen: ransom für „Lösegeld“).

187 Bei „Advanced Persistant Threats“ handelt es sich um zielgerichtete Cyberangriffe auf spezifisch ausgewählte Institutionen und Einrichtungen, bei denen sich ein Angreifer persistent (=andauernd) Zugriff auf ein System verschafft und auf weitere Systeme ausweitet. Die Angriffe zeichnen sich durch einen sehr hohen Ressourceneinsatz und erhebliche technische Fähigkeiten aufseiten der Angreifer aus und sind in der Regel schwierig festzustellen (siehe Internetseite des Bundesamtes für Sicherheit in der Informationstechnik, www.bsi.bund.de).

und Durchführung. Ziel eines solchen Angriffs ist es, sich möglichst lange unentdeckt in fremden IT-Systemen zu bewegen, um sensible Daten auszuleiten oder anderweitig Schäden anzurichten. Im Gegensatz zu vielen anderen Cyberkriminellen verfolgen diese Angreifer ihre Ziele grundsätzlich langfristig, meist über mehrere Monate oder Jahre hinweg. Sie stimmen ihre Aktivitäten auf die Sicherheitsmaßnahmen ihrer anvisierten Opfer ab und greifen diese oft mehrfach an. Die Bearbeitung solcher Cyberangriffe stellt aufgrund der Anonymität des Angriffs und der nicht erkennbaren Motivation der Angreifer für die Sicherheitsbehörden eine große Herausforderung dar.

Die Abgrenzung zwischen Cybercrime und Cyberspionage ist häufig sehr schwierig, da auch bei einem augenscheinlich in erster Linie bestehenden finanziellen Interesse des Angreifers, wie dem Einsatz von Ransomware, staatliche Akteure im Vorfeld an der



Kompromittierung beteiligt gewesen sein können. Denn auch einem staatlichen Akteur kann eine Verschlüsselung der Systeme des Opfers zur Verschleierung der Aktivitäten und finanziellen Bereicherung dienen.
Auch Hochschulen befinden sich weiterhin im Zielspektrum einiger staatlicher Akteure, deren vorrangiges Ziel es ist, Informationen und Forschungsergebnisse zu erlangen, um sich so einen Wissensvorsprung zu verschaffen oder bestehende Know-how-Lücken zu schließen. In diesem Kontext sind iranische und nordkoreanische Akteure besonders auffällig geworden.

Des Weiteren gab es im vergangenen Jahr in Niedersachsen Verdachtsmomente, wonach staatliche Akteure an Cyberangriffen auf KRITIS beteiligt sind. Diese besonders sensiblen Einrichtungen der Daseinsvorsorge sind aufgrund diverser (gesetzlicher) Vorgaben grundsätzlich gut vor Cyberangriffen geschützt. Jedoch zeigt die Erfahrung, dass keine hundertprozentige Sicherheit zu gewährleisten ist. Erkenntnisse über erfolgreiche Kompromittierungen von Systemen der KRITIS in Niedersachsen durch staatliche Akteure liegen jedoch bislang nicht vor.

Neben direkten Cyberangriffen zum Zweck der Spionage oder Sabotage können häufig kompromittierte Systeme festgestellt werden, die als Bestandteil eines Botnetzes[188] von dem jeweiligen Akteur gesteuert werden. Hierbei handelt es sich meist um kompromittierte Systeme von Unternehmen, Behörden, Parteien oder Privatpersonen. Häufig will der Angreifer ohne Wissen der Betroffenen deren IP-Adresse für weitere Angriffe nutzen. Beim Aufbau eines Botnetzes geht es hauptsächlich um Verschleierungsaktivitäten und Stärkung der eigenen Ressourcen in Form von Rechenkapazität durch die Vernetzung mehrerer PCs. Im Jahr 2024 wurde in Zusammenarbeit mit verschiedenen Sicherheitsbehörden, auch auf internationaler Ebene, ein von russischen

188 Ein Botnet oder Botnetz besteht aus gekaperten IT-Systemen, deren Besitzer und Nutzer in aller Regel nichts davon wissen, dass ihre Rechner ferngesteuert werden. Die heimliche Übernahme des Rechners beginnt mit einer Malware-Infektion. Die Schadsoftware ermöglicht es dem Angreifer, die Kontrolle über das System zu übernehmen, der Computer agiert wie ein Roboter oder kurz Bot. Gesteuert werden die gekaperten Computer meistens über sogenannte Command-and-Control-Server (C2-Server), welche wiederum vom Angreifer gesteuert werden.

Akteuren genutztes Botnetz abgeschaltet. Zum Aufbau des Netzwerks wurden vorwiegend Router eines bestimmten Anbieters mit Schadsoftware versehen, um zu einem späteren Zeitpunkt Cyberspionage- oder Cybersabotagehandlungen zu betreiben. Auch in Niedersachsen wurden diesem Botnetz zugehörige kompromittierte Systeme festgestellt.

Niedersachsen im Fokus von Cyberangriffen

Eine weitere Angriffsmethode staatlicher Akteure sind Supply Chain-Angriffe[189], deren Intention die Manipulation oder Kompromittierung von Lieferketten darstellt. Ein solcher Angriff kann auf verschiedene Arten erfolgen, u. a. durch die Injektion von Schadsoftware in Hardware oder Software während des Herstellungsprozesses, die Kompromittierung von Lieferanten- oder Herstellerdatenbanken oder die Unterwanderung von Drittanbieterdiensten. Die Detektion solcher Angriffe stellt auch Systeme niedersächsischer Unternehmen vor große Herausforderungen, da die Anzahl von Abhängigkeiten zu Softwarebibliotheken und eingesetzten Programmen stetig zunimmt.

189 Bei Supply Chain-Angriffen werden Viren oder andere Schadsoftware über einen Lieferanten oder Drittanbieter verbreitet. Z. B. kann ein Keylogger auf einem USB-Laufwerk bei einem großen Einzelhändler eingeschleust werden und dann Tastenanschläge protokollieren, um Passwörter von Mitarbeiterkonten zu ermitteln.

Die Sicherheitsbehörden beschäftigt auch die voranschreitende Entwicklung Künstlicher Intelligenz (KI), deren Nutzung sowohl positive als auch negative Auswirkungen auf die Sicherheit haben kann. Als Frühwarnsystem für Politik und Gesellschaft ist es Aufgabe des Verfassungsschutzes, die Gefahren solcher Entwicklungen zu bewerten. Staatliche Akteure verwenden KI-Technologie bereits für Desinformationskampagnen, indem mittels KI gezielt gefälschte Nachrichten, Videos oder Bilder generiert werden. Diese Technologie eröffnet auch staatlichen Akteuren neue Handlungsmöglichkeiten und vermag künftig Verfahrensweisen zu vereinfachen oder zu verfeinern.

8.4 Hilfe für Betroffene

Personen, die Opfer eines Anwerbungsversuchs fremder Geheimdienste oder eines elektronischen Angriffs mit vermutetem nachrichtendienstlichem Hintergrund geworden sind, wird geraten, sich an das

Niedersächsisches Ministerium für Inneres und Sport
Verfassungsschutzabteilung
Postfach 44 20
30044 Hannover
Telefon 0511 6709-0

zu wenden.
Weitere Informationen können Sie auch dem Flyer „Spionage – (k)ein Thema?!“ entnehmen, den Sie sowohl auf unserer Internetseite herunterladen, als auch über die vorstehenden Kontaktdaten bestellen können.