Spionageabwehr und Wirtschaftsschutz

Ausländische Nachrichtendienste zeigen weiterhin großes Interesse an Informationen zu Politik, Militär, Wirtschaft, Wissenschaft und Forschung in Deutschland und Nordrhein-Westfalen. Einen großen Stellenwert nimmt zudem auch die Ausspähung von in Deutschland lebenden Oppositionellen ein. So ist die Aufklärung und Ausspähung Oppositioneller beispielsweise eine der vorrangigen Hauptaufgaben des türkischen Nachrichtendienstes (MIT) im Ausland. Dem nordrhein-westfälischen Verfassungsschutz NRW lagen vier Listen vor, in denen Personen, Vereine und Institutionen benannt werden, die von der türkischen Regierung mit der Gülen-Bewegung in Verbindung gebracht werden. Umfang und Inhalt der Listen belegen, dass der MIT systematisch Informationen über mutmaßliche Gülen-Anhänger zusammenträgt.

In 2017 bestand nach wie vor weiterhin ein Interesse mehrerer Staaten am Erwerb von proliferationsrelevanten Gütern in Nordrhein-Westfalen. Dabei handelt es sich um sogenannte Dual-Use-Produkte, die neben ihrer zivilen Bestimmung auch Verwendung in Programmen zur Herstellung von Massenvernichtungswaffen finden können. Damit der eigentliche Empfänger unerkannt bleiben kann, werden solche Beschaffungen üblicherweise durch ein auf mehrere Länder verteiltes Netzwerk aus Tarnfirmen und Strohmännern getarnt.

Die Gefahr Opfer von Wirtschaftsspionage zu werden ist in 2017 weiter angewachsen. Ein Grund dafür ist die immer weiter fortschreitende Digitalisierung in der Wirtschaft und die zunehmende Verzahnung industrieller Produktion mit modernster Informations- und Kommunikationstechnik. Hierdurch wachsen neben ökonomischen Chancen die möglichen Angriffsziele für Cyberangriffe auf deutsche Unternehmen.

Dabei sind nicht nur große, börsennotierte DAX-Unternehmen potentielle Ziele von Angreifern. Häufig werden kleine und mittlere Unternehmen Opfer von Spionage. Dies gilt insbesondere für Firmen, die nicht selten in ihrer Branche auf dem Weltmarkt eine Vorreiterstellung innehaben. Jeder vierte deutsche Weltmarktführer stammt aus Nordrhein-Westfalen. Ihr hohes besonderes technisches Know-how und die hoch innovativen Produkte sind genauso Ziel von Wirtschaftsspionage wie Kalkulationen, Kundenlisten oder andere sensible Daten. Der Schutz gegen Spionage und Sabotage darf sich nicht alleine auf die Sicherung von Informations- und Kommunikationstechnik beschränken. Der Mensch bleibt weiterhin die größte Sicherheitslücke. Awareness zu schaffen, ist daher ein wichtiger Bestandteil einer ganzheitlichen Sicherheitsstrategie, die Technik, Organisation und Personal beinhalten muss.

Der Verfassungsschutz hat im Jahr 2017 seine intensive Beratungs- und Sensibilisierungsarbeit mit zahlreichen Vorträgen und Veranstaltungen bei Unternehmen, Verbänden und Organisationen fortgeführt. Auf 80 Veranstaltungen wurden etwa rund 3.100 Beschäftigte im Management und in Fachabteilungen sowie Manager, Mitarbeiter oder beispielsweise Wissenschaftler erreicht.

Spionage – Auftraggeber, Ziele und Methoden

Im politischen, wirtschaftlichen, wissenschaftlichen oder militärischen Wettbewerb nutzen Regierungen Spionage, um sich einen Informationsvorsprung zu verschaffen. Sie versuchen Zugang zu Informationen zu erhalten, mit denen sich politische Positionen und die wirtschaftliche Wettbewerbsfähigkeit des ausspionierten Staates besser einschätzen lassen. Von Interesse sind zudem Angaben zur militärischen Leistungsfähigkeit gegnerischer Bündnisse.

Wegen seiner politischen und wirtschaftlichen Bedeutung ist Deutschland im besonderen Blick ausländischer Nachrichtendienste. Sie zielen auf einem unautorisierten Transfer wissenschaftlich-technischen Know-hows ab und sind interessiert an Informationen über politische Vorhaben, Krisenmanagement und Handlungsstrategien. Wegen seiner Bedeutung innerhalb der Bundesrepublik beziehen sich diese Bemühungen insbesondere auch auf Nordrhein-Westfalen. Im Land sind 70 Universitäten und Fachhochschulen sowie mehr als 50 Technologiezentren angesiedelt. Es steht für eine herausragende Innovations- und Wirtschaftskraft.

Methoden der Spionage

Fast neunzig Prozent der für Nachrichtendienste interessanten Informationen lassen sich offen über das Internet und andere Medien, durch den Besuch von Messen, bei gegenseitigen Delegationsbesuchen sowie durch geschickte Gesprächsführung mit Informations- und Wissensträgern erlangen. Dazu müssen nicht einmal aufwändige nachrichtendienstliche Operationen durchgeführt werden.

An die verbleibenden rund zehn Prozent versuchen Nachrichtendienste mit verdeckten Methoden zu gelangen. Das Spektrum reicht von der Herbeiführung und Kultivierung zunächst unverdächtiger Kontakte mit dem Ziel einer direkten oder indirekten Abschöpfung der Kontaktpersonen bis hin zu einer konspirativen Vorgehensweise, bei der Personen beispielsweise mit falschem Namen und Angaben zum eigenen Lebenslauf (sogenannte Legende) aktiv sind. Es kommt dabei in der Regel nicht auf die Hierarchieebene der Zielpersonen an. Manchmal geht es lediglich darum, Zugang zu einem interessanten Bereich zu erhalten. In einigen Fällen zielen Nachrichtendienste darauf ab, einen belastenden Umstand – ein sogenanntes Kompromat – zu schaffen, mit dem der jeweilige Informations- und Wissensträger erpressbar gemacht werden soll. Diese Methode wird vorrangig im Ausland, beispielsweise bei Geschäftsreisenden, angewendet.

Nachrichtendienste nutzen zur Spionage aber auch die vielfältigen Möglichkeiten, die sich durch die rasanten Entwicklungen in der Informations- und Kommunikationstechnologie sowie durch die zunehmende Vernetzung und Digitalisierung ergeben. Elektronische Angriffe auf Rechnersysteme mit hochsensiblen Daten bieten hohe Erfolgsaussichten und lassen sich mit geringem Entdeckungsrisiko durchführen.

Typische Angriffsmethoden über IT-Systeme

- Schadhafte E-Mail-Anhänge

  verdecktes Einschleusen von Schadsoftware (Trojanern) über E-Mails

- Drive-by-downloads

  Anbieten von Links auf Webseiten und in E-Mails, die zu manipulierten Downloads führen

- Präparierte Datenträger

  Ausstattung von USB-Sticks, CD-ROM oder Speicherkarten mit Schadsoftware, die bei einer Nutzung automatisch ausgeführt wird

- Umweg über private Geräte

Angriff von häufig weniger geschützten privaten Geräten, die von Mitarbeitern beruflich genutzt werden („Bring-your-own Devices“, beispielsweise USB-Sticks, Smartphones, Tablets).

Außenstehenden gelingt es auf diesen Wegen, in Systeme einzudringen und Daten zu entwenden oder Systeme zu manipulieren. Mit dem digital operierenden „Spion 4.0“ lässt sich zudem bereits seit längerem eine neue Qualität in der Spionage feststellen.

Der Mensch stellt jedoch stets die größte Sicherheitslücke dar. Diese lässt sich selbst durch eine noch so ausgefeilte materielle Absicherung über Firewalls, Anti-Viren-Programme, Passwortschutz und Zugangsregelungen nicht schließen. Nachrichtendienste setzen über sogenanntes „Social Engineering“ an dieser Stelle an. Sie versuchen das Vertrauen eines Unternehmensangehörigen zu gewinnen, um über diesen Kontakt Zugang zu Systemen zu erhalten. Erkenntnisse belegen, dass aber auch der Spion am Kopierer und mit der Kamera am Zielobjekt weiterhin im Einsatz ist. Wachsamkeit sollte daher auch in dieser Hinsicht weiter bestehen.

Die Zahl nachrichtendienstlichen Personals in sogenannten Legalresidenturen im Bundesgebiet ist auch im europäischen Vergleich anhaltend hoch. Dies verdeutlicht und belegt das hohe Interesse an Informationen aus Deutschland. Legalresidenturen sind getarnte Stützpunkte ausländischer Nachrichtendienste, insbesondere in den diplomatischen und konsularischen Vertretungen, bei staatsnahen Unternehmen oder bei Medienagenturen. Von dort aus entwickelt das nachrichtendienstliche Personal über eigens bereitgestellte Tarndienstposten die geheimdienstlichen Aktivitäten.

Der Einsatz von sogenannten Illegalen dient ebenfalls der Verschleierung nachrichtendienstlicher Tätigkeiten. Dabei handelt es sich um Personen, die als Nachrichtendienstoffiziere von der Zentrale des ausländischen Nachrichtendienstes unter einer Falschidentität eingeschleust werden und häufig über viele Jahre in Deutschland unauffällig leben. Unter diesem Deckmantel führen sie teilweise aufwendige nachrichtendienstliche Operationen aus.

Erkenntnisse der Spionageabwehr

Der nordrhein-westfälische Verfassungsschutz beobachtet mit einem 360-Grad-Blick eine Vielzahl hier tätiger ausländischer Nachrichtendienste. Besondere Bedeutung haben wegen ihrer Aktivitäten die Nachrichtendienste der Russischen Föderation, der Volksrepublik China, der Islamischen Republik Iran und der Türkei.

Im Berichtszeitraum konnten weiterhin zahlreiche Versuche ausländischer Nachrichtendienste beobachtet werden, Kontakte mit Gesprächspartnern aus Politik, Wissenschaft und Wirtschaft aufzunehmen. Dabei wurden verstärkt soziale Netzwerke genutzt. Die nordrhein-westfälische Spionageabwehr führt Sensibilisierungsgespräche mit Personen, die als potenzielle Gesprächspartner erkannter Nachrichtendienstoffiziere in Frage kommen, beziehungsweise bei denen bereits Gesprächskontakte zu diesen bestehen. Gesprächspartnern, die selbst den Verdacht eines nachrichtendienstlichen Hintergrunds vermuten, wird dringend geraten, sich an die Spionageabwehr zu wenden.

Russische Föderation

Die russischen Nachrichtendienste haben nach wie vor ein großes Ausforschungsinteresse an Deutschland und Nordrhein-Westfalen. Sie sind wesentliche Elemente der russischen Sicherheitsarchitektur und einbezogen in die Vorbereitung und Realisierung politischer Vorhaben im In- und Ausland.

Die Informationsbeschaffung durch die russischen Nachrichtendienste erfolgt aus offen zugänglichen Quellen, über menschliche Quellen und über elektronische Angriffe auf Behörden und Wirtschaftsunternehmen. Es werden gezielt Kontakte zu Wissensträgern aus Politik, Wirtschaft und Behörden aufgebaut und schützenswerte Informationen abgeschöpft. Dies geschieht unter anderem bei Urlaubsaufenthalten, beim Besuch von Messen und Fachkongressen oder bei gegenseitigen Delegationsbesuchen. Im Jahr 2017 hat es in Nordrhein-Westfalen weitere Hinweise auf derartige Kontaktversuche gegeben. Es wurde zudem bekannt, dass Polizeibeamte bei Urlaubsreisen an der Grenze zur Russischen Föderation befragt wurden. Von einem nachrichtendienstlichen Hintergrund ist auszugehen. Die Vorfälle wurden zum Anlass genommen, den Polizeibehörden sowie den übrigen Behörden des Landes "Allgemeine Sicherheits- und Reisehinweise insbesondere für Reisen in Staaten mit besonderem Sicherheitsrisiko" an die Hand zu geben.

Die russischen Nachrichtendienste sind gegliedert in einen Inlands-, einen Auslands- und einen militärischen Nachrichtendienst, wobei sich die Zuständigkeiten im Einzelfall überschneiden. Die folgenden Dienste sind auch in Deutschland aktiv:

Inlandsnachrichtendienst - FSB
Der FSB ist unter anderem für die zivile und militärische Spionageabwehr sowie für die Bekämpfung von Terrorismus und organisierter Kriminalität zuständig.

Ziviler Auslandsnachrichtendienst - SWR
Der SWR ist vorrangig für die Aufklärung in den Bereichen Politik, Wirtschaft, Wissenschaft und Technologie zuständig.

Militärischer Auslandsnachrichtendienst - GRU
Aufgabe des GRU ist die Aufklärung des gesamten militärischen Bereichs. Neben der NATO gehört dazu auch die deutsche Bundeswehr.

Volksrepublik China

Die chinesische Regierung ist nach wie vor bestrebt, das das eigene Land an weltpolitischer und wirtschaftlicher Bedeutung gewinnt und sich als führende Wirtschaftsmacht der Welt etabliert. Zur Durchsetzung dieser Ziele nutzt der chinesische Staat in vielfältiger Weise die Arbeit seiner Nachrichtendienste. Nordrhein-Westfalen steht dabei mit seinen hochinnovativen kleinen und mittleren Unternehmen sowie seinen zahlreichen Hochschulen, Forschungseinrichtungen und Technologie- und Gründerzentren im besonderen Fokus nachrichtendienstlicher Aktivitäten.

Wie Russland und Iran nutzt auch China die klassische Methode, Angehörige des eigenen Nachrichtendienstes mit Hilfe von diplomatischen und konsularischen Vertretungen zu tarnen. China bedient sich für den illegalen Wissenstransfer teilweise aber auch der Hilfe hier dauerhaft lebender Chinesen oder von Gastwissenschaftlern, Studenten und Praktikanten, die sich vorübergehend in Deutschland aufhalten. Darüber hinaus konnten im vergangenen Jahr umfangreiche Aktivitäten chinesischer Nachrichtendienste in sozialen Netzwerken festgestellt werden. Dabei wurden beispielsweise im Karrierenetzwerk LinkedIn zahlreiche gefälschte Profile erstellt, mit denen Kontakt zu Mitarbeitern aus Ministerien, Behörden und Hochschulen gesucht wurde. Sie sollten für eine Zusammenarbeit mit der chinesischen Seite gewonnen werden. Der Verfassungsschutz Nordrhein-Westfalen hat daraufhin seine Bemühungen zur Sensibilisierung möglicher Zielpersonen weiter verstärkt.

Der Machterhalt der Kommunistischen Partei sowie die Wahrung der territorialen Integrität Chinas stehen darüber hinaus im Mittelpunkt der Staatsführung. Diese sieht sich in erster Linie durch die sogenannten "Fünf Gifte" bedroht. Gemeint sind damit die Demokratiebewegung, Anhänger eines unabhängigen Taiwan sowie eines unabhängigen Tibet, Falun-Gong-Anhänger und turkstämmige (muslimische) Uiguren. Angehörige dieser Bestrebungen und Vereinigungen werden sowohl im In-, als auch im Ausland verfolgt.

Islamische Republik Iran

In Nordrhein-Westfalen, wie im gesamten Bundesgebiet, gehen die nachrichtendienstlichen Aktivitäten des Iran vor allem vom "Ministry of Information and Security" (MOIS) aus. Beim MOIS handelt es sich um den zivilen In- und Auslandsnachrichtendienst der islamischen Republik Iran. Dieser beobachtet schwerpunktmäßig im Exil agierende Oppositionskräfte, insbesondere die in Nordrhein-Westfalen stark vertretene "Volksmodjahedin Iran-Organisation" (MEK) und deren politischen Arm, den "Nationalen Widerstandsrat Iran" (NWRI). Das MOIS versucht, die Exilopposition durch Infiltration zu überwachen und durch gezielte Propaganda zu diskreditieren. Darüber hinaus spielen für den Iran klassische Spionageziele wie Politik, Militär, Wirtschaft und Wissenschaft eine bedeutende Rolle.

In Nordrhein-Westfalen, wie auch bundesweit, wurden verstärkt Aktivitäten der sogenannten "Quds Force Brigade" (QF) festgestellt. Bei den QF handelt es sich um eine Spezialeinheit der Revolutionsgarden, die über eine eigene nachrichtendienstliche Abteilung, einen Sicherheitsdienst und eine Spionageabwehr verfügen. Die QF betreibt unter anderem Informationsbeschaffung im Ausland. Ein Hauptaugenmerk liegt in der Ausspähung von israelischen und pro-israelischen Institutionen, hier lebenden Staatsangehörigen des Staates Israel sowie

Personen jüdischen Glaubens. Dem Verfassungsschutz Nordrhein-Westfalen liegen Erkenntnisse vor, dass es im Berichtsjahr Ausforschungsaktivitäten der QF in Nordrhein-Westfalen gegeben hat.

Türkei

Der türkische Nachrichtendienst "Millî Istihbarat Teşkilâtı" (MIT) ist sowohl für die In- als auch die Auslandsaufklärung zuständig. Er ist mit Exekutivbefugnissen ausgestattet. Die Befugnisse und Aufgaben des MIT wurden im Zuge der Reformen der vergangenen Jahre weiter ausgeweitet.

Der MIT unterhält in Deutschland Legalresidenturen in offiziellen Repräsentanzen. In Nordrhein-Westfalen befinden sich insgesamt vier der 13 türkischen Generalkonsulate auf deutschem Boden (Düsseldorf, Essen, Hürth und Münster). Als einer der weltweiten Schwerpunkte der türkischen Diaspora gilt Nordrhein-Westfalen als Operationsgebiet des türkischen Nachrichtendienstes.

Die Aufklärung und Ausspähung Oppositioneller ist eine der Hauptaufgaben des MIT im Ausland. Neben den kurdischen Gruppierungen wie der **Arbeiterpartei Kurdistans** (**PKK**), linksextremistischen Organisationen wie die **Revolutionäre Volksbefreiungspartei-Front** (**DHKP-C**) und die "Marxistisch-Leninistische Kommunistische Partei" (MLKP) gilt die nach dem Prediger Fetullah Gülen benannte "Gülen-Bewegung" als oppositionell.

Dem nordrhein-westfälischen Verfassungsschutz lagen im Berichtszeitraum vier Listen vor, die durch die türkische Regierung an die Bundesregierung übergeben wurden. In diesen Dokumenten sind Personen sowie Vereine und Institutionen benannt, die von der türkischen Regierung mit der Gülen-Bewegung in Verbindung gebracht werden. Umfang und Inhalt der Listen belegen, dass der MIT systematisch Informationen über mutmaßliche Gülen-Anhänger zusammenträgt. Alle Personen und Institutionen aus Nordrhein-Westfalen wurden von der nordrhein-westfälischen Polizei über den Umstand informiert, dass sie auf den Listen geführt werden. Sie wurden zudem auf sich daraus möglicherweise ergebende Konsequenzen, etwa bei Einreisen in die Türkei, hingewiesen.

Kostenloses Angebot des Verfassungsschutzes

Zur Sensibilisierung vor den Gefahren nachrichtendienstlicher Tätigkeit führt der nordrhein-westfälische Verfassungsschutz auf Wunsch und auch unabhängig von konkreten Verdachtsfällen Informationsveranstaltungen für interessierte Unternehmen und Organisationen durch. Im Einzelfall berät er vertraulich, wenn sich Anhaltspunkte für den Verdacht eines Angriffs durch einen fremden Nachrichtendienst ergeben.

Anfragen mit der Bitte um Kontaktaufnahme können an kontakt.verfassungsschutz@im1.nrw.de gerichtet werden.

Aufklärung und Abwehr von Proliferation

Bis heute ist es Staaten wie Iran, Nordkorea, Syrien und Pakistan nicht gelungen, die zur Weiterentwicklung der eigenen Waffenprogramme erforderlichen Güter ausschließlich im eigenen Land herzustellen. Nordrhein-Westfalen als starker Wirtschaftsstandort mit einer Vielzahl relevanter Unternehmen und Forschungseinrichtungen stand daher im Jahr 2017 weiterhin im Fokus proliferationsrelevanter Beschaffungsstellen.

Proliferation

Unter Proliferation wird die Weiterverbreitung atomarer, biologischer oder chemischer Massenvernichtungswaffen beziehungsweise der zu ihrer Herstellung verwendeten Produkte verstanden. Dazu gehören entsprechende Waffenträgersysteme und das für deren Betrieb erforderliche Know-how. Bei proliferationsrelevanten Staaten steht zu befürchten, dass Massenvernichtungswaffen in Konflikten eingesetzt oder als politisches Druckmittel genutzt werden.

Proliferationsrelevante Güter und Beschaffungswege

Staaten, die Proliferation betreiben, interessieren sich in der Regel für sogenannte Dual-use-Güter. Das sind Produkte, die sich sowohl im zivilen als auch im militärischen Bereich verwenden lassen. Bei entsprechenden Anfragen wird gegenüber Herstellern oder Händlern anstatt der tatsächlich vorgesehenen Endverwendung eine angeblich angestrebte zivile Nutzung vorgegeben. Das eigentliche Ziel der Lieferung wird verschwiegen und eine Lieferadresse in einem auf den ersten Blick unverdächtigen Land vorgeschoben.

Im vergangenen Jahr nutzten die Proliferationsstaaten erneut umfangreiche Beschaffungsnetzwerke, bestehend aus Tarnfirmen und Strohmännern in unterschiedlichen Staaten. Für diese Umgehungslieferungen können entsprechende Einkäufer jedes beliebige Land nutzen. Häufig liegen „Umgehungsstaaten“ jedoch in geographischer Nähe zum Zielland.

Aufklärung durch den Verfassungsschutz

Die Spionageabwehr des nordrhein-westfälischen Verfassungsschutzes bemüht sich um eine kontinuierliche Ausweitung der Aufklärungsbemühungen im Bereich der Proliferation. Sie sensibilisierte im Jahr 2017 erneut zahlreiche Unternehmen mit Vorträgen und Einzelberatungen, mit Erfolg für die Proliferationsbekämpfung. Die Gesprächspartner in den Unternehmen werden auf Gefahren illegaler Lieferungen sowie die einschlägigen Beschaffungsmethoden hingewiesen. In konkreten Einzelfällen bietet der Verfassungsschutz eine individuelle und vertrauensvolle Beratung, bei der Probleme und Fragen der Unternehmen stets vertraulich behandelt werden.

Eine erhöhte Sensibilität in der Wirtschaft führt zu einer Zunahme von Hinweisen auf mögliche Anbahnungen mit Proliferationshintergrund und letztlich zu einem Anstieg der Fälle, in denen Beschaffungsnetzwerke identifiziert und geplante Proliferationsgeschäfte rechtzeitig verhindert werden können.

Entwicklungen im Berichtsjahr

Mit dem Inkrafttreten des Atomabkommens mit dem Iran im Jahr 2016 war ein starker Rückgang entsprechender iranischer Beschaffungsversuche zu verzeichnen. Wegen der Nachfrage nach relevanten Gütern für seine Raketenprogramme stellt der Iran dennoch weiterhin den Bearbeitungsschwerpunkt in der Proliferationsabwehr dar. Es konnte darüber hinaus eine steigende Anzahl pakistanischer Beschaffungsversuche festgestellt werden. In der überwiegenden Zahl der Fälle erfolgte jedoch keine Auslieferung der jeweiligen Waren. Der Verfassungsschutz konnte die betroffenen Unternehmen rechtzeitig warnen und bereits sensibilisierte Firmen erkannten verdächtige Anfragen und bedienten diese nicht.

Wirtschaftsspionage und Konkurrenzausspähung

Wirtschaftsspionage ist die staatlich gelenkte oder gestützte, von fremden Nachrichtendiensten ausgehende Ausforschung von Wirtschaftsunternehmen und Betrieben. Unter Konkurrenz- oder auch Industriespionage wird die Ausspähung von Unternehmen durch ein konkurrierendes Unternehmen verstanden.

Für das Jahr 2017 gehen Expertenschätzungen von einem Schaden in Höhe von 55 Milliarden Euro für die deutsche Volkswirtschaft durch Wirtschaftsspionage aus. Aktuelle Umfragen belegen, dass statistisch jedes zweite Unternehmen von einer zielgerichteten Attacke betroffen war. Dabei sind sich nach einschlägigen Studien 76 Prozent der Unternehmen dieser Bedrohungslage nicht bewusst. Vor dem Hintergrund einer immer weiter fortschreitenden Digitalisierung und entsprechender Entwicklungen, die sich unter dem Schlagwort "Industrie 4.0" zusammenfassen lassen, gleichen sich Methoden, Techniken und Angriffsmöglichkeiten von Nachrichtendiensten und Cyberkriminellen immer mehr an. Deshalb wird es immer wichtiger, dass sich die Unternehmen mit umfassenden Sicherheitskonzepten gegen Spionage, Sabotage und Datendiebstahl schützen.

Hierbei unterstützen die Wirtschaftsschutzexperten des nordrhein-westfälischen Verfassungsschutzes. In Sensibilisierungsvorträgen stellen Sie die Bedrohungen dar, denen Unternehmen aller Branchen und Größenordnungen in der heutigen Zeit durch Wirtschaftsspionage ausgesetzt sind. Zusätzlich wird über die wichtigsten, aktuellen Angriffsstrategien informiert und es werden wirksame Schutzstrategien für Unternehmen vorgestellt. Der Verfassungsschutz besucht Unternehmen auf Wunsch vor Ort, um praktische Hilfestellung bei der Erstellung eines Sicherheitskonzeptes zu geben und die Sicherheitsverantwortlichen in einem vertraulichen Gespräch über die aktuellen Bedrohungen zu informieren.

Im Jahr 2017 führten die Mitarbeiter des nordrhein-westfälischen Verfassungsschutzes 80 Beratungen und Vorträge durch. Damit wurden rund 3.100 Zuhörerinnen und Zuhörer erreicht. Zudem wurden auf dem IT-Sicherheitstag der IHK NRW sowie bei Messen in Neuss und Bonn die dortigen Aussteller und Besucher über die Gefahren der Wirtschaftsspionage und das Beratungsangebot des Verfassungsschutzes informiert.

Im Bereich geheimschutzbetreuter Unternehmen haben darüber hinaus gesonderte Einzelfallberatungen und Sensibilisierungsgespräche stattgefunden. Diese Unternehmen sind mit Aufträgen und Projekten befasst, die als Verschlusssachen eingestuft sind. Da bei diesen Firmen von einer erhöhten Bedrohung durch Spionageaktivitäten ausgegangen werden muss, kooperieren der Verfassungsschutz und das Bundesministerium für Wirtschaft und Energie in besonderem Maße bei der Betreuung dieser Unternehmen.

Potenzielle Angreifer

Im Fokus der Spionageabwehr stehen insbesondere Staaten wie die Volksrepublik China, die Islamische Republik Iran und die Russische Föderation. Darüber hinaus ist das Know-how innovativer deutscher Unternehmen auch für weitere - auch westliche - Staaten von großem Interesse. Teilweise gibt es einen gesetzlichen Auftrag für ausländische Nachrichtendienste, deutsche Wirtschaftsunternehmen auszuspionieren, um die Wirtschaft im eigenen Land zu unterstützen.

Häufige Angriffsmethoden

Die häufigste Angriffsvariante bestand im Jahr 2017 weiterhin darin, einer E-Mail Schadsoftware anzuhängen. Dabei handelte es sich in der Regel um sogenannte Trojaner, die sich im Unternehmensnetzwerk festsetzen und anschließend Unternehmensdaten an den Angreifer übertragen. Dies birgt für Unternehmen gerade in der Industrie 4.0 besondere Gefahren. Setzt ein Unternehmen auf die Verzahnung der Produktionsmittel mit modernster Informations- und Kommunikationstechnik, erhöht sich die Zahl der Angriffsmöglichkeiten erheblich. Es lassen sich einzelne Maschinen in einer Fabrik angreifen sowie Produktionsabläufe von außen über das Internet sabotieren und manipulieren.

Professionelle Spionageangriffe werden oftmals überhaupt nicht oder erst sehr spät erkannt. Die durchschnittliche Zeit zwischen Infizierung und Entdeckung beträgt derzeit rund 250 Tage. In dieser Zeit können wichtige Geschäftsgeheimnisse verloren gehen und ein Unternehmen in eine existenzielle Bedrohungslage geraten.

Social Engineering als beliebte Methode

Fremde Nachrichtendienste haben auch in 2017 versucht, mit Hilfe von Social Engineering Zugang zu Unternehmen zu erhalten. Sie versuchen Menschen so zu manipulieren, dass durch ihr Fehlverhalten auf fremde IT-Netzwerke zugegriffen werden kann. Dafür werden bewusst menschliche Eigenschaften wie Hilfsbereitschaft, Gutgläubigkeit und Naivität von Mitarbeiterinnen und Mitarbeitern ausgenutzt. E-Mails werden beispielsweise unter vermeintlich bekannten Namen versendet. Der Inhalt einer Nachricht wird dabei häufig gezielt auf den jeweiligen Beschäftigten des Unternehmens angepasst. Anknüpfungspunkt kann beispielsweise ein Hobby der jeweiligen Zielperson sein. Sie wurde dafür im Vorfeld gezielt beispielsweise in sozialen Netzwerken ausspioniert, auch unter Zuhilfenahme von gefälschten Benutzerprofilen. Der Empfänger einer solchen Nachricht hegt häufig wenig Misstrauen, was die Erfolgsaussichten eines Angriffs erhöht. Die mit einem Trojaner versehene Anlage in einer E-Mail des Angreifers oder ein Link zu einer mit Schadsoftware präparierten Internetadresse werden sorglos geöffnet. Ein Firmennetzwerk kann auf diese Weise mit wenig Aufwand infiltriert werden. Schutzsoftware wird laufend weiterentwickelt und macht es Angreifern schwer. Daher rückt der Faktor Mensch in den Mittelpunkt der Bemühungen, einen unberechtigten Zugang zu einem gut gesicherten IT-Netzwerk zu erhalten. Mitarbeiterinnen und Mitarbeiter werden weiterhin persönlich angesprochen und ausgehorcht, beispielsweise auf Messen oder Fortbildungen.

Reisen ins Ausland

In vielen Unternehmen gehören Dienstreisen zum Arbeitsalltag. Sie bieten Angreifern zahlreiche Ansätze, um wichtige Daten auszuspähen.

Unternehmen sollten sich daher im Vorfeld genau über die Rechts- und Sicherheitslage in Zielländern informieren. Reisen Firmenangehörige beispielsweise mit verschlüsselter Hardware selbst in bestimmte europäische Staaten, drohen ihnen Haftstrafen, wenn sie sich weigern, bei einer Überprüfung die Daten auf dem Rechner zu entschlüsseln. In einer solchen Drucksituation gerät der Einzelne schnell in einen Loyalitätskonflikt. Gibt er das Passwort preis, verstößt er wohlmöglich gegen Regelungen in seinem Arbeitsvertrag. Dies kann als zusätzliches Druckmittel zur weitergehenden Kooperation gegen den Mitarbeiter eingesetzt werden.

Eine Lösung kann der Einsatz eines separaten Smartphones oder Notebooks sein, das nur die für die jeweilige Reise notwendigen Daten enthält. Der Verlust dieser Daten würde zwar immer noch das spezifische Projekt gefährden. Es gäbe jedoch keinen Zugriff auf die Infrastruktur des Unternehmens mit darüber hinausgehenden Geschäftsgeheimnissen.

Ganzheitliches Sicherheitskonzept

Der nordrhein-westfälische Verfassungsschutz rät allen Unternehmen, sich auf der Grundlage eines ganzheitlichen Sicherheitskonzepts zu schützen. Unternehmenssicherheit ist dabei mehr als IT-Sicherheit. Sie gehört in professionelle Hände und sollte von einer eigenen Organisationseinheit (Corporate Security) bearbeitet werden, die alle Sicherheitsprozesse in einem Unternehmen verantwortet und verzahnt. Sicherheit selbst ist zwar kein wertschöpfender Vorgang, sie flankiert aber erfolgreich die Gewinnerzielung und stellt somit einen wichtigen Wettbewerbsvorteil dar. Bei einem einzigen professionellen Angriff kann ein Großteil des Know-how eines Unternehmens abfließen. Unternehmen sollten sich daher sehr frühzeitig mit dem Thema Sicherheit auseinandersetzen. Innovative „Start-Ups“ sollten dies beispielsweise schon in der Gründungphase ihres Unternehmens berücksichtigen.

Kontakt zum Wirtschaftsschutz

Der Verfassungsschutz steht nordrhein-westfälischen Firmen mit einem breiten Sensibilisierungs- und Beratungsangebot zur Seite. Insbesondere kleine und mittelständische Unternehmen werden dabei unterstützt, sich besser vor Spionageversuchen fremder Nachrichtendienste zu schützen.

Für eine Kontaktaufnahme ist das E-Mail-Postfach **wirtschaftsschutz@im1.nrw.de** eingerichtet. Telefonisch sind die Experten des Wirtschaftsschutzes unter 0211 871 2821 erreichbar.

Broschüre für Unternehmen

Die neue Broschüre "Wirtschaftsspionage - So schützen Sie Ihr Unternehmen" des nordrhein-westfälischen Verfassungsschutzes gibt einen Überblick über die vielfältigen Gefahren der Spionage und schlägt jeweils entsprechende Lösungsansätze vor.

Sie kann über die Internetseite **www.im.nrw.de/wirtschaftsschutz** bestellt und heruntergeladen werden.