Beitrag aus: „Sächsischer Verfassungsschutzbericht 2015“

Spionage in Politik und Wirtschaft

Methoden und Arbeitsweisen der ausländischen Nachrichtendienste

Beschaffung offener Informationen

Ausländische Nachrichtendienste können einen großen Teil ihrer Informationen bereits aus offen zugänglichen Quellen gewinnen. Sie ergeben sich beispielsweise bei dem Besuch öffentlicher Tagungen, Vortragsveranstaltungen oder Messen, ebenso wie bei der Lektüre von Werbebroschüren oder Tageszeitungen sowie aus Funk und Fernsehen. Selbst brisante Informationen sind oft ohne Weiteres und völlig legal zugänglich, etwa über Fachzeitschriften und -bücher, über Bachelor-, Master- oder Diplomarbeiten oder über Dissertations- oder Habilitationsschriften, für die im Regelfall sogar eine Veröffentlichungspflicht besteht. Nicht zuletzt erweitert die rasante technische Entwicklung im Bereich der modernen Medien das Spektrum frei zugänglicher Informationen in einem stetig wachsenden Ausmaß. Das reguläre Informationsangebot der öffentlichen Medien bietet fremden Nachrichtendiensten zahlreiche Informationen, die als Grundlage und Ausgangspunkt für weitere Spionageaktivitäten von erheblicher Bedeutung sein können.

Beschaffung nicht öffentlich zugänglicher Informationen

Neben der Beschaffung offener Informationen gehört auch die konspirative Beschaffung von nicht öffentlich zugänglichen Informationen zu den Zielen der ausländischen Nachrichtendienste. Die konspirative Informationsbeschaffung erfolgt in erster Linie über den Einsatz menschlicher Quellen, durch technische Mittel oder durch eine Kombination beider.

Einsatz menschlicher Quellen

Der Einsatz menschlicher Quellen kann unter anderem durch den Aufbau langjähriger persönlicher Kontakte oder durch die unmittelbare Einschleusung in relevante Bereiche geschehen. Der in den letzten Jahren in der Öffentlichkeit prominent gewordene Fall „Anschlag“[1], der in Deutschland zu einem der bedeutendsten Strafverfahren in Spionagesachen führte, belegt das nach wie vor eindrucksvoll.

Nicht in jedem Fall betreiben Nachrichtendienste einen solchen Aufwand. Je nach Einzelfall kommen auch kleiner angelegte Spionageaktionen in Betracht. So treten etwa Mitarbeiter russischer und chinesischer Nachrichtendienste als Diplomaten, Journalisten oder als Mitglieder von Wirtschaftsdelegationen auf, die mögliche Informanten unter anderem auf Tagungen, Fachmessen oder diplomatischen Empfängen zunächst in scheinbar unverfängliche Gespräche verwickeln. Insbesondere chinesische Nachrichtendienste

[1] Der Fall zeigt besonders deutlich eine übliche Vorgehensweise russischer Nachrichtendienste. Das Oberlandesgericht Stuttgart verurteilte ein unter dem Namen Andreas und Heidrun ANSCHLAG auftretendes Agentenpaar unter anderem zu mehrjährigen Haftstrafen wegen geheimdienstlicher Agententätigkeit gegen die Bundesrepublik Deutschland in einem besonders schweren Fall. Das Gericht sah es als erwiesen an, dass die Angeklagten für den russischen Auslandsnachrichtendienst SWR in Deutschland tätig waren.

bedienen sich dabei ihrer Landsleute, die im jeweiligen Ausland als Wissenschaftler, Studenten oder Praktikanten leben und in ihren Arbeitsbereichen über ein erhebliches Wissenspotential verfügen. Wann immer die Agenten fremder Nachrichtendienste mit potentiellen Informanten Kontakt aufnehmen, greifen sie zurück auf die Möglichkeiten zwischenmenschlicher Beeinflussung, um Informationen zu erhalten. Dabei werden oft menschliche Eigenschaften, wie zum Beispiel Dankbarkeit, Hilfsbereitschaft, Habgier, Autoritätshörigkeit, Geltungssucht, Unsicherheit oder Bequemlichkeit, ausgenutzt, um auf diesem Weg Zugang zu sensiblen Daten zu erhalten (sogenanntes „Social Engineering“). Auf eine solche Vorgehensweise deutet auch der bereits im Beitrag „Westliche Dienste“ erwähnte Spionagefall hin, in dem der US-amerikanische Nachrichtendienst CIA einen Spion beim BND installiert haben soll.
Die erlangten Informationen werden auf unterschiedlichste Art und Weise weitergegeben. Nur exemplarisch sei auf die sogenannten Legalresidenturen der Nachrichtendienste in Deutschland verwiesen. Solche Legalresidenturen sind regelmäßig in Botschaften und Konsulaten angesiedelt, wo Mitarbeiter von Nachrichtendiensten als reguläre Mitarbeiter auftreten.

Einsatz technischer Mittel, insbesondere „Elektronische Angriffe“

Die Informationsbeschaffung durch den Einsatz technischer Mittel, insbesondere über moderne Kommunikationsmedien, wird in Zukunft weiter an Bedeutung gewinnen. Das gilt umso mehr, als auch öffentlich nicht zugängliche Informationen im neuen digitalen Zeitalter oft leicht und ohne größere Risiken erlangt werden können. Fremde Nachrichtendienste können diese Möglichkeiten nutzen und Kommunikationsverbindungen vor allem über Internetknoten und Server im Ausland abhören. Darauf deuten die Erkenntnisse um die Abhörpraktiken der US-amerikanischen NSA und des britischen GCHQ hin. In dieselbe Richtung weist die Entwicklung in Russland, wo die Nachrichtendienste immer mehr Möglichkeiten zur Überwachung und Beeinflussung des Internetverkehrs erhalten, etwa durch Zugriffsmöglichkeiten auf IP- und E-Mail-Adressen, Telefonnummern und Daten aus sozialen Netzwerken oder durch die bereits erwähnten datenschutzrechtlichen Restriktionen im Internet aus dem Jahr 2015.

Neben Abhörmaßnahmen sind „Elektronische Angriffe“, also gezielte Maßnahmen mit und gegen IT-Infrastrukturen, ein probates und wichtiges Mittel der Informationsgewinnung und -beeinträchtigung geworden. Die Möglichkeiten „Elektronischer Angriffe“ reichen vom Ausspähen, Kopieren oder Verändern von Daten (z.B. von Kundenlisten oder Strategiepapieren) über den Missbrauch von Identitäten bis hin zur Übernahme und Sabotage von Produktions- und Steuerungseinrichtungen. Derartige technische Maßnahmen können schnell erfolgen, sie sind kostengünstig und weitgehend risikofrei, auch wenn eine Identifizierung der Urheber durchaus möglich ist. Im Rahmen solcher Angriffe werden klassische Trojaner-E-Mails[2], Wasserloch-Angriffe[3] mit Drive-By-Infektionen[4] und vieles mehr

[2] Als Trojaner-E-Mails gelten hier E-Mails, die zumeist im Anhang eine Schadsoftware enthalten. Diese als nützliche Datei getarnte Schadsoftware wird beim Öffnen der Datei aktiviert, um den betroffenen Rechner dann im Hintergrund zu manipulieren.

[3] Bei Wasserloch-Angriffen (Watering-Hole-Attacs) manipuliert der Angreifer bestimmte Webseiten, bei denen er mit einem Aufruf durch das Opfer rechnen darf. Die Manipulation entfaltet im Regelfall erst dann ihre Wirkung, wenn das Opfer die Seite aufruft.

[4] Eine Drive-By-Infektion ist die Infektion eines Rechners mit Schadsoftware allein durch das Aufrufen einer mit Schadsoftware manipulierten Webseite. Die Manipulation kann ohne Wissen und Wollen des Betreibers geschehen sein. Drive-By-Infektionen sollen in den letzten Jahren weiter an Bedeutung gewonnen und die E-Mail als Hauptverbreitungsweg für Schadsoftware abgelöst haben.

eingesetzt. Ausgangspunkt ist auch hier oft ein ausgefeiltes „Social Engineering“. Das Sächsische Verwaltungsnetz ist seit 2012 nachweislich Ziel „Elektronischer Angriffe“, die auch einen nachrichtendienstlichen Hintergrund haben können. Chinesische Nachrichtendienste stehen im Verdacht, die überwiegende Zahl „Elektronischer Angriffe“ mit einem möglichen nachrichtendienstlichen Hintergrund auf Deutschland initiiert zu haben. Diese Angriffe richteten sich sowohl gegen staatliche Einrichtungen als auch gegen Wirtschaftsunternehmen vor allem aus dem Bereich Rüstung, Satellitentechnik, Maschinen- und Anlagenbau sowie Chemie- und Pharmaindustrie. Daneben führten vor allem russische Nachrichtendienste derartige Angriffe durch. Der Anfang 2015 mutmaßlich von russischen Nachrichtendiensten initiierte „Elektronische Angriff“ auf den Deutschen Bundestag belegt diese Einschätzung eindrucksvoll. In diesem Zusammenhang hat sich besonders deutlich gezeigt, dass sich ein „Elektronischer Angriff“ keineswegs in einer einmaligen punktuellen Maßnahme erschöpfen muss, sondern zu einer länger andauernden, komplexen und herausfordernden Bedrohung heranwachsen kann, die mit großem Aufwand betrieben wird (sogenannter „Advanced Persistent Threat“ [APT]).
Besondere Brisanz erhalten „Elektronische Angriffe“ letztendlich dadurch, dass sie selbst bei ausgeprägtem Sicherheitsbewusstsein der Betroffenen und trotz der Benutzung aktueller Schutzprogramme gegen Schadsoftware oft über längere Zeit nicht erkannt werden.

Beeinflussung der öffentlichen Meinung

Fremde Nachrichtendienste haben 2015 neben der Beschaffung von Informationen erneut versucht, die öffentliche Meinung in Deutschland und damit auch im Freistaat Sachsen zu beeinflussen. Das Portfolio der dafür eingesetzten Mittel hat sich verbreitert und reicht von dem bereits aus der Vergangenheit bekannten Einsatz von Einflussagenten über den zielgerichteten Aufbau und die Pflege von Kontakten zu Multiplikatoren in Politik und Wirtschaft bis hin zu regelrechten Propagandaoffensiven im Internet.

Der vor allem aus dem Kalten Krieg bekannte Einsatz von Einflussagenten dient zum einen der Desinformation der Bevölkerung in den Heimatländern. Die hierbei von den Einflussagenten bevorzugt in Presse, Rund- und Fernsehfunk abgegebenen Erklärungen haben das Ziel, die Politik ihrer Heimatländer zu unterstützen. Die Bevölkerung soll annehmen, dass „Experten“ im Ausland die eigene Regierungspolitik befürworten.
Der Einsatz von Einflussagenten kann aber auch der Einflussnahme auf relevante Entwicklungen in Deutschland und Sachsen dienen. Solche Aktivitäten haben aufgrund der aktuellen politischen Entwicklung insbesondere für die russischen und die chinesischen Nachrichtendienste wieder an Bedeutung gewonnen.

Die erstmals im Jahr 2015 in solcher Intensität feststellbaren Propagandaoffensiven im Internet hatten vor allem einen russischen Hintergrund und dürften der prekären außenpolitischen und wirtschaftlichen Lage der Russischen Föderation geschuldet gewesen sein. Zum Einsatz kamen sogenannte „Internettrolle“, Personen, die sich gegen Bezahlung in sozialen Netzwerken, in Kommentaren auf Internetseiten und Blogs positiv zur Politik der Staatsführung positionieren und gleichzeitig deren Gegner verunglimpfen. Nach der offensichtlich professionellen Analyse von Rankingregeln im Internet gelang es etwa, durch massenhafte Posts eine russlandfreundliche Sichtweise auf die vorderen Plätze bei den meistdiskutierten Themen zu lancieren.