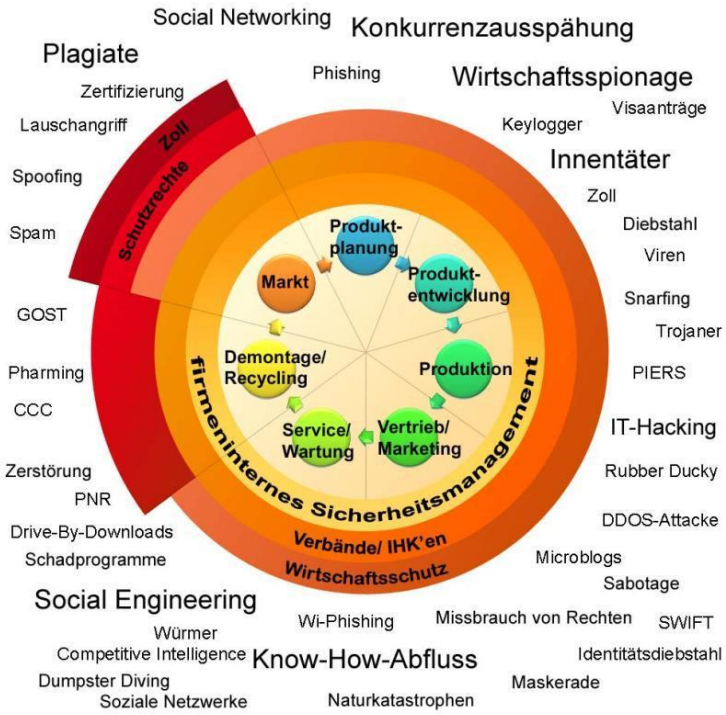
Wirtschaftsspionage
Angriffsvektoren auf die Berliner Wirtschaft

Bedingt durch den Zerfall des kommunistischen Machtbereichs und der einsetzenden Globalisierung der Weltwirtschaft in den 1990er Jahren hat sich seither der Fokus staatlich gelenkter Spionagetätigkeit deutlich verschoben.
Standen zuvor in erster Linie sensible Informationen aus den Bereichen Politik und Militär auf der Agenda fremder Nachrichtendienste, ist nunmehr insbesondere auch das Know-how von Wirtschaftsunternehmen gefragt.
Angetrieben durch die Entwicklung neuer Märkte und moderner Kommunikationstechniken haben sich die Nachrichtendienste vieler Länder im Zeichen der Globalisierung entsprechend neu ausgerichtet.

Diese Entwicklung gefährdet insbesondere auch die Sicherheit von deutschen Unternehmen.

Ausländische Nachrichtendienste versuchen den technologischen Rückstand ihrer Auftrag gebenden Staaten durch die illegale Beschaffung von Wissen aus den Bereichen Wirtschaft, Wissenschaft und Technik auszugleichen.
Als starker Technologie- und Wissenschaftsstandort steht Deutschland dabei mit im Zentrum derartiger Begehrlichkeiten.

Der Vorteil für Staaten mit technologischem Nachholbedarf liegt in diesem Zusammenhang auf der Hand:
Durch den illegalen Zugriff auf das Know-how aus anderen Staaten können erhebliche Summen an eigenen Forschungs- und Entwicklungskosten eingespart und dadurch das fertige Produkt im Zweifel kostengünstiger als im Ursprungsland produziert und so entsprechend erfolgreicher verkauft werden.
Ziel der Spionagetätigkeit ist daher oftmals nicht nur das Produkt selbst, sondern sind vor allem auch die dafür erforderlichen Herstellungstechniken.



Grafik: Wirtschaftsschutz Berlin

Der finanzielle Schaden für die deutsche Wirtschaft ist insgesamt beträchtlich: Eine von Corporate Trust im Juli 2014 durchgeführte Studie zur Industriespionage beziffert den jährlichen Gesamtschaden durch Industriespionage auf ca. 11,8 Milliarden Euro. Berücksichtigt wurden bei dieser Schadensprognose neben den Entwicklungskosten und dem Ausfall des ursprünglich erwarteten Gewinns, auch die Kosten für Rechtsstreitigkeiten und Imageschäden bei Kunden und Lieferanten.

Industriespione, egal ob sie für die Konkurrenz oder für einen fremden Nachrichtendienst arbeiten, nutzen vielfältige Mittel und Methoden. Neben der Auswertung von öffentlich frei verfügbaren Informationen, wie z.B. Datensammlungen im Rahmen von Produktpräsentationen auf Messen und dem Einsatz diverser technischer Aufklärungsmittel, wie z.B. das Abhören von Telefonen und Handys, die von außen auf das angegriffene Unternehmen einwirken, geht jedoch die größte Gefahr vom sogenannten Innentäter im eigenen Betrieb aus. Dabei handelt es sich um hauseigene Mitarbeiter, die Zugang zu den sogenannten Kronjuwelen ihrer Firma haben, also den elementaren Unternehmenswerten, die für den Erfolg und Bestand des Unternehmens unabdingbar sind. Dieser Personenkreis befindet sich in der potentiellen Gefahr, von einem Konkurrenzunternehmen oder einem ausländischen Geheimdienst durch Erpressung oder Bestechung zur Preisgabe seines speziellen Wissens veranlasst zu werden.
Innentäter kann aber auch sein, wer aus reiner Unwissenheit, Leichtfertigkeit oder mangelnder Achtsamkeit Informationen weitergibt, die eigentlich hätten vertraulich bleiben sollen.

Von besonderer Bedeutung sind in diesem Zusammenhang die Gefahren, die von der Methode des sogenannten Social Engineering ausgehen. Unter Social Engineering versteht man das Ausspionieren oder Ausforschen eines Menschen durch die Abklärung seines persönlichen Umfelds; meist durch zwischenmenschliche Beeinflussung, bzw. durch geschickte Fragestellungen.
In der Regel verschleiert der Angreifer seine Identität und verwendet stattdessen eine Legende. Social Engineering hat das Ziel, unberechtigt an vertrauliche Daten, geheime Informationen oder Gegenstände zu gelangen.
Nur 19,8 % der deutschen Unternehmen führen nach Ergebnissen der Studie von Corporate Trust regelmäßig Schulungen für ihre Mitarbeiter durch, um sie für diese Gefahr zu sensibilisieren. In den restlichen Unternehmen wurden die Mitarbeiter noch nie darauf hingewiesen, dass sie beim persönlichen Gespräch, am Telefon und auch im Internet manipuliert werden könnten. Die Unwissenheit der Mitarbeiter ist im Zeitalter der zunehmenden Globalisierung und Digitalisierung ein großes Sicherheitsrisiko. Immer öfter werden von professionellen Tätern menschliche Quellen genutzt, um Hackerangriffe vorzubereiten. Die Kenntnisse über interne Bezeichnungen, Verfahrensabläufe, verwendete IT-Systeme oder Ansprechpartner erleichtert z.B. erheblich die Erstellung eines auf das Zielsystem zugeschnittenen Trojaners und dessen Einbringung in das Firmennetzwerk. Diese Form der Spionage ist sehr effizient, die Gefahr, entdeckt und zur Rechenschaft gezogen zu werden, relativ gering.

Zu den Hauptakteuren auf dem Feld der Wirtschaftsspionage sind vor allem die Volksrepublik China und die Russische Föderation zu zählen.
So möchte China mit dem ehrgeizigen „Projekt 2020“ bis zum Ende des Jahrzehnts die stärkste Wirtschaftsmacht der Welt werden. Die Mitarbeiter der Nachrichtendienste sollen an diesem Projekt einen großen Anteil haben. Sie unterstützen dabei ihre heimische Wirtschaft im offiziellen gesetzlichen Auftrag. Das chinesische Ministerium für Staatssicherheit weiß beispielsweise sehr genau, wo die im Ausland tätigen chinesischen Studenten und Doktoranten eingesetzt werden. Vorrangiges Ziel dieser sogenannten Non-Professionals sind Unternehmen der Hochtechnologie. Branchen wie die Energietechnik, Umwelttechnik oder Biotechnologie stehen besonders im Fokus der Bemühungen.

Auch die russischen Nachrichtendienste unterstützen die heimische Wirtschaft auf der Grundlage eines eindeutigen gesetzlichen Auftrags. Der Auslandsnachrichtendienst SWR mit seinen 13.000 Mitarbeitern ist nicht nur für Politik, sondern auch für Ökonomie, Wissenschaft und Technik zuständig. Der Aufklärungsschwerpunkt russischer Nachrichtendienste ist oft im Bereich der Militärtechnik zu suchen, aber auch andere Wirtschaftszweige sind betroffen.

Die Methoden der Nachrichtendienste sind vielfältig.
Wichtig ist, die Methoden zu kennen und eine Sensibilität dafür zu entwickeln. Wenn dann noch die Schwachstellen im Unternehmen analysiert und so gut wie möglich beseitigt werden, ist es für fremde Nachrichtendienste schwierig, Know-how unbemerkt abzuschöpfen.

Die Verfassungsschutzbehörden des Bundes und der Länder – so auch die Abteilung Verfassungsschutz der Senatsverwaltung für Inneres und Sport Berlin - tragen im Bereich der Wirtschaftsspionage präventiv zum Schutz der deutschen Wirtschaft bei. Spionageabwehr ist eine der Kernkompetenzen des Verfassungsschutzes (siehe hierzu § 5 Abs. 2 Nr. 2 Verfassungsschutzgesetz Berlin-VSG). Vorhandene nachrichtendienstliche Erfahrungen und Analysen aus dem Gesamtspektrum der Spionageabwehr besitzen einen hohen Erkenntniswert auch zur Abwehr der Wirtschaftsspionage.

Die Mitarbeiter des Bereiches Wirtschaftsschutz sensibilisieren als Teil der Öffentlichkeitsarbeit des Berliner Verfassungsschutzes (§ 26 Abs. 1 VSG Berlin) Wirtschaftsunternehmen und Forschungseinrichtungen individuell und kostenlos zum Thema Wirtschaftsspionage. Dabei werden insbesondere Themen des personellen und materiellen Geheimschutzes, sowie die IT-Sicherheit im Unternehmen angesprochen.
In diesem Zusammenhang ist auf den Umstand zu verweisen, dass der Verfassungsschutz bei seiner Tätigkeit weitgehend nach dem Opportunitätsprinzip arbeiten kann und nicht wie die Strafermittlungsbehörden an ein ausschließliches Legalitätsprinzip gebunden ist. Dies bedeutet, dass die Verfassungsschutzbehörde in vielen Fällen nach eigenem Ermessen prüfen kann, ob sie einen ihr von Dritten gemeldeten Sachverhalt an Polizei und Staatsanwaltschaft weiterleitet und damit öffentlich macht oder vorerst in eigener Zuständigkeit bearbeitet.
An uns übermittelte Informationen werden grundsätzlich vertraulich behandelt.

Grafik: Wirtschaftsschutz Berlin

Ansprechpartner im Wirtschaftsschutz

Leiterin des Bereichs: Frau Zitting
Geheimschutzbetreute Wirtschaft: Herr Werder
Technische Beratung: Herr Klink

Tel.: 030/90129-470
Fax: 030/90129-466
E-Mail: wirtschaftsschutz@verfassungsschutz-berlin.de
www.verfassungsschutz-berlin.de