Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Nachrichtendienst des Bundes NDB

PROPHYLAX

Präventions- und Sensibilisierungsprogramm
des Nachrichtendienstes des Bundes

Inhaltsverzeichnis

Proliferation **5**

Risikoländer 6

Exportkontrolle und geltende Rechtsgrundlagen 7

Inwiefern sind Unternehmen, Hochschulen und Forschungsinstitute von Proliferation betroffen? 9

Wissensaustausch und Proliferation 14

Was machen die Behörden? 16

Spionage **19**

Schweizer Unternehmen und Hochschulen als Spionageziele 20

Legale Informationsbeschaffung 21

Spionagemethoden 22

Welchen Bedrohungen sind Unternehmen und Hochschulen durch den Einsatz von IKT ausgesetzt? 28

Wie können sich Unternehmen und Hochschulen vor einem Informations- und Datenabfluss schützen? 31

Sicherheit auf Geschäftsreisen im Ausland 37

Kontakt **42**

Wie kann Sie der NDB unterstützen? 42

Weiterführende Informationen 43

Einleitung

Rund um die Welt geniessen Schweizer Produkte einen sehr guten Ruf. Know-how und Innovationsfähigkeit hiesiger Unternehmen und Forschungseinrichtungen sind Schlüsselfaktoren der Wettbewerbsfähigkeit der Schweizer Volkswirtschaft. Sie bilden die Grundlage einer internationalen Spitzenreiterrolle in vielen Wirtschafts- und Forschungsbereichen. Dieses Know-how und die hier hergestellten Hochtechnologieprodukte ziehen nicht nur das Interesse von Konkurrenzunternehmen auf sich, sondern auch dasjenige ausländischer Staaten. Für viele ausländische Nachrichtendienste gehören die Beschaffung von Produkten und Technologien, die sie wegen Sanktionen und Exportkontrollen auf dem freien Markt nicht erhalten, sowie die Ausforschung fremder Wirtschaftsunternehmen zu den Kernaufgaben.

Um Schweizer Unternehmen und Forschungseinrichtungen auf diese Bedrohungen aufmerksam zu machen, gründete 2004 der damalige Schweizer Inlandnachrichtendienst[1] das Präventions- und Sensibilisierungsprogramm Prophylax. Das Programm erfüllt auch heute noch den gesetzlichen Auftrag, Programme zur Information und Sensibilisierung betreffend Bedrohungen der inneren und äusseren Sicherheit zu führen.[2]

In enger Zusammenarbeit mit den Kantonalen Nachrichtendiensten sensibilisiert der Nachrichtendienst des Bundes (NDB) schweizerische und liechtensteinische Unternehmen, Hochschulen und Forschungsinstitute für die von Spionage und

1 2010 fusionierten der In- und Auslandnachrichtendienst zum Nachrichtendienst des Bundes.
2 Vgl. Art. 6 Abs. 6 des Bundesgesetzes über den Nachrichtendienst (Nachrichtendienstgesetz, NDG) vom 25. September 2015.

Proliferation ausgehenden Bedrohungen. Prophylax verfolgt das Ziel, die Kontrolle von Exporten kritischer und proliferationsrelevanter Güter (namentlich Dual-use-Güter[1]) und Technologien zu stärken, indem illegale Beschaffungsaktivitäten frühzeitig erkannt und verhindert werden. Dies ist deshalb so wichtig, weil die Schweiz einer der weltweit grössten Exporteure von Dual-use-Gütern ist. Mehrere Staaten unterhalten ähnliche Programme zur Sensibilisierung ihrer Wirtschafts- und Technologieunternehmen. Mit Prophylax unterstützt der NDB internationale Bemühungen, die Proliferation von Massenvernichtungswaffen einzudämmen.
Proliferation und Wirtschaftsspionage können enge Verknüpfungen aufweisen. Der NDB und die Kantonalen Nachrichtendienste sensibilisieren Unternehmen und Institutionen auch auf Spionagerisiken, einschliesslich der Bedrohungen durch Cyberspionage. Diese sollen im Umgang mit schützenswerten Informationen umsichtiger werden und so ungewollten Informations- und Datenabflüssen vorbeugen.

1 Doppelt, also im zivilen wie im militärischen Bereich verwendbare Güter.

Proliferation

Definition

Unter Proliferation versteht man die Weiterverbreitung einerseits von Massenvernichtungswaffen sowie deren Trägersystemen (ballistische Lenkwaffen, Marschflugkörper und Drohnen) und andererseits von Ausrüstungsgütern, Materialien und Technologien, die auch zur Herstellung dieser Waffen verwendet werden können (sog. Dual-use-Güter).
Anfänglich wurde der Begriff Proliferation nur auf dem Gebiet der Atomwaffen gebraucht; heute sind die Bereiche der biologischen und chemischen Massenvernichtungswaffen und deren Ausgangsprodukte mitgemeint.

Rechts:
Eine nordkoreanische ballistische Lenkwaffe längerer Reichweite (IRBM) HWASONG-12 beim Start (Zentrale koreanische Nachrichtenagentur, KCNA)

Risikoländer

Die Proliferation ist eine Bedrohung für den Frieden und die Sicherheit weltweit. Sie wird von Ländern betrieben, die aus machtpolitischen Gründen die internationale bzw. regionale Ordnung herauszufordern gewillt sind. Mit der Entwicklung von atomaren, biologischen und chemischen Waffen (sog. ABC-Waffen) sowie deren Trägermitteln versuchen sie, ihre Mittel zur Kriegsführung zu stärken, ihr militärisches Droh- und Abschreckungspotenzial zu erhöhen und politische Forderungen durchzusetzen. Diese Staaten bilden ein Risiko für die internationale Sicherheit und werden deswegen als Risikoländer bezeichnet. Diese Kategorisierung ist nicht nur technisch, sondern auch politisch motiviert und verpflichtet die Staatengemeinschaft, aktive Massnahmen gegen bestimmte Tätigkeiten dieser Länder zu ergreifen. Als Risikoländer gelten heute folgende Staaten: Iran, Nordkorea, Pakistan und Syrien. Diese Staaten unterhalten nachweislich Programme zur Entwicklung von Massenvernichtungswaffen bzw. stellen solche Waffen bereits her. Allerdings sind sie für die Entwicklung, die Herstellung und den Ausbau

bestehender Arsenale auf Güter und Know-how aus dem Ausland angewiesen. Sie versuchen, internationale Kontrollmechanismen mittels klandestiner Beschaffungsaktivitäten zu umgehen, indem sie z. B. den Verwendungszweck eines Produkts verschleiern oder Tarnfirmen gründen. Ferner werden einige Länder wie z. B. Malaysia, die Vereinigten Arabischen Emirate (u. a. Dubai) oder Singapur für proliferationsrelevante Geschäfte als Transitzonen benutzt. Aber auch bei weiteren Staaten, die mutmasslich Ambitionen im Bereich der Proliferation haben, ist besondere Sorgfalt im Geschäftsverkehr angebracht.
Die Forschungs- und Entwicklungsprogramme für Massenvernichtungswaffen und deren Trägersysteme sind in den verschiedenen Risikoländern unterschiedlich weit gediehen. Aus militärtechnischer Sicht wollen diese Länder ihre Programme weiterentwickeln, um ihre Waffenarsenale zu ergänzen, die Lagerungssicherheit zu verbessern sowie die Einsatzmöglichkeiten, die Präzision, die Reichweite und die Effizienz der Waffensysteme zu erhöhen. Ausserdem streben sie eine möglichst weitgehende Unabhängigkeit in der Rüstungstechnik an.

Exportkontrolle und geltende Rechtsgrundlagen

Der Kampf gegen die Proliferation ist Aufgabe der internationalen Gemeinschaft. Die am 28. April 2004 einstimmig verabschiedete Resolution 1540 des UNO-Sicherheitsrats fordert seine Mitgliedstaaten auf, «wirksame Massnahmen zu ergreifen und durchzusetzen, um innerstaatliche Kontrollen zur Verhütung der Verbreitung von nuklearen, chemischen und biologischen Waffen und ihren Trägersystemen einzurichten, einschliesslich angemessener Kontrollen über verwandtes Material». Zu diesem Zweck bestehen auf internationaler Ebene vier sog. Exportkontrollregime. Im Bereich der Bio- und Chemiewaffen existieren darüber hinaus völkerrechtlich verbindliche Übereinkommen, deren Ziel die weltweite Ächtung dieser

Links:
Vermutete Chemiewaffenanlage des Scientific Studies Research Center in Syrien,
die am 07.09.2017 von Israel bombardiert wurde (PLE-Aufnahme vom 24.09.2017)

Waffen ist. Die Schweiz ist Mitglied all dieser Regime und Übereinkommen. Die Schweizer Politik der Rüstungskontrolle und Abrüstung verfolgt das Ziel, die nationale und internationale Sicherheit zu gewährleisten, indem das weltweite Rüstungsniveau auf einem möglichst tiefen Stand gehalten wird. Die Schweiz setzt sich dafür ein, dass Massenvernichtungswaffen nicht weiterverbreitet (Nonproliferation) bzw. vollständig beseitigt werden (Abrüstung). Durch ihre Teilnahme an den internationalen Exportkontrollregimen stellt die Schweiz sicher, dass sie ein solides Glied in der Massnahmenkette gegen die Proliferation ist. Im Zusammenhang mit der Exportkontrolle bestehen in der Schweiz folgende nationale Rechtsgrundlagen[1]:

- Güterkontrollgesetz (GKG); SR 946.202
- Güterkontrollverordnung (GKV); SR 946.202.1
- Chemikalienkontrollverordnung (ChKV); SR 946.202.21
- Kriegsmaterialgesetz (KMG); SR 514.51
- Kernenergiegesetz (KEG); SR 732.1
- Waffengesetz (WG); SR 514.54
- Sprengstoffgesetz (SprstG); SR 941.41
- Embargogesetz (EmbG); SR 946.231
- 24 Verordnungen gestützt auf das Embargogesetz.

1 Siehe auch www.seco.admin.ch (Aussenwirtschaft & Wirtschaftliche Zusammenarbeit → Exportkontrollen und Sanktionen → Rüstungskontrolle und Rüstungspolitik → Rechtliche Grundlagen).

Es ist festzuhalten, dass auch Güter, die in den Exportkontrollregimen nicht explizit aufgelistet werden, einer Melde- und Bewilligungspflicht unterstehen, wenn der Exporteur weiss oder Grund zur Annahme hat, dass ein Gut für die Herstellung oder den Einsatz von Massenvernichtungswaffen bestimmt ist (Catch-all-Klausel). Ferner erfasst die Exportkontrolle auch bestimmte Technologien.
Proliferationsaktivitäten in der Schweiz können nicht nur gegen nationales Recht oder völkerrechtliche Verpflichtungen verstossen, sondern auch die aussen- und handelspolitischen Beziehungen und die Glaubwürdigkeit der Politik der Schweiz beeinträchtigen. Firmen, Hochschulen oder Forschungsinstitute, die – auch unwissentlich – in Proliferationsaktivitäten involviert werden, verlieren ihren guten Ruf, können schwere finanzielle Einbussen erleiden oder Ziel von Retorsionsmassnahmen werden.

Inwiefern sind Unternehmen, Hochschulen und Forschungsinstitute von Proliferation betroffen?

Beschaffungsbemühungen

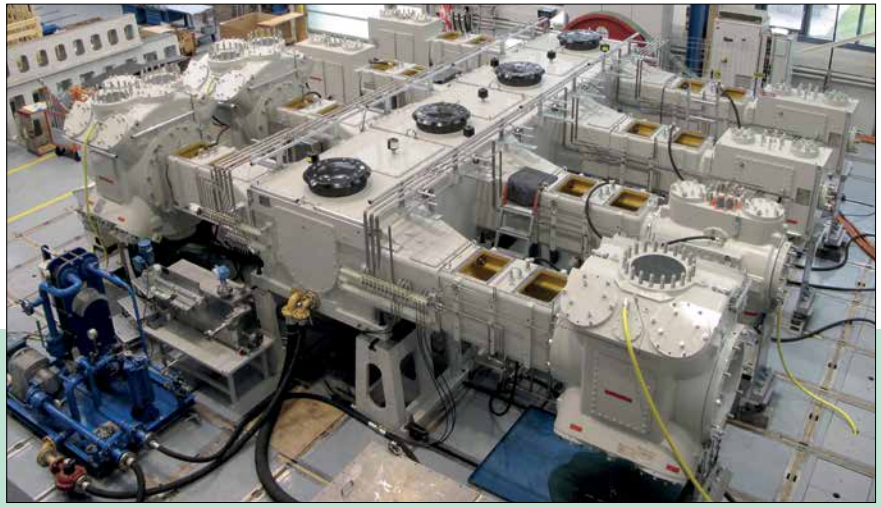
Massenvernichtungswaffen und die entsprechenden Trägersysteme sind nicht auf dem freien Markt erhältlich, und die Gegenmassnahmen der internationalen Gemeinschaft dienen dazu, die Beschaffungsbemühungen der Risikoländer zu unterbinden. Die Beschaffungsversuche beschränken sich jedoch nicht nur auf Güter, sondern auch auf das entsprechende Wissen. Dem Risiko des sog. immateriellen Technologietransfers (Intangible Transfer of Technology, ITT) sind v. a. Universitäten, Fachhochschulen und Forschungsinstitute ausgesetzt.

Proliferationsrelevante Akteure benutzen verschiedene Methoden und verdeckte Beschaffungsnetzwerke, um Exportkontrollen zu umgehen und an kritische Güter zu gelangen:

- Die staatlichen Endverbraucher verstecken sich hinter einem unverdächtigen Firmennamen, einer konventionellen Rüstungsorganisation oder einer Universität, die als Besteller oder Käufer auftreten, oder gründen eine Tarnfirma. Dabei greifen sie auch auf die Unterstützung der jeweiligen Nachrichtendienste zurück.
- Neutrale Handelsfirmen werden vorgeschoben, um Lieferfirmen über den tatsächlichen Kauf durch ein staatlich gesteuertes Unternehmen zu täuschen.
- Die proliferationsrelevanten Akteure gründen für eine einzige Transaktion eine kleine Firma und schliessen sie nach Geschäftsabschluss wieder. Um den tatsächlichen Endempfänger zu verschleiern, schalten sie für die Lieferung und Zahlungsabwicklung mehrere Zwischenhändler ein und wickeln die Lieferung über Drittländer ab (Umweglieferung). Solche Firmen sind u. a. in Transitnationen festgestellt worden.
- Die proliferationsrelevanten Akteure verwenden unauffällige, zivil anmutende Projektnamen und nutzen die Unerfahrenheit gewisser Lieferfirmen im Exportbereich aus. Sie suchen gezielt nach Firmen, insbesondere KMU, die über eine schwache Exportkontrolle und Compliance verfügen.
- Sie missbrauchen im Produktions- oder Lieferland Firmen dazu, illegale Beschaffungen hinter legalen Geschäften zu tarnen, und legen gefälschte Exportdokumente oder nicht der Wahrheit entsprechende Endverbraucherzertifikate vor.

- Sie teilen die Beschaffung in einzelne kleine Bestellungen auf, sodass es sehr schwierig wird, deren Proliferationsrelevanz zu erkennen.
- Sie suchen Ersatzmaterialien und -ausrüstungen, um diejenigen Produkte zu ersetzen, die sich auf den Güterlisten der Exportkontrollen befinden.

Durch diese Vorgehensweisen wird es für die Lieferfirmen schwierig, den effektiven Verwendungszweck ihres Produkts zu erkennen. Dabei sind vor allem die doppelt verwendbaren Güter problematisch, die sowohl im zivilen als auch im militärischen Bereich Anwendung finden können.



Rechts:
Ähnliche Kompressoren aus Schweizer Produktion hätten Hinweisen zufolge in Pakistan im Rahmen des Kernwaffenprogramms verwendet werden sollen (Foto privat)

Wie erkennt man illegale Geschäfte?

An einer Bestellung allein lässt sich oft nicht erkennen, ob die Ware für die Entwicklung von Massenvernichtungswaffen oder Raketensystemen bestimmt ist. Es gilt deshalb, Bestell-, Transport- und Zahlungsmodalitäten sorgfältig zu prüfen. Dafür ist die Beschaffung von detaillierten Informationen über das Bestimmungsland, den Verbraucher und allfällige Zwischenhändler notwendig.

Die Erfahrung hat gezeigt, dass u. a. folgende Verhaltens- bzw. Vorgehensweisen des Kunden Indizien für ein proliferationsrelevantes Geschäft sein können.

Endverwender

- Die Identität eines neuen Kunden ist ungewiss: Er gibt ausweichende Antworten zum Firmenprofil und zu Kontaktpersonen oder kann keine überzeugenden Referenzen vorweisen.
- Der Kunde stellt keinerlei geschäftliche oder technische Fragen, die üblicherweise bei Geschäftsverhandlungen oder in entsprechenden Unterlagen gestellt werden.
- Der Kunde bittet um Fertigstellung eines Vorhabens, das von einer anderen Firma begonnen wurde.
- Der Kunde verlangt unübliche und übertriebene Vertraulichkeit hinsichtlich des Bestimmungsorts oder der zu liefernden Produkte. Er verweigert dem Verkäufer den Zugang zu Anlagenbereichen ohne nachvollziehbare Begründungen. Die Käuferfirma schickt Mitarbeiter zu Ausbildungszwecken zur Herstellerfirma in die Schweiz, obwohl eine entsprechende Schulung vor Ort praktischer und sinnvoller wäre, oder der Kunde verzichtet ganz auf die Schulung, auf Service- oder Garantieleistungen.

Verwendungszweck

- Die Beschreibung der angefragten Güter ist unklar, oder die Güter erscheinen unnötigerweise hoch spezifiziert zu sein.
- Der Kunde verfügt nicht über das notwendige Fachwissen und weiss offensichtlich nicht, welche Sicherheitsvorkehrungen im Umgang mit den bestellten Gütern üblich sind. Er kann den Verwendungszweck des Produkts nicht angeben (oder weigert sich).
- Der vom Hersteller vorgesehene Verwendungszweck der Güter weicht erheblich von dem vom Käufer vorgesehenen ab.
- Der Endverbleib der Ware ist unklar oder nicht plausibel.

Geschäftsabwicklung

- Zwischenhändler treten ohne erkennbaren Grund in Erscheinung.
- Der Kunde bietet ungewöhnlich günstige Zahlungskonditionen an (Bar- oder grosse Vorauszahlungen sowie überdurchschnittliche Provisionen).
- Der Kunde verlangt Sicherheitsvorkehrungen, die im Hinblick auf die beabsichtigte Verwendung übertrieben scheinen. Die Verpackungswünsche sind nicht nachvollziehbar (z. B. seefeste Verpackung bei Lieferung innerhalb Europas), oder es wird eine spezielle Etikettierung, Beschriftung oder Kennzeichnung gewünscht.
- Die vom Kunden vorgesehenen Transportrouten sind geografisch oder wirtschaftlich betrachtet sinnlos.
- Die Güter sind zur Einlagerung in einem Zolllager bestimmt.

Wissensaustausch und Proliferation

Die weltweite Verbreitung von Erkenntnissen aus Wissenschaft und Forschung ist erwünscht und soll nicht behindert oder kontrolliert werden. Die wissenschaftliche Zusammenarbeit kann jedoch auch für proliferationsrelevante Zwecke missbraucht werden.

Besonders problematisch ist der immaterielle Technologietransfer (ITT). Dieser kann sowohl durch den Know-how-Transfer im Rahmen von Fachberatungen, Konferenzen, Schulungen, akademischen Austauschprogrammen, gemeinsamen Forschungs- und Entwicklungsprojekten als auch durch Weitergabe technischer Informationen z. B. mittels E-Mails, Fax, über Webseiten oder Cloud geschehen. Diese Art von Technologietransfer hat mit der Digitalisierung und der Verbreitung und Weiterentwicklung der Informations- und Kommunikationstechnologie (IKT) deutlich zugenommen und stellt für die Exportkontrolle eine besondere Herausforderung dar, weil sie – im Gegensatz zum Güterexport – an den nationalen Grenzen nicht physisch kontrollierbar ist.

Einer der bedeutendsten Fälle von illegalem Know-how- und Technologietransfer ist der des weltweit tätigen Netzwerks um den pakistanischen Ingenieur und Atomwissenschaftler Abdul Qadeer Khan, dem sog. «Vater des pakistanischen Atomwaffenprogramms». Khan studierte in den 1960er-Jahren Metallurgie in Westeuropa. Nach Erlangung seines Doktorats 1972 führte er am niederländischen Physics Dynamics Research Laboratory Studien zu hochfesten Metallen für die Entwicklung von Gaszentrifugen durch. Das Labor war ein Unterauftragnehmer für die Urenco-Gruppe, die u. a. eine Urananreicherungsanlage in den Niederlanden betreibt und angereichertes Uran für Atomkraftwerke in den Niederlanden und weiteren Ländern herstellt. Urenco gewährte Khan Zugriff auf die Baupläne für die Gasultrazentrifuge, um Übersetzungen der niederländischen Unterlagen für die deutschen und britischen Partner im Urenco-Konsortium anzufertigen. Nachdem Indien 1974 seine erste Atombombe zündete, stellte Khan aus eigener Initiative sein Wissen der pakistanischen Regierung zur Verfügung und ermöglichte so den Aufbau einer Urananreicherungsanlage für das pakistanische Atomwaffenprogramm. Später lieferte er sein Wissen sowie Güter zum Auf- und Ausbau eines Nuklearprogramms an Iran, Nordkorea und Libyen.

Proliferationsrelevante Akteure profitieren vom freien Informationsaustausch und können so via immateriellen Technologietransfer zu technischen und wissenschaftlichen Kenntnissen gelangen, die erforderlich sind, um Massenvernichtungswaffen und deren Trägersysteme zu entwickeln. Dabei sind insbesondere die Fachbereiche von Interesse, deren Inhalte in der Entwicklung von Massenvernichtungswaffen und Trägersystemen Anwendung finden, wie z. B. Maschinenbau, Ingenieurwesen, Messtechnik, Naturwissenschaften usw.

Zusätzlich scheuen sich Risikoländer nicht, ihre Nachrichtendienste einzusetzen, um durch den Einsatz von eigenen Nachrichtendienstoffizieren oder rekrutierten Agenten sowie weiteren verdeckten Methoden an die nötigen Expertisen in den Lieferländern zu gelangen. Die Aktivitäten solcher Agenten in den Forschungsinstituten oder Hochschulen sind schwierig zu erkennen und zu bekämpfen.

Um die vertraulichen oder proliferationsrelevanten Informationen zu schützen und die Risiken eines Image- und Glaubwürdigkeitsverlusts zu minimieren, sollten sich Unternehmen, Hochschulen und Forschungsinstitute des Risikos des ITT bewusst sein und die internen Richtlinien und Handlungsdirektiven überprüfen und entsprechend anpassen.

Was machen die Behörden?

Firmen und wissenschaftliche Institutionen sind primär selbst für die Einhaltung der Exportkontrollbestimmungen verantwortlich. Das Staatssekretariat für Wirtschaft (SECO) als Exportbewilligungsinstanz kann über das Vorgehen und die bewilligungspflichtigen sowie meldepflichtigen Produkte Auskunft geben.[1] Andere eidgenössische und kantonale Instanzen wie die Eidgenössische Zollverwaltung (EZV), das Eidgenössische Departement für auswärtige Angelegenheiten (EDA), der NDB und die Kantonalen Nachrichtendienste sind in den Vollzug dieser Bestimmungen involviert.

Wissenschaft und Wirtschaft sind oft nicht in der Lage, die wahren Absichten ihrer Partner aus kritischen Staaten zu erkennen. So kann es dazu kommen, dass ein Unternehmen oder ein Forschungsinstitut unwissentlich eine strafbare Handlung begeht, indem es kritische Güter oder Technologien weitergibt, die in einem Massenvernichtungswaffenprogramm eingesetzt werden. Dagegen verfügen nur sie über das erforderliche Wissen, um zu beurteilen, ob die bestellten Güter in Bezug auf Anzahl und Eigenschaften mit dem vom Abnehmer angegebenen Einsatz übereinstimmen können und inwiefern die Güter oder die Technologie missbraucht werden können.

Zu diesem Zweck kontaktieren, beraten und sensibilisieren der NDB und die Kantonalen Nachrichtendienste Vertreter aus Wissenschaft, Wirtschaft und Industrie mit der notwendigen Diskretion und im partnerschaftlichen Verhältnis.

1 siehe auch www.seco.admin.ch → Aussenwirtschaft & Wirtschaftliche Zusammenarbeit → Exportkontrollen und Sanktionen

Rechts:
Ein elektronisches Messgerät, das Hinweisen zufolge in Pakistan im Rahmen des Kernwaffenprogramms hätte verwendet werden sollen (Foto privat)

PROLIFERATION

Spionage

Definition

Beim verbotenen Nachrichtendienst (Spionage) geht es um die Beschaffung von bewusst vertraulich oder geheim gehaltenen Informationen und Daten aus den Bereichen Politik, Wirtschaft, Militär, Wissenschaft und Technologie, sofern dies zum Nachteil der Schweiz oder ihrer Unternehmen, Institutionen oder von Personen in der Schweiz geschieht und die Informationen an einen ausländischen Akteur (Staat, Gruppierung, Unternehmen, Person usw.) weitergegeben werden.

Bei der Wirtschaftsspionage im Speziellen wird ein Fabrikations- oder Geschäftsgeheimnis aufgeklärt und anschliessend einer fremden amtlichen Stelle, einer ausländischen Organisation oder einem privaten Unternehmen oder ihren Agenten zugänglich gemacht.

Die Verletzung des Fabrikations- und Geschäftsgeheimnisses und der verbotene Nachrichtendienst sind im Schweizerischen Strafgesetzbuch aufgeführt (Artikel 162, 271, 272, 273, 274 und 301).

Schweizer Unternehmen und Hochschulen als Spionageziele

Die Schweiz als Hochtechnologiestandort, als Sitz von Konzernen und internationalen Organisationen, als Durchführungsort internationaler Verhandlungen sowie als Standort wichtiger Datenzentren ist ein interessantes Ausforschungsziel für staatliche und nichtstaatliche Akteure.

Wieso ein bestimmtes Unternehmen Ziel von Wirtschaftsspionage wird, kann verschiedene Gründe haben. Zum einen kann es sich beim Unternehmen um einen Produzenten von Hochtechnologiegütern handeln, der über kritisches Know-how verfügt und dessen Produkte Exportkontrollen unterliegen. Zum anderen sind auch weltweit führende Unternehmen von Interesse, die einen Nischenmarkt bedienen (sog. Hidden Champions). Aber auch Unternehmen und Hochschulen, die angewandte Forschung und Entwicklung betreiben oder Kontakte zu kritischen Staaten pflegen (z. B. in der Form von Joint Ventures oder Forschungskooperationen), sind einem erhöhten Spionagerisiko ausgesetzt.

Die neuen Informations- und Kommunikationstechnologien haben viele Fortschritte ermöglicht, u. a. im Bereich der Datenspeicherung und -analyse. Allerdings sind diese Technologien auch angreifbar und deren unvorsichtige Verwendung kann ein Risikofaktor für Unternehmen und Hochschulen sein. Die Zahl der Cyberspionageangriffe steigt weltweit, und jedes Unternehmen, jede Hochschule und jede Forschungseinrichtung kann zum Ziel werden.

Gewisse ausländische Nachrichtendienste haben den expliziten Auftrag, im Ausland Know-how zu beschaffen, um damit die Wirtschaft und Unternehmen ihrer Länder aktiv zu unterstützen und ihren technologischen Entwicklungsrückstand zu verringern. Spionageangriffe gegen Schweizer Unternehmen und Forschungseinrichtungen haben negative und langfristige Auswirkungen auf die wirtschaftliche und technologische Wettbewerbsfähigkeit der Schweiz.

Legale Informationsbeschaffung

Open Source Intelligence

Nicht verboten ist die Beschaffung von Informationen aus öffentlich zugänglichen Quellen wie z. B. Firmenwebseiten, Produktebroschüren, sozialen Netzwerken, was als Open Source Intelligence (OSINT) bezeichnet wird. Auch das Sammeln von Informationen im Rahmen von Konferenzen, Messen oder diplomatischen Anlässen gehört zur Routinetätigkeit von ausländischen Delegierten in der Schweiz. Es muss aber darauf hingewiesen werden, dass gerade ausländische Nachrichtendienste und Konkurrenzfirmen mit solchen Informationen mögliche Spionageziele (Unternehmen, Organisationen, Personen usw.) evaluieren können. Das Problem besteht darin, dass auf der einen Seite das Produkt einer Firma oder Institution werbewirksam dargestellt werden soll und auf der anderen Seite keine Details veröffentlicht werden sollten. Diese könnten von der Konkurrenz genutzt werden. Auch an internationalen Ausstellungen, Konferenzen und Forschungsprojekten können mit OSINT Informationen über Technologien, die ökonomische Situation eines Unternehmens, Investitionen im Zusammenhang mit Projekten, Forschung und Entwicklung, Mitarbeiterinnen und Mitarbeiter sowie Kunden und zukünftige Verträge beschafft werden. Das Teilen von persönlichen und beruflichen Informationen in sozialen Online-Netzwerken bietet ausländischen Nachrichtendiensten die Gelegenheit, gezielt nach interessanten Personen- und Tätigkeitsprofilen zu suchen und zu versuchen, Personen anzuwerben.

Die Auswertung öffentlich zugänglicher Publikationen und der Austausch wissenschaftlicher Forschungsergebnisse eröffnet ein breites Spektrum an Wissen, gibt wertvolle Hinweise zu aktuellen Projekten und erlaubt gezielte Aktionen gegen die Verantwortlichen. Wer Informationen publiziert, hat es in der Hand, wie detailliert und tiefgründig sie oder er über ein Projekt, ein Produkt, eine Institution oder eine Firma und ihre Mitarbeiterinnen und Mitarbeiter informiert.

Spionagemethoden

Ausländische Nachrichtendienste, aber auch private Akteure bedienen sich verschiedener Spionagemethoden. Im Verborgenen arbeiten sie nach wie vor mit traditionellen Mitteln wie Human Intelligence (HUMINT) und Communications Intelligence (COMINT, Fernmeldeaufklärung). Als HUMINT gilt das Anwerben und Abschöpfen von Informanten. Bei COMINT kommen hochentwickelte elektronische Mittel zum Einsatz, die es ermöglichen, elektronische Übermittlungen aller Art abzuhören bzw. mitzulesen und auszuwerten. Die zunehmende Digitalisierung von Informationen, Daten und Geschäftsprozessen führt zu immer grösseren und kritischeren Datensammlungen. Auch die steigende Verbreitung von Systemen von miteinander verbundenen – und meist schwach geschützten – Geräten und Objekten (sog. Internet of Things, Internet der Dinge) macht diese verwundbar. Dies hat zur Folge, dass die illegale Beschaffung von schützenswerten Informationen und Daten zunehmend mit Mitteln der Cyberspionage geführt wird. Nachrichtendienste und Unternehmen beschäftigen zudem private Agenturen (Detekteien, Treuhand- oder Auskunftsbüros, Beratungs- oder Umstrukturierungsfirmen usw.), aber auch Hacker, um an vertrauliche Daten und Informationen heranzukommen.

Communications Intelligence

Mit COMINT werden Kommunikationen von Unternehmen oder Privatpersonen, die über Kabel, Satellit oder Radiowellen übermittelt werden (z. B. Telefongespräche, E-Mails, SMS), abgefangen und ausgewertet, um an nützliche Informationen über wirtschaftliche oder strategische Ziele heranzukommen. E-Mails, Chatnachrichten und Faxmeldungen können systematisch nach Schlüsselwörtern durchsucht und Telefonate mit automatischer Spracherkennung ausgewertet werden.

Human Intelligence

Tarnung

Z. B. als Diplomaten, Journalisten, Wissenschaftler oder Geschäftsleute getarnt, erhalten ausländische Nachrichtendienstoffiziere in der Schweiz Zugang zu Entscheidungsträgern aus den Bereichen Politik, Militär, Wirtschaft und Wissenschaft. Sie können so erste Informationen sammeln und Personen kontaktieren, ohne sich verdächtig zu machen. Ausländische Nachrichtendienstoffiziere besuchen häufig öffentliche Veranstaltungen und halten Ausschau nach Zielpersonen, wofür alle Informationsträger in Frage kommen. Dabei verwenden sie u. a. Social-Engineering-Taktiken, also gezielte Manipulationsversuche, um an bestimmte Informationen heranzukommen. Dolmetscher und Übersetzer haben oft Zugang zu vertraulichen Informationen, ebenso wie Praktikanten und Doktoranden. Auch sie sind deshalb wertvolle Ziele für ausländische Nachrichtendienste.

An einer öffentlichen Tagung zur Cybersicherheit sprach ein ausländischer Nachrichtendienstoffizier unter diplomatischer Tarnung einen Schweizer IT-Spezialisten an. In der Folge kam es zu einem Treffen, an dem der ausländische Nachrichtendienstoffizier mit dem Schweizer Fragen zur Cybersicherheit in der Schweiz thematisierte. Ziel des Nachrichtendienstoffiziers war es, an detaillierte und womöglich vertrauliche Informationen zu gelangen.

Links:
Ein Fake-Profil auf Linkedin, das von einem chinesischen Nachrichtendienst zur Kontaktaufnahme mit potenziell interessanten Personen verwendet wurde (Deutsches Bundesamt für Verfassungsschutz)

Mehr als nur eine diplomatische Handelsvertretung

Gerade nachrichtendienstlich aktive und als Diplomaten getarnte Angehörige von ausländischen Handelsvertretungen versuchen Firmen im Hochtechnologiebereich anzusprechen. Sie laden zu Ausstellungen, Seminaren und internationalen Kongressen ein, schauen aber auch spontan bei Unternehmen oder Forschungseinrichtungen vorbei. Sie zeigen Interesse an Forschungsprojekten und betrieblichen Abläufen, fordern materiell sehr detaillierte Offerten an oder fragen nach betriebsinternen Handbüchern.

Vom offenen zum konspirativen Kontakt

Ausländische Nachrichtendienstoffiziere bauen kontinuierlich eine Vertrauens- und allenfalls eine Abhängigkeitsbeziehung zu ihren Zielpersonen auf. Anfänglich versuchen sie, nicht klassifizierte und öffentlich zugängliche Informationen zu erlangen. Kleine Geschenke und Einladungen erhalten die Freundschaft – die Zielperson gibt vermehrt vertrauliche Informationen preis. Das Vertrauensverhältnis wird soweit vertieft, bis schliesslich auch Geheiminformationen verraten werden. Die Zielperson verstrickt sich immer tiefer und kann nicht mehr zurück; mit dem Hinweis darauf, welche Informationen sie bereits verbotenerweise geliefert hat, wird erpresserischer Druck aufgebaut.

Erpressung

Besonders die Annahme von Geld kompromittiert und bindet die Zielperson an den ausländischen Nachrichtendienstoffizier. Erpressungsmöglichkeiten können auch von den Nachrichtendiensten selbst geschaffen werden. So werden Zielpersonen in gewissen Staaten Gesetzesübertretungen vorgeworfen. Die Vorwürfe können begründet oder vorgeschoben sein, der Anlass dazu z. B. ein Verkehrsunfall. Gegen Informationen und Zusammenarbeit bietet ein Nachrichtendienst sodann seine Hilfe an. Erpressungsmöglichkeiten können auch durch Überwachung geschaffen werden, etwa durch die Dokumentation von Liebesaffären, Drogenkonsum, Devisenvergehen oder der Annahme von Geld.

Firmen und Forschungseinrichtungen im Visier

Neben den oben bereits genannten, sind im Bereich der Wirtschaftsspionage folgende Methoden üblich, um sich Zugang zu vertraulichen Informationen zu verschaffen:

- Unternehmensbesuche von ausländischen Delegationen mit oder ohne Begleitung durch einen Botschaftsvertreter
- Ausländische Investitionsabsichten (insbesondere bei Start-up-Unternehmen), Teilnahme an gemeinsamen Unternehmen (Joint Ventures) oder Erwerb von Unternehmen zwecks Technologietransfer und Platzierung neuer Mitarbeiterinnen und Mitarbeiter in sensiblen Bereichen
- Forschungszusammenarbeiten mit Unternehmen zwecks Aneignung von technischem Know-how für den Aufbau und Betrieb einer Produktionsanlage
- Wissenschaftliche Kooperationen mit Hochschulen und Forschungsinstituten zwecks Zutritt zu hochwertigen Forschungsgeräten und -anlagen
- Angriffe auf Kunden, externe Dienstleister, Berater oder Lieferanten einer Firma, die das eigentliche Hauptziel ist
- Ausnutzen von Schwächen in der Organisation der Firma, z. B. indem es Mitarbeitern erlaubt ist, private mobile Endgeräte wie Notebook, Tablet oder Smartphone ans Firmennetzwerk anzuschliessen

- Regulatorische und gesetzliche Einschränkungen in anderen Staaten für ausländische Niederlassungen, die diese z. B. dazu zwingen, ihre Daten auf Servern im Land der Niederlassung zu speichern
- Rekrutierung eines Angestellten als Informant, um an vertrauliche Informationen zu gelangen, aber auch Abschöpfung ehemaliger Angestellter, die Zugang zu sensiblen Bereichen und Informationen hatten sowie die internen betrieblichen Abläufe kennen.

Der Kurzfilm «Im Visier» des NDB zeigt, wie ausländische Nachrichtendienstoffiziere vorgehen und welche Mittel sie einsetzen, um an vertrauliches Know-how eines Schweizer Unternehmens zu gelangen.[1]

1 Abrufbar unter www.ndb.admin.ch/wirtschaftsspionage

Innentäter

In vielen Spionagefällen gibt der eigene Mitarbeiter oder die eigene Mitarbeiterin vertrauliche Firmendaten an Unberechtigte (Konkurrenten, ausländische Nachrichtendienste) weiter, sei dies aus Vorsatz oder Zwang. Die Motivationsfaktoren für eine solche Tat sind unterschiedlich. Oft werden Warnzeichen übersehen oder ignoriert. Folgende Verhaltensmuster können auf einen Innentäter hinweisen:

- Ungewöhnliche Arbeits- bzw. Gebäudezutrittszeiten (z. B. sehr früh morgens oder spät abends, um möglichst allein im Büro zu sein)
- Übermässiges Drucken oder Kopieren von Firmenunterlagen
- Speichern von besonders grossen Datenmengen auf elektronischen Datenträgern
- Unerlaubte Mitnahme vertraulicher Unterlagen ausserhalb des Firmengeländes
- Unerlaubtes Mitführen elektronischer Geräte in sensitiven Arbeitsbereichen
- Zugriffe auf Firmendaten, die der Mitarbeiter für seine Arbeit nicht benötigt
- Frustration am Arbeitsplatz wie z. B. Desillusionierung aufgrund einer nicht erhaltenen Beförderung oder anderen wahrgenommenen Missständen, Ärger mit Vorgesetzten und Arbeitskollegen
- Unerklärlicher und plötzlicher Reichtum
- Anfälligkeit für Erpressung (z. B. aufgrund einer ausserehelichen Beziehung, Drogenkonsum, Gesetzesverstössen)
- Mangelnde Diskretion

- Risikofreudigkeit, Leichtsinnigkeit und bewusste Missachtung der Sicherheitsvorschriften
- Persönliche Kontakte zu Vertretern ausländischer Botschaften oder Diplomaten, die der Firmenleitung weder bekannt noch von ihr bewilligt wurden.

Wird ein solches Verhalten bei einer Mitarbeiterin oder einem Mitarbeiter festgestellt, sollte es umgehend der für die Sicherheit des Unternehmens verantwortlichen Person gemeldet werden.

Welchen Bedrohungen sind Unternehmen und Hochschulen durch den Einsatz von IKT ausgesetzt?

Cyberspionage und Datendiebstahl

Das Schweizerische Strafgesetzbuch unterscheidet folgende Delikte:

- Art. 143 Unbefugte Datenbeschaffung
- Art. 143bis Unbefugtes Eindringen in ein Datenverarbeitungssystem
- Art. 144bis Datenbeschädigung
- Art. 147 Betrügerischer Missbrauch einer Datenverarbeitungsanlage

Die Verwendung der IKT, um an Informationen zu gelangen, zu denen man mit Standardmitteln keinen Zugang hätte, hat in den letzten Jahren stark zugenommen. Kriminelle, Konkurrenten, Staaten, Terroristen oder unabhängige Gruppen verwenden die IKT, um in Informatiksysteme einzudringen und sich Zugang zu sensiblen Daten zu verschaffen. Cyberspionage und über das Internet erfolgter Datendiebstahl erlauben es dem Angreifer, die Anonymität zu wahren und die Kosten der illegalen Informationsbeschaffung zu reduzieren. Immer häufiger verüben diese Akteure gezielte Angriffe mit hochentwickelter Schadsoftware. Dabei setzen sie über eine längere Zeitspanne grosse finanzielle und persönliche Mittel ein, um ausgewählte Opfer gezielt anzugreifen (Advanced Persistent Threat, APT). Hinter solchen komplexen Angriffen stecken meist staatliche Akteure mit dem Ziel, sich unbemerkt und über längere Zeit im Netzwerk einer Firma oder Organisation aufzuhalten, sei es zu Spionage- oder Sabotagezwecken. Sie können das Netzwerk aber auch dazu missbrauchen, Cyberoperationen gegen weitere Ziele durchzuführen. Des Weiteren kann ein vermeintlicher krimineller Cyberangriff mittels Ransomware eine Tarnung für einen gravierenderen Angriff sein: Dabei geht es dem Angreifer weniger um die Einforderung eines Lösegelds als um den Diebstahl oder die Vernichtung von Daten.

Unternehmen und Hochschulen sind nicht nur Kleinkriminellen mit beschränkten Fähigkeiten ausgesetzt, sondern müssen auch mit Bedrohungen und Angriffen seitens organisierter und technisch bewanderter Gruppen rechnen. Jedoch nehmen sie diese Bedrohung oft nicht in ausreichendem Mass wahr. Im Gegenteil, sie scheint vielen ein nur virtuelles und infolgedessen harmloses Phänomen zu sein.

Massive Datensammlung

Oft beauftragen Unternehmen externe Anbieter mit Dienstleistungen im IKT-Bereich. Sie geben dadurch die IKT-Infrastruktur des Unternehmens und die darin enthaltenen Informationen an Dritte weiter, deren Aktivitäten sie nicht immer ausreichend kontrollieren können. Die für Wirtschafts- und Forschungsaktivitäten notwendige Kommunikation, z. B. über Informatik- und Mobilfunknetze, kann die Aufmerksamkeit von Drittstaaten auf sich ziehen, die über Technologien zur massiven Datenabschöpfung verfügen. Diese sind in der Lage, die Kommunikation auszuwerten und zu ihren Gunsten oder zur Unterstützung von Konkurrenzunter-

nehmen und -organisationen auszunützen. Unternehmen und Hochschulen müssen damit rechnen, dass jede Information, die das eigene Netzwerk verlässt, durch einen externen Akteur gesammelt, analysiert und missbraucht werden kann. Folglich ist die Gewährleistung der Vertraulichkeit einer Information eines der grundlegenden Elemente der Sicherheit.

Datenbeschädigung

Der nicht autorisierte Zugang zu einem Datenverarbeitungssystem kann auch die Zerstörung von Daten zum Ziel haben. Der Grund für solche Aktivitäten liegt oft im Wunsch, einen Vorteil gegenüber der Konkurrenz zu erlangen, oder im Versuch, ein laufendes Geschäft zu blockieren. Informationen sind ein besonders schützenswertes Gut. Der Wert einer Information bestimmt auch die Sicherheitsmassnahmen, die zu ihrem Schutz ergriffen werden sollten.

Netzwerkstörungen

Wenn ein Netzwerkdienst für die berechtigten Benutzerinnen und Benutzer für längere Zeit nicht verfügbar ist, kann das bei einem Unternehmen oder einer Hochschule zu grossem Schaden führen. Ein klassisches Beispiel aus diesem Bereich sind verteilte Überlastungsangriffe (distributed denial-of-service attack, DDoS attack). Diese Angriffe versuchen, mit einer grossen Anzahl externer Kommunikationsanfragen ein oder mehrere Elemente der angegriffenen IT-Infrastruktur zu überlasten, um so ein Leistungsdefizit zu provozieren und einen Internetdienst funktionsunfähig zu machen. Unternehmen, die teilweise oder vollständig auf das Web angewiesen sind, benötigen eine praktisch permanente Aktivitätszeit ihres Informatiksystems. Ist ihr Informatiksystem nicht genügend vor einem Angriff geschützt, müssen sie mit Gewinneinbussen oder entgangenen Aufträgen rechnen, falls dieses angegriffen wird.

Wie können sich Unternehmen und Hochschulen vor einem Informations- und Datenabfluss schützen?

Die weltweit verschärfte Konkurrenzsituation und eine steigende Abhängigkeit von modernen Informations- und Kommunikationssystemen führen zu neuen Verwundbarkeiten und Herausforderungen für Unternehmen, Hochschulen und weitere Einrichtungen. Es wird immer wichtiger, sich gegen die illegale Nutzung des eigenen Wissens durch Unbefugte zu schützen. Kleine und mittlere Unternehmen stellen häufig wegen ihrer innovativen Forschungs- und Entwicklungsvorhaben und des vorhandenen Know-hows interessante Ausspähungsziele dar. Mit zunehmender Vernetzung kommt der Sicherheit der Informationsinfrastruktur Priorität zu. Die Unterbrechung der Kommunikationsnetze sowie Diebstahl, Manipulation oder Verlust von Daten können für Wirtschaft, Gesellschaft und Staat zum existenziellen Risiko werden.

Informationssicherheit darf nicht an Firmen- oder Landesgrenzen Halt machen. International tätige Unternehmen müssen sich bewusst sein, dass Informationsverluste bei ausländischen Niederlassungen, Konzerngesellschaften oder Geschäftspartnern möglich sind. In den letzten Jahren haben einige Staaten strenge Gesetze zur Cybersicherheit eingeführt, die ausländische Unternehmen dazu zwingen, ihre Daten auf Servern im Gastland zu speichern. Möchte das Unternehmen seine Daten ins Ausland transferieren, so benötigt es die staatliche Bewilligung des Gastlands. Gewisse Staaten fordern die Überprüfung der Quellcodes der innerhalb ihres Lands verkauften ausländischen Technologien durch die eigenen Instanzen. Ausländische Unternehmen sind somit zunehmend dem Risiko ausgesetzt, dass ihre Daten und Informationen unwissentlich an Dritte abfliessen oder missbraucht werden.

Schutzmassnahmen

Einen vollständigen Schutz gegen Informationsabfluss gibt es nicht, doch geeignete Massnahmen zur Risikoeindämmung können wirkungsvoll und finanziell tragbar sein. Folgende präventive Massnahmen können u. a. ergriffen werden.

Informationssicherheit

- Erstellung und Umsetzung eines Informationssicherheitskonzepts und Ernennung einer dafür verantwortlichen Person, die mit Unterstützung der Geschäftsleitung Kontrollen durchführt und die Sicherheitsmassnahmen durchsetzt
- Regelung und Einschränkung der Zugriffsrechte der Mitarbeiterinnen und Mitarbeiter auf Daten und Akten
- Keine Mitnahme von Mobiltelefonen zu Geschäftssitzungen, in denen sensitive Themen besprochen werden, sowie keine vertraulichen Gespräche über das Mobiltelefon
- Clean-Desk-Richtlinie («sauberer Schreibtisch»): Sind Mitarbeiterinnen und Mitarbeiter nicht an ihrem Arbeitsplatz, z. B. während der Mittagspause oder ausserhalb der Arbeitszeiten, schliessen sie alle Dokumente weg (insbesondere vertrauliche und geheime Informationen). Computer sollten auch bei kurzen Abwesenheiten immer gesperrt werden (Bildschirmsperrung).
- Sichere Vernichtung vertraulicher Akten (z. B. mittels Aktenvernichter) und Datenträger wie USB-Sticks
- Genaue Überprüfung der Mitarbeiter und Mitarbeiterinnen vor der Einstellung (z. B. Strafregisterauszug, Personensicherheitsprüfung)

- Regelmässige Ausbildung, Weiterbildung und Sensibilisierung der Mitarbeiterinnen und Mitarbeiter betreffend die Informations- und IT-Sicherheit sowie die Spionagebedrohung
- Systematische und zentralisierte Kontrolle der vom Unternehmen und von seinen Mitarbeiterinnen und Mitarbeitern publizierten Informationen (auf der Firmenwebseite, in den sozialen Netzwerken, in Produktebroschüren usw.)
- Richtlinien für das Verhalten der Mitarbeiterinnen und Mitarbeiter an Messen, Konferenzen, Veranstaltungen und auf Geschäftsreisen

Externe

- Zutrittskontrollen und ständige Begleitung von externen Besuchern und Delegationen: u. a. Überprüfung der Personalien der Delegationsmitglieder, Besucher-Badges, Sicherstellen eines angemessenen Betreuungsverhältnisses und Sensibilisierung der für die Betreuung aufgebotenen Personen sowie von weiteren vom Besuch betroffenen Mitarbeitern, Festlegen der Agenda, keine Mitnahme elektronischer Geräte durch Delegationsmitglieder usw.
- Überprüfung von Zulieferern, Beratern und weiteren Dienstleistern

IT- und Datensicherheit

Durch unbeabsichtigte Handlungen bei der Bereitstellung und Benutzung von IKT, z. B. menschliches Fehlverhalten oder technische Ausfälle, oder durch bewusste und illegale Handlungen (Cyberangriffe) können Informationen und Daten in falsche Hände gelangen. In einem Unternehmen oder an einer Hochschule sowie im privaten Bereich sollten technische Lösungen wie Firewall, die den eingehenden wie auch ausgehenden Datenverkehr filtert, Antivirenprogramme und eine regelmässige, rasche Aktualisierung der Betriebssysteme und verwendeten Software die Regel sein. Es sind jedoch weitere Massnahmen notwendig, wie z. B. Verschlüsselung der Festplatten (insbesondere von Notebooks, die auch ausserhalb des Firmengeländes verwendet werden), Blockierung sämtlicher Anschlüsse der Firmencomputer für externe Speichermedien (USB-Stick, SD-Karten usw.) sowie die Trennung (virtuell oder physisch) des internen und des externen IT-Netzwerks. Für die persönlichen Zugänge zu Computer, Notebooks und E-Mails sollte grundsätzlich die Zwei-Faktor-Authentifizierung (z. B. mittels Sicherheits-Token oder USB-Sicherheitsschlüssel) oder Smartcard-Authentifizierung (z. B. PKI-Karte) verwendet werden. Weiter ist es angezeigt, Sicherheitslösungen bei der Datenübermittlung anzuwenden. Sensible Informationen sollten verschlüsselt werden, bevor sie in ein externes Netz geleitet werden (z. B. bei der Übermittlung via E-Mail), und die Datenübermittlung sollte über einen sicheren Kanal wie z. B. ein Virtual Private Network (VPN) erfolgen (insbesondere wenn Mitarbeiter von extern auf das Firmennetzwerk zugreifen). Vorsicht ist angezeigt bei der Verwendung von Cloud-Diensten zur Datenspeicherung, insbesondere wenn sich die Server im Ausland befinden. Die Benutzung von E-Mail ist oft der grösste Schwachpunkt im Schutz eines Unternehmens oder einer Organisation vor Cyberangriffen und kann bei unvorsichtigem Umgang einem Gegner Tür und Tor öffnen, um in das Netzwerk eines Unternehmens oder einer Organisation einzudringen (z. B. mittels eines Spearphishing-Angriffs[1]).

Unternehmen und Hochschulen benötigen Instrumente, um illegale Zugriffe auf die eigene Netzwerkinfrastruktur festzustellen. Besondere Lösungen wie Intrusion Detection Systems (IDS) oder Intrusion Prevention Systems (IPS) eignen sich, um das Sicherheitsniveau auf dem Netzwerk zu erhöhen. Die Absicherung von Endgeräten im Netzwerk bzw. die Überwachung von Aktivitäten auf den Endgeräten sowie das Loggen von Netzwerk- (IP-Adressen, Ports) und Dateizugriffen ermöglichen es, Vorfälle zu erkennen und aufzuarbeiten. Um einen Ressourcenmissbrauch zu verhindern, sollten auch Lösungen implementiert werden, die das Netzwerk vor externen Angriffen schützen. Solche Lösungen werden oft von Netzprovidern zur Verfügung gestellt (Anti-DDoS).

Verhaltensregeln und Ausbildung

Im Informatikbereich sind Weisungen notwendig, die nicht nur während der Arbeitszeit, sondern auch im Privatleben angewendet werden können. In diesen Weisungen zur Verwendung von Informatikmitteln ist es vorteilhaft, die grundsätzliche Positionierung des Unternehmens oder der Forschungseinrichtung zur allgemeinen Internetverwendung, der Benützung der privaten E-Mailsysteme und sozialen Netzwerke am Arbeitsplatz darzulegen. Zudem sollten regelmässige Ausbildungs- und Weiterbildungskurse zu den mit der Verwendung der IKT verbundenen aktuellen Risiken für alle Mitarbeiterinnen und Mitarbeitern durchgeführt werden.

1 Phishing-Methode, die gezielt an einzelne Personen oder Gruppen innerhalb eines Unternehmens oder einer Organisation gerichtet ist. Im Gegensatz zu Phishing-Mails, die breit gestreut werden, ist ein Spearphishing-Mail (oder eine Spearphishing-SMS) auf die Zielperson und ihre Interessen zugeschnitten. Die Zielperson wird aufgefordert, persönliche Informationen (z. B. Login-Informationen und Passwörter) preiszugeben oder einen Anhang zu öffnen bzw. auf einen Link zu klicken, der Schadsoftware enthält und den Computer der Zielperson und somit das Firmennetzwerk infiziert.

Auswahl der Partner und der IT-Lösungen

Insbesondere KMU verfügen oft nicht über genügend personelle und finanzielle Ressourcen, um die Sicherheit ihrer Informatiknetzwerke lückenlos zu überwachen. Daher sind Investitionen in externe Unterstützung empfehlenswert. Allerdings sollten Unternehmen bei der Auswahl eines IT-Partners verschiedene Faktoren berücksichtigen. Zwar sind die technische Kompetenz eines Anbieters und die Qualität seiner Dienstleistung zweifellos grundlegende Elemente bei der Auswahl. Doch auch unterschiedliche rechtliche und politische Rahmenbedingungen, denen der Anbieter unterworfen ist, oder dessen Teilnahme an staatlichen Datensammlungsprogrammen sind entscheidende Faktoren, die zu berücksichtigen sind, wenn ein Datenabfluss oder eine Schädigung des IT-Netzwerks verhindert werden sollen.

Hilfestellungen/Unterstützung

Das Bundesamt für wirtschaftliche Landesversorgung hat einen IKT-Minimalstandard definiert; der konkrete Handlungsanweisungen zur Verbesserung der IKT-Resilienz bietet.[1] Diese richten sich insbesondere an die Betreiber kritischer Infrastrukturen, können aber von jedem Unternehmen oder jeder Organisation angewendet werden. Mittels Selbsteinschätzung und Bewertungsinstrument kann der Stand der Umsetzung beurteilt werden.

Speziell für KMU hat ICT Switzerland einen Online-Schnelltest zur Cybersicherheit entwickelt. Hier können Unternehmen überprüfen, ob sie die Minimalstandards für KMU erfüllen.[2]

1 Abrufbar unter www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard.html
2 Abrufbar unter www.cybersecurity-check.ch

Sicherheit auf Geschäftsreisen im Ausland

Auf Geschäftsreisen im Ausland erhöht sich das Risiko, Opfer von Spionage zu werden. Ein ausländischer Nachrichtendienst oder Konkurrent kann Personen direkt, wegen ihrer Tätigkeit, ihres Know-hows oder der Informationen und elektronischen Daten, die sie mit sich führen, zum Ziel machen. Elektronische Geräte wie Notebooks, Smartphones, Tablets und Datenträger wie USB-Sticks stellen heikles Material dar, über das sich böswillige Kreise unbemerkt Informationen beschaffen können. Einige Staaten überwachen den Internetverkehr, die Telekommunikation und die Postwege; hier wird Gepäck durchsucht und werden elektronische Geräte und Datenträger von Reisenden manipuliert. Gewisse Staaten sind auch dazu bereit, kompromittierende Situationen zu schaffen, Verkehrsunfälle zu fingieren oder die Ausreise zu verhindern, um so die Zielperson zur Herausgabe von vertraulichen Informationen zu zwingen oder diese sogar als Informanten zu rekrutieren. In bestimmten Staaten sammeln die Behörden Informationen bereits vor der Ankunft einer Person, etwa durch Recherchen in den sozialen Netzwerken. In einem Visumsantrag kann ein ausländischer Nachrichtendienst feststellen, ob eine Person ein interessantes Ziel ist; insbesondere Antworten auf Fragen zur beruflichen Tätigkeit enthüllen Details.

Mögliche Szenarien

- Ein Zollbeamter verlangt an einer Grenzübergangsstelle von einer reisenden Person die vorübergehende Übergabe ihrer elektronischen Geräte. Sie weiss nach der Übergabe nicht, was der Zollbeamte damit getan hat. Auch offizielle Stellen können daran interessiert sein, einen Einblick in geschäftliche und private Daten reisender Personen zu gewinnen.

- Eine Geschäftsperson befindet sich im Ausland und muss über ihr Mobiltelefon heikle Informationen übermitteln. Das Telefonsignal wird zwar verschlüsselt, aber nur auf der Funkstrecke und mit kostengünstigen Technologien; so ist es möglich, das Signal zu entschlüsseln und das Gespräch abzuhören. Sobald das Signal von der Funkstrecke in das Festnetz eingespeist wurde, ist es ohnehin nicht mehr verschlüsselt.
- Eine Firmenvertreterin benötigt eine Information und loggt sich unterwegs im Internet ein: Ihre Kommunikation kann an den verschiedensten Orten (Hotel, Flughafen, Bahnhof, Café usw.) abgefangen werden.
- Auf einer Geschäftsreise nimmt sich der Forschungsverantwortliche ein paar Stunden Zeit für einen Stadtbummel und lässt seine elektronischen Geräte und Geschäftsdokumente im Hotelzimmer zurück: Sein Hotelzimmer (inkl. Zimmersafe) kann möglicherweise nach interessantem Material durchsucht werden.
- Während einer Konferenz verlassen die Teilnehmerinnen und Teilnehmer für die Kaffeepause den Saal und lassen das Notebook offen auf dem Tisch stehen. Jemand könnte einen USB-Stick bereithalten, um die auf einem Notebook gespeicherten Dateien zu kopieren oder um eine Schadsoftware auf ein Notebook hochzuladen.
- Nach einem Geschäftstreffen bleibt ein Firmenvertreter privat weiterhin in Kontakt mit einer Mitarbeiterin des ausländischen Unternehmens. Die Mitarbeiterin überreicht dem Firmenvertreter ein teures Geschenk oder lädt ihn zu einem privaten und von ihr finanzierten Besuch in ihr Land ein. Sie kann dafür eine Gegenleistung erwarten, z. B. in der Form von sensitiven Geschäftsinformationen.

Persönliche Sicherheitsmassnahmen

- Nehmen Sie nur die elektronischen Geräte auf Auslandsreisen mit, die Sie für Ihre Tätigkeit unbedingt benötigen und die keine heiklen Informationen enthalten. Es ist ratsam, spezielle Notebooks und Mobiltelefone zu verwenden, die nur für Geschäftsreisen bestimmt und so konfiguriert sind, dass Sie nach ihrer Rückkehr die Geräte ohne grossen Aufwand neu aufsetzen können. Die Geräte sind auch verwundbar, wenn Sie sie nicht aus der Hand geben.
- Stellen Sie sicher, dass die Betriebssysteme und die auf Ihren elektronischen Geräten installierten Anwendungen auf dem aktuellsten Stand sind. Verwenden Sie starke und einmalige Passwörter (alphanumerische Zeichen, Gross- und Kleinbuchstaben, Sonderzeichen), die keine persönlichen Informationen wie Geburtsdatum beinhalten. Empfehlenswert sind Passwörter mit mindestens 12 Zeichen, die z. B. aus den Anfangsbuchstaben von mehreren Wörtern zusammengesetzt sind (z. B. das Passwort HMgjMu7msHs! steht für **H**err **M**eier **g**eht **j**eden **M**orgen **u**m 7 **m**it **s**einem **H**und **s**pazieren**!**).
- Die Festplatte Ihres Computers bzw. die darauf gespeicherten Daten sollten verschlüsselt sein. Da in einigen Ländern aber die Einreise mit verschlüsselten Daten verboten ist, sollten Sie mit einem Computer reisen, der keine heiklen Daten enthält. Wenn Sie im Ausland angelangt sind, können Sie die Daten über eine gesicherte Verbindung (Virtual Private Network, VPN) herunterladen und sie nach Gebrauch mit einer geeigneten Software vollständig löschen.

- Händigen Sie elektronische Geräte (z. B. am Grenzübergang) nur aus, wenn Sie dem Beamten oder der Beamtin physisch folgen können. So wissen Sie, was mit Ihrem Material geschieht. Sollten Sie nicht sehen können, was mit Ihrem Gerät passiert, dann gehen Sie davon aus, dass es manipuliert wurde.
- Lassen Sie Ihr Material nie unbeaufsichtigt liegen (z. B. während der Kaffeepause auf einer Konferenz oder auch nur für den Toilettenbesuch).
- Verwenden Sie keine geliehenen oder geschenkten externen Peripheriegeräte (USB-Stick, externe Festplatte, Mobiltelefon, digitaler Fotoapparat usw.) und erlauben Sie niemandem, ein Peripheriegerät an Ihren Computer anzuschliessen (z. B. um Ihren Computer für eine Präsentation zu benutzen oder um ein fremdes Mobiltelefon aufzuladen). Wenn Sie ein Peripheriegerät an einen unbekannten Computer angeschlossen haben, sollten Sie es formatieren, bevor Sie es wieder verwenden.
- Da Internetverbindungen über frei zugängliche – und teilweise auch passwortgeschützte – WLAN (z. B. in Hotels, Cafés oder Flughäfen) generell nicht verschlüsselt und somit unsicher sind, sollten Sie diese nur über eine VPN-Verbindung nutzen oder – falls VPN im Gastland blockiert wird – via 3G/4G/5G-Datenübertragung im Roaming auf das Internet zugreifen. Achten Sie darauf, dass die Kommunikation zwischen Ihrem Webbrowser und der von Ihnen aufgerufenen Webadresse verschlüsselt ist (http**s**://...).
- Deaktivieren Sie drahtlose Schnittstellen wie WLAN und Bluetooth sowie Lokalisierungsdienste bei Nichtgebrauch.
- Wenn Sie Ihr Mobiltelefon oder Notebook nicht zu einer Sitzung oder in ein Gebäude mitnehmen können, schalten Sie es aus und bewahren Sie es in einer sicheren Verpackung auf (Sicherheitsbeutel oder Sicherheitsbehältnis).

- Seien Sie vorsichtig mit persönlichen Informationen, die Sie in den sozialen oder beruflichen Online-Netzwerken preisgeben.
- Lassen Sie Vorsicht walten bei Kontaktversuchen Ihnen unbekannter Personen, die nichts mit Ihrer Geschäftsreise zu tun haben.
- Informieren Sie sich vor Ihrer Abreise über die geltenden Gesetze und kulturellen Gepflogenheiten im Zielland.
- Bleiben Sie aufmerksam und achten Sie darauf, wer Ihnen – im Zug, im Flugzeug oder auf einer Konferenz – über die Schulter schaut, um Ihren Bildschirm auszuspähen.

Nach der Rückkehr

- Ändern Sie alle Passwörter, die Sie während der Auslandsreise benutzt haben.
- Lassen Sie im Verdachtsfall Ihre elektronischen Geräte durch die IT-Abteilung Ihres Unternehmens oder durch einen privaten IT-Dienstleister prüfen und im Zweifelsfall neu aufsetzen.
- Melden Sie verdächtige Vorkommnisse Ihrer Sicherheit und dem NDB.

Kontakt

Wie kann Sie der NDB unterstützen?

Der NDB hilft in Zusammenarbeit mit den Kantonalen Nachrichtendiensten, die schweizerischen und liechtensteinischen Unternehmen, Hochschulen und Forschungseinrichtungen über Proliferation und Spionage aufzuklären, zu sensibilisieren und zu beraten.

- www.ndb.admin.ch
- prophylax@ndb.admin.ch

Sensibilisierung Wirtschaftsspionage

www.ndb.admin.ch/wirtschaftsspionage

- Sensibilisierungsfilm über Wirtschaftsspionage «Im Visier»
- Erläuterungen zu den im Film gezeigten Spionagemethoden und entsprechende Schutzmassnahmen
- Merk- und Faktenblätter zu den Themen Proliferation und Spionage
- Prophylax-Broschüre (auch unter www.ndb.admin.ch/prophylax abrufbar)

Vorgehen bei Verdacht

Bei Verdacht auf Spionage oder Proliferationsaktivitäten (z. B. dubiose Produkteanfragen oder Bestellungen) zögern Sie nicht, den NDB oder Ihre Kantonspolizei zu kontaktieren. Sichern Sie mögliche Beweise und löschen Sie verdächtige E-Mails nicht. Der NDB sammelt und wertet die Hinweise aus. Er garantiert eine diskrete Behandlung des Falls.

Weiterführende Informationen

Staatssekretariat für Wirtschaft

www.seco.admin.ch
→ Aussenwirtschaft & Wirtschaftliche Zusammenarbeit → Exportkontrollen und Sanktionen

- Elic (e-licensing): elektronisches Bewilligungssystem für die Erfassung und Bearbeitung von Anträgen, die der Exportkontrolle unterliegen (Dual-use-Güter, Kriegsmaterial und besondere militärische Güter)
  (auch unter www.elic.admin.ch abrufbar)
- Sanktionen/Embargos: Suche nach sanktionierten Personen, Unternehmen und Organisationen (Datenbank SESAM)
- Industrieprodukte (Dual-use) und besondere militärische Güter (Licensing)
  - Merkblatt zur firmeninternen Kontrolle der Einhaltung der Exportkontrollvorschriften (Internal Compliance Program, ICP) (unter Formulare und Merkblätter)

Eidgenössisches Departement für auswärtige Angelegenheiten

www.eda.admin.ch
→ Vertretungen und Reisehinweise

Einschätzung der eigenen Sicherheitsvorkehrungen im IT-Bereich

Melde- und Analysestelle Informationssicherung

www.melani.admin.ch
www.antiphishing.ch (Meldung von Phishing-Mails)

Bundesamt für wirtschaftliche Landesversorgung

www.bwl.admin.ch
→ Themen → IKT-Minimalstandard
IKT-Minimalstandard zur Verbesserung der IKT-Resilienz von Betreibern kritischer Infrastrukturen, Unternehmen und Organisationen (inkl. Bewertungsinstrument)

ICT Switzerland

www.cybersecurity-check.ch
Online-Schnelltest zur Cybersicherheit für KMU

Redaktion
Nachrichtendienst des Bundes NDB

Redaktionsschluss
Februar 2019

PROPHYLAX
Nachrichtendienst des Bundes NDB
Papiermühlestrasse 20
CH-3003 Bern
www.ndb.admin.ch