

Wirtschaftsspionage und Proliferation im Kanton Schwyz – Relevanz und Einordnung



Nadine Kürzi

Nadine Kürzi arbeitet als Ermittlerin im Bereich Wirtschaftskriminalität. Sie verfügt über einen Bachelor of Science in Betriebsökonomie mit Vertiefung in Management & Law und hat das MAS Economic Crime Investigation 21 absolviert.

Die aktuelle geopolitische Lage mit Machtkämpfen unter den Grossmächten und den kriegesischen Auseinandersetzungen hat dazu geführt, dass der Nachrichtendienst des Bundes (NDB) sowie Experten das Risiko für Wirtschaftsspionage und illegale Beschaffungsbemühungen für Massenvernichtungswaffen (Proliferation) als zunehmend respektive anhaltend hoch einschätzen.

Grundsätzlich kann jedes Unternehmen ungeachtet seiner Grösse, jede Hochschule und jede Forschungseinrichtung zum Ziel von Spionage werden. Insbesondere sind heutzutage die neuen Informations- und Kommunikationstechnologien angreifbar und stellen diesbezüglich einen Risikofaktor dar. Ein Unternehmen ist als Spionageziel umso attraktiver, je sensibler sein Know-how ist, wie dies zum Beispiel bei Produzenten von Hochtechnologiegütern der Fall ist, deren Produkte der Exportkontrolle unterliegen. Als einem erhöhten Spionagerisiko ausgesetzt gelten auch Unternehmen, die in einem Nischenmarkt tätig sind (sog. Hidden Champions) oder die Kontakte zu heiklen Staaten pflegen, beispielsweise über Joint Ventures oder Forschungskooperationen. Heikel oder kritisch sind Staaten, die im Verdacht stehen, aktiv Wirtschaftsspionage zu betreiben; allen voran Russland und China, aber auch andere autoritär regierte Staaten. Eine Studie der deutschen Hochschule Aalen bestätigte zudem die Hypothese, dass kleine und mittlere Unternehmen (KMU) als Türöffner respektive Eintrittstickets in die Informationssysteme grösserer Gesellschaften verwendet werden; ein Vorgehen, das auch als Lieferketten-Attacke bezeichnet wird. Als konkrete Spionageziele kommen jedoch nicht nur Unternehmen und Institutionen, sondern auch Organisationen und natürliche Personen in Frage; eben alle, die über sensibles Know-how verfügen oder Zugang dazu haben. Solches Know-how ist in der Regel auf Computern gespeichert, weshalb neben Angriffen auf Firmennetzwerke auch Notebook-Diebstähle aus Hotelzimmern oder Einbrüche in Betriebsgebäude vorkommen. Weil auch

Menschen individuelle Träger von Wissen sind, werden beispielsweise Angestellte auf Messen gezielt nach sensiblen Geschäftsdaten ausgefragt. Der Faktor Mensch gilt generell als schwächstes Glied und ist am anfälligsten für Spionageangriffe, insbesondere wenn die Täterschaft böswilliges Social Engineering einsetzt. Die Spionagemethoden sind vielfältig und bewegen sich in legalen, grauen und illegalen Bereichen. Bei der Täterschaft unterscheidet man zwischen jener von innen und jener von aussen, wobei die Gefahr der Innentäterschaft von Fachleuten als höher eingeschätzt wird. Sie hat Zugang zu unternehmensbezogenen Informationen, welche Personen von aussen nicht oder nur erschwert haben. Folglich können Innentäter_innen neben eigenen Angestellten unter Umständen auch Beraterinnen oder Lieferanten sein.

Die Schweiz stellt ein interessantes Ausforschungsziel dar, weil sie als Hochtechnologiestandort gilt, viele Konzerne und internationale Organisationen ihren Sitz in der Eidgenossenschaft haben und eine bedeutende Anzahl internationaler Verhandlungen in der Schweiz stattfinden. Ausserdem zählt sie zu den weltweit grössten Exporteuren von proliferationsrelevanten Technologien und Gütern, namentlich Dual-Use-Gütern. Dasselbe trifft auf den Wirtschaftsraum des Kantons Schwyz zu. Weil jedoch kaum Daten vorhanden sind darüber, ob bzw. wie sich die Problematik der Wirtschaftsspionage und der Proliferation im Kanton Schwyz konkret zeigt, geht diese Masterarbeit genau dieser Frage nach.

Ziel war es, mittels einer Online-Umfrage bei Schwyzer Unternehmen diese Datenlücke zu schliessen. Da die Rücklaufquote mit 19 vollständigen Fragebögen (8.5%) bei insgesamt 224 angefragten Unternehmen jedoch ungenügend war, können aus den Umfrageergebnissen keine statistisch signifikanten Erkenntnisse gewonnen und somit keine Aussagen bezogen auf den gesamten Kanton Schwyz gemacht werden. Die Gründe für die mangelnde Teilnahme liegen nicht vor, d. h. es bleibt offen, ob einzelne Unternehmen eventuell zwar von

Wirtschaftsspionage oder Proliferation betroffen waren, jedoch aus allfälligen Sicherheits- oder Datenschutzbedenken auf eine Rückmeldung verzichteten. Die Datenanalyse der Arbeit beschränkte sich folglich auf Stichprobe beschreibende Erkenntnisse und verzichtete auf Analysen mithilfe schliessender Statistik, wie statistische Hochrechnungen oder die Bestimmung von Wahrscheinlichkeiten in Bezug auf die Grundgesamtheit.

Ergänzende Anhaltspunkte lieferten je ein Vertreter und eine Vertreterin zweier Unternehmen, die sich für ausführlichere Interviews zur Verfügung stellten und Auskunft gaben über in ihren Unternehmen festgestellte Vorfälle von Wirtschaftsspionage und Proliferation. In den Gesprächen stellte sich heraus, dass beide Unternehmen Teil internationaler Konzerne sind und dass die Spionagevorfälle sich nicht in der Schweiz, sondern in ausländischen Niederlassungen des einen Konzerns ereigneten. Es besteht allerdings die Vermutung, dass auch die Schweizer Niederlassung wiederholt Ziel versuchter Cyberspionage wurde. Die genaue Absicht hinter den Attacken steht nicht eindeutig fest, weil aufgrund der Schutzmassnahmen solche Angriffe jeweils geblockt werden. Dass hingegen Proliferationsbemühungen im Kanton Schwyz nachweislich stattfinden, bestätigte der Vertreter eines Messtechnikunternehmens, welcher mehrmals pro Jahr proliferationsrelevante Bestellanfragen erhält, die er als solche erkennt und ablehnt sowie konzernintern zu Sensibilisierungszwecken verbreitet. Wo erkennbar, stammten solche Anfragen fast ausnahmslos von Firmen in der Europäischen Union für Russland, was bedeutet, dass die Enddestination der Lieferungen Russland gewesen wäre.

In der Online-Umfrage gab lediglich ein Unternehmen an, im Bereich von Waffen oder Dual-Use-Gütern oder solcher Technologien tätig zu sein, obwohl mehrere Befragte proliferationsgefährdeten Branchen angehören und ihre Güter oder Technologien exportieren dürften. Ob dies daran liegt, dass den Unternehmen die Bedeutung von Dual-Use-Gütern zu wenig bekannt ist und sie folglich hinsichtlich illegaler Beschaffungstätigkeit zu wenig sensibilisiert sind, oder ob es andere Gründe gibt, die mit den Fragen der Umfrage nicht erfasst wurden, ist unklar.

Bei den an der Umfrage teilgenommenen KMUs ist die Schere zwischen sensibilisiert und die Thematik der Wirtschaftsspionage ernst nehmend bis ignorant weit offen. Immerhin ist für rund drei Viertel der befragten Unternehmen Wirtschaftsspionage ein relevantes Thema, auch wenn sich 47% als uninteressant für ausländische, staatliche Akteure erachten. Es bestehen bei fast allen Betrieben präventive Massnahmen, insbesondere zum Schutz der Informationstechnik (IT) und der elektronischen Daten sowie durch Schulung der Mitarbeitenden im richtigen Verhalten im digitalen Umfeld, aber selten ganzheitliche Schutzkonzepte gegen Spionageangriffe. Den Risiken bei Geschäftsreisen ins Ausland, innerhalb der Lieferkette, auf Messen oder an Kongressen sowie bei der eigenen Werbung und dem Webauftritt sind sich die Unternehmen nur kaum bewusst.

Keines der 19 befragten Unternehmen erfuhr in den vergangenen 10 Jahren in der Schweiz einen Vorfall von Wirtschaftsspionage. Ob es keinen gab oder ob er nicht erkannt wurde, bleibt offen. Etwas mehr als die Hälfte der Befragten (58%) würde bei einem erkannten Spionagevorfall eine externe Stelle informieren. Bei einem Grossteil wäre dies die Polizei, und lediglich fünf Unternehmen gaben an, sich an den Nachrichtendienst des Bundes zu wenden. Mehrere Befragte nannten andere Behörden und Organisationen, was den Eindruck erweckt, dass vielen Unternehmen die Zuständigkeiten nicht klar sind. Als häufigster Grund (63%) bei jenen, die nicht wissen, ob sie eine externe Stelle über den Vorfall orientieren würden, wurde das Bedürfnis genannt, zunächst situativ Risiken und Chancen abzuwägen.

Das seit 2004 existierende Sensibilisierungs- und Präventionsprogramm «Prophylax» des NDB ist einem der 19 Umfrageteilnehmenden bekannt. Angesichts der durchschnittlichen Sensibilisierungsrate der Befragten im Bereich Wirtschaftsspionage und der praktisch gänzlich fehlenden Sensibilisierung in Bezug auf Proliferation müssten die Prophylax-Bemühungen wieder intensiviert werden, welche seit circa 2020 im Kanton Schwyz stark zurückgingen. Da Verbände als Multiplikatoren in der Kommunikation wirken, wäre für eine effizientere Sensibilisierung zu begrüssen, dass der NDB über Branchenverbände und Handelskammern mit den Unternehmen in Kontakt tritt.