„Die wirtschaftliche und gesellschaftliche Stabilität ist in Gefahr“

Spionageexperte Alexander Huber über die Auswirkungen des Ausspähens

Welchen Schaden richtet Wirtschaftsspionage an – ökonomisch, politisch, gesellschaftlich? Und wie können wir uns dagegen schützen? Alexander Huber, Spezialist für Unternehmenssicherheit, warnt im Gespräch mit der *IP*: Die Gefahr wird in Deutschland immer noch unterschätzt. Vor allem kritische Infrastrukturen wie die der Energiewende sind akut bedroht.

IP: *Herr Huber, nach Schätzungen beträgt der Schaden, der Deutschland durch Wirtschaftsspionage entsteht, mindestens 50 Milliarden Euro jährlich. Ist das realistisch?*
Alexander Huber: Die vorliegenden Zahlen und Studien bieten uns nicht mehr als ein Stochern im Nebel. Was sagt es denn aus, dass der potenzielle Schaden bei einer oder hundert Milliarden Euro liegt? Außerdem färbt die Herkunft der meisten Studien die Ergebnisse. Angenommen, Sie arbeiten an einer Studie für eine Beratungsfirma, und die Vorgängerstudie hat einen Schaden von 70 Milliarden Euro errechnet. Wenn Sie dann mit Ihrer neuen Studie zum Schluss kommen, jetzt sind es nur 60 Milliarden, wie sähe das aus?

IP: *Nach Entwarnung?*
Huber: Genau. Eine Beratungsfirma will die Angst schüren, um Aufträge zu erhalten; eine Behörde will ihr Handeln legitimieren oder kämpft um zusätzliche Mittel. Solange die Studien so hohe Unsicherheiten aufweisen, was Erhebung, Analyse und Interpretation angeht, können wir keine Schlüsse über die zeitliche Veränderung ziehen – und schon gar keine Schlüsse aus den absoluten Zahlen.

IP: *Wie lassen sich Schäden wie der Verlust von geistigem Eigentum, mögliche Marktmanipulationen oder die Kosten für erhöhten Sicherheitsaufwand denn überhaupt beziffern?*
Huber: Da gibt es verschiedene Modelle. Zum Beispiel das Lizenzmodell: Wenn bestimmte Informationen „abgeflossen“ sind, kann ich keine Lizenzen mehr verkaufen. Nur stellt sich die Frage: Was genau wären denn solche Lizenzen überhaupt wert gewesen? Wir können aber auch versuchen, geschmälerte Wettbewerbsfähigkeit als Kriterium zu nehmen, weil dadurch die Gewinne

zurückgehen. Oder die volkswirtschaftliche Perspektive: der Wegfall von Arbeitsplätzen zum Beispiel. Doch alle Versuche, sich dem Thema zu nähern, scheitern letztlich daran, dass kaum ein Unternehmen den erlittenen Schaden kennt oder offen beziffern wird. Ein Geschäftsführer oder ein Vorstand haftet mit seinem Privatvermögen, wenn er die kaufmännische Sorgfalt vernachlässigt. Der wird in der Regel Besseres zu tun haben, als die Polizei oder den Verfassungsschutz im Detail darüber zu informieren, was er falsch gemacht hat.

IP: *Was sind denn die großen Einfallstore für Wirtschaftsspionage? Ist es der Mobilfunk, ist es die E-Mail?*
Huber: Laut einer aktuellen Studie der Beraterfirma Pricewaterhouse Coopers verschlüsselt jedes fünfte Unternehmen seine Mobilfunkkommunikation zusätzlich. Nun ja. Ich kenne die Situation in vielen Unternehmen, und ich habe noch nie erlebt, dass in einem nicht geheimschutzbetreuten Unternehmen Kryptotelefone eingesetzt wurden. Immerhin: Zumindest die Vorstände haben in einigen Firmen abhörsichere Festnetzleitungen, die auch tatsächlich verschlüsselt sind. Viel wichtiger aber: Es gibt in Deutschland jede Menge von den so genannten „Hidden Champions“ – mittelständische Unternehmen mit 200, 300 Mitarbeitern, die sich auf ein bestimmtes Segment wie etwa Pumpentechnik spezialisiert haben und darin Weltmarktführer sind. An diese Unternehmen kommen Sie als Wirtschaftsspion sogar ausgesprochen leicht heran. Sehr beliebt ist da zurzeit das Thema Vorstellungsgespräche: Über einen Headhunter wird ein Mitarbeiter zum Beispiel aus der Entwicklungsabteilung angesprochen, zu einem vermeintlichen Bewerbungsgespräch eingeladen und über den Betrieb ausgefragt. Da fehlt die Sensibilisierung der Mitarbeiter – und zwar vollkommen.

PROF. ALEXANDER HUBER lehrt Betriebswirtschaftslehre an der Beuth Hochschule für Technik in Berlin. Zu seinen Schwerpunkten gehören Strategische Planung, Informationsschutz und Unternehmenssicherheit. Zuvor war Huber bei Accenture in der IT-Beratung und als Mitglied des Führungskreises bei Siemens im Bereich Corporate Development tätig.

IP: *Wie stellen wir denn fest, ob Wirtschaftsspionage stattgefunden hat?*
Huber: Es gibt da ein paar Indikatoren. Am eindeutigsten ist der Fall natürlich, wenn Mitarbeiter oder Studenten beim Abschöpfen von Informationen ertappt werden. Einer der bekanntesten Fälle hat sich an meiner eigenen Hochschule ereignet. Da wurde ein chinesischer Austauschstudent an ein Ingenieurbüro vermittelt. Eines Abends machte der Geschäftsführer des Büros seine Runde und sah, dass neben dem Schreibtisch des Studenten alles blinkte und flackerte. Der wurde misstrauisch, hat die Polizei verständigt und die den Verfassungsschutz.

IP: *Und wenn die Täter nicht auf frischer Tat ertappt werden?*
Huber: Dann bietet sich noch beispielsweise auf internationalen Messen die Gelegenheit, eine Verletzung von geistigem Eigentum oder Schutzrechten nachzuweisen. Da passiert es schon mal, dass die Mitarbeiter eines deutschen Unternehmens auf Produkte stoßen, die den eigenen verdächtig ähneln. Nicht nur im Design, sondern auch in der Funktionsweise. Denn das eigentliche Know-how liegt im zugrundeliegenden Code und in der Verdrahtung der Bauteile. Und schließlich ist da noch das Thema Zertifizierung. Der Export in bestimmte Länder setzt Produkttests und Werksaudits voraus. So dürfen Waren aus den meisten technischen Branchen nur nach China eingeführt werden, wenn sie das Siegel der China Compulsory Certification haben. Dazu werden nicht nur die Produkte untersucht, sondern auch die Werke, also auch die Produktionsverfahren. In Einzelfällen, etwa wenn es um Kryptografie geht, verlangen die Chinesen sogar die Offenlegung des Quellcodes. Wir im umgekehrten Fall nicht.

„Auf Messen findet man schon mal Produkte, die den eigenen ähneln“

IP: *Sind die Deutschen zu unbedarft?*
Huber: Ich will mal ein Beispiel nennen. Das Deutsche Forschungsnetzwerk hat eine Ausschreibung veranstaltet. Mitbewerber waren deutsche, europäische und amerikanische Unternehmen sowie die chinesische Firma Huawei. Das Angebot der Chinesen war um wenige Prozentpunkte günstiger als das der anderen Anbieter. Nun sieht das deutsche Vergaberecht vor, dass man als öffentliche Institution zwingend das günstigste Angebot nehmen muss. Also erhielt die chinesische Seite den Zuschlag. Mit der Folge, dass die Kommunikation des gesamten deutschen Forschungsnetzwerks über chinesische Netzwerktechnik läuft. Die Amerikaner sind da vorsichtiger. Huawei etwa steht bei ihnen auf dem Index, weil sie davon ausgehen, dass die Firma heimlich Backdoors einbaut. Die Amerikaner haben Angst vor Wirtschaftsspionage – die Deutschen vor Verstößen gegen das Vergaberecht.

IP: *Sie haben einmal erklärt, gegen gezielte Angriffe von Nachrichtendiensten seien Unternehmen chancenlos. Es gehe eher darum, die Hürden für nicht nachrichtendienstlich gestützte Angreifer möglichst hoch zu setzen und „Lücken zu schließen, die vielerorts scheunentorweit offen stehen“. Welche sind das?*
Huber: Ein Anfang wäre schon gemacht, wenn es den Unternehmen gelänge, ihre Mitarbeiter zu sensibilisieren. Sie könnten 99 Prozent der Angriffe abwehren, indem sie sich auf drei wesentliche Grundlagen beschränken: IT, Telekommunikation, Mitarbeitersensibilisierung.

IP: *Wenn es um den Schutz gegen Hauseinbrüche geht, pflegen die Sicherheitsexperten zu sagen, es genüge, wenn der Einbrecher das Schloss in den ersten Minuten nicht aufbekommt …*
Huber: Das Beispiel verwende ich auch gern. Zwei, drei Minuten hat ein Einbrecher Zeit. Wenn er es dann nicht geschafft hat und die Gefahr steigt, dass

jemand ihn entdeckt, dann gibt er auf. Eigentlich müsste es die deutsche mittelständische Industrie hinbekommen, alles zumindest so gut abzusichern, dass ein Spionageangriff zu aufwändig und zu gefährlich ist.

IP: *Und warum wird es nicht gemacht?*
Huber: Ich glaube, es wird noch einige Zeit brauchen, bis sich die deutschen Mittelständler des Gefahrenpotenzials überhaupt so recht bewusst sind. Die machen sich Gedanken darüber, ob sie ihre Pumpen in die USA exportieren oder ob sie eine Niederlassung in Schanghai aufmachen. Über den Schutz ihrer Firma machen sie sich in der Regel nicht ganz so viele Gedanken. Denn ihr Erfolg wird nicht daran gemessen, wie gut ihre Firma gegen Spionage geschützt ist, sondern an ihrem Umsatz und ihrem Gewinn. Und es gibt einfach noch zu wenige Fälle, in denen Firmen durch Wirtschaftsspionage eindeutig messbare Nachteile haben. Das Abfließen von Wissen spiegelt sich nicht in den Bilanzen wider. Das spiegelt sich allenfalls darin wider, dass ein Wettbewerber aus China sich ein paar Monate oder ein Jahr Entwicklungsaufwand sparen kann. Und auch das wird die Firma im Zweifel gar nicht mitkriegen.

„Der Abfluss von Wissen spiegelt sich nicht in den Bilanzen wider“

IP: *Die wachsende Zahl von Spionagefällen führen Experten zum Teil auf den Abbau der Stammbelegschaften in den Unternehmen zurück. Auch ein Edward Snowden war ja kein Festangestellter der NSA. Sind Mitarbeiter, die mit den Firmen nur lose verbunden sind, potenzielle Einfallstore für Cyberspionage? Und ist das Problem nicht letztlich auch eins der mangelnden Loyalität und damit der Unternehmenskultur?*
Huber: Das Betriebsmodell aus früheren Zeiten, „von der Stammhauslehre bis zur Rente“, das gibt es so nicht mehr. Mit diesen gebrochenen Arbeitsverhältnissen müssen wir zu leben lernen. Ich glaube aber, das ist machbar. Hätte die NSA Edward Snowden im Vorhinein aussortieren können? Hätte es Kriterien gegeben, die dazu geführt hätten, dass er durchs Raster fällt? Das kann ich mir nicht vorstellen. Er war bei der Firma Booz Allen Hamilton angestellt, nicht bei der NSA. Aber Booz Allen Hamilton ist ein etablierter Sicherheitspartner der US-Regierung. Snowden hatte durch seinen Werdegang den besten Leumund, den man sich nur vorstellen kann. Und er war ja auch kein leitender Mitarbeiter, sondern ein Systemadministrator.

IP: *Wettbewerbs- und Innovationsfähigkeit ist ein wesentlicher Faktor für den Erfolg einer Wirtschaft – das gilt in ganz besonderem Maß für eine Exportnation wie Deutschland. Ist der Schutz vor Wirtschaftsspionage auch ein Faktor nationaler Sicherheit? Was können Politik und Geheimdienste dazu beitragen?*
Huber: Im Vergleich zu den amerikanischen Diensten sind unsere Behörden Winzlinge, und sie werden von den Amerikanern auch nicht ernst genommen. Nehmen wir alle drei einschlägigen nichtmilitärischen deutschen Behörden zusammen – das Bundesamt für Verfassungsschutz, den Bundesnachrichtendienst

und das Bundesamt für Sicherheit in der Informationstechnik – dann stellen wir fest, dass allein die NSA um ein Vielfaches stärker besetzt ist als alle unsere Dienste zusammen. Die NSA hat 40 000 Mitarbeiter, das Bundesamt für Sicherheit in der Informationstechnik gerade mal 600. Dabei ist das aus meiner Sicht eine ganz wichtige Behörde, der in Zukunft weitaus mehr Aufgaben zukommen werden – gerade für den Schutz der kritischen Infrastruktur. Wir tun viel zu wenig, um die Behörde dafür auszustatten und vorzubereiten.

IP: *Ausgerechnet hochgradig brisante Infrastruktur wie die der Energiewende gilt als besonders anfällig für Angriffe von außen. Ist der Schutz dieser Strukturen im Zweifel nicht genauso wichtig wie der vor Wirtschaftsspionage?*
Huber: Wahrscheinlich sogar wichtiger. Und das ist ein Punkt, der leider noch gar nicht auf unserer Agenda steht. Das Thema wird seit den neunziger Jahren diskutiert, aber so nonchalant, dass es mir große Sorge macht. Die eigentliche Bedrohung – und das ist es, was Snowdens Enthüllungen uns lehren – ist eben nicht der Abfluss einzelner Geschäftsgeheimnisse, sondern die Gefährdung der wirtschaftlichen und gesellschaftlichen Stabilität. Sie nennen das Stichwort Energie: Viele Unternehmen in dieser Branche sind privatwirtschaftlich organisiert. Warum nun sollte ein Energieversorger massiv in Sicherheitstechnik investieren, wenn er genau weiß, dass ihn selbst ein ganzer Tag, an dem der Strom ausfällt, nur einen Bruchteil seines Jahresumsatzes kostet und ihm ein bisschen schlechte Presse bereitet? Die volkswirtschaftlichen Kosten, die ein Blackout auslöst, trägt ja nicht der Energieversorger. Und die liegen natürlich um ein Vielfaches höher. Wir haben hier also eine Form des Marktversagens.

„Warum sollte ein Energieversorger in Sicherheit investieren?“

IP: *Da wäre also der Staat in der Pflicht?*
Huber: Im Grunde schon. Aber in allen Papieren, die man von der Bundesregierung dazu liest, ist von Selbstverantwortung und freiwilligem Handeln der Netzwerkinfrastrukturunternehmen die Rede. Und genau das werden die nicht machen. Schon gar nicht, wenn dahinter Investmentfonds aus China oder den USA stehen. Denen ist es ja völlig gleichgültig, ob in Deutschland mal für einen Tag das Licht ausgeht.

IP: *Welche Rolle spielen die privaten Sicherheitsfirmen?*
Huber: Früher lief das in der Regel so: Es gab einen bestimmten Bedarf, zum Beispiel den, für Botschaften eine sichere Datenübertragung zu gewährleisten. Dieser Bedarf wurde über die entsprechenden Ministerien an das Bundesamt für Sicherheit in der Informationstechnik (BSI) herangetragen, und das hat dann einen Entwicklungsauftrag an eine Firma wie Rohde & Schwarz oder SecureNet gestellt. Die haben dann ein paar Jahre an einer entsprechenden Informationsplattform gearbeitet, und anschließend wurde die vom BSI zertifiziert – ein typisch deutsches System. Dauert alles ein bisschen länger, ist dafür aber auch doppelt so gut.

IP: *Und heute?*
Huber: Heute läuft das meistens anders. Deutschland hatte mal eine funktionierende Sicherheitswirtschaft, aber die ist in weiten Teilen zusammengebrochen. Die wichtigsten Partner der Bundesregierung sind immer noch Rohde & Schwarz und die SecureNet. Rohde & Schwarz entwickelt traditionell Produkte zur sicheren Sprachübertragung, SecureNet Produkte zur sicheren Datenübertragung. Derzeit setzen die deutschen Firmen rund 300 Millionen Euro um – zusammengerechnet. Unternehmen wie Thales aus Frankreich oder die US-Firma General Dynamics setzen in den Geschäftsbereichen, die sichere Sprach- und Datenkommunikation umfassen, jeweils rund eine Milliarde Euro um. Insgesamt liegt das weltweite Marktvolumen bei ca. zehn Milliarden. Der deutsche Marktanteil ist also verschwindend gering.

„Der Sicherheitsmarkt wäre prädestiniert für deutsche Firmen“

IP: *Mit der Folge, dass die Firmen aus den USA oder Frankreich den Zuschlag bekommen?*
Huber: In der Regel schon. Schnell heißt es: Das Produkt gibt es ja eigentlich schon. Warum sollte ich da eine deutsche Firma beauftragen, das in mühevoller Kleinarbeit zu entwickeln? Warum nicht bei Cisco ein Verschlüsselungsgerät für 1200 Euro kaufen – die Amerikaner sind ja NATO-Partner? Und so geraten die deutschen Unternehmen in einen ruinösen Preiswettbewerb. Das ist schade, weil dieser Markt eigentlich prädestiniert für deutsche Firmen wäre. Nicht nur, weil wir über die Ingenieure verfügen. Wir gelten auch als neutral und glaubwürdig – anders als etwa die Amerikaner.

IP: *Wenn es um den Schutz der kritischen Infrastruktur eines Landes und damit um Vertrauen geht, sollte man da nicht im Zweifel eher die einheimischen Firmen beauftragen? Und, da wir ja gerade dabei sind, eine europäische Energieinfrastruktur zu entwickeln: Warum nicht statt Cisco eine europäische Firma beauftragen?*
Huber: Im Prinzip völlig richtig. Aber was die deutsche Sicherheitsindustrie angeht, da dürfte der Zug mehr oder weniger abgefahren sein. Wir müssten jede Menge Geld in die Hand nehmen, um auch nur annäherungsweise mit den Großen mithalten zu können. Realistischer wäre es, sich zumindest auf europäischer Ebene nach dem Vorbild von EADS zusammenzuschließen. Da könnten dann die Box von Thales aus Frankreich stammen und der eingebaute Krypto-Chip aus deutscher Produktion. Die EU verfügt ähnlich wie Deutschland über eine gewisse Glaubwürdigkeit, die sie für den Export nutzen kann. Und wenn wir das auf die europäische Ebene heben, müssen wir uns auch nicht mit dem Problem herumärgern, dass jedes Land seine eigenen Standards einführt, die dann wieder für viel Geld mit den anderen abgeglichen werden müssen. Es wäre ausgesprochen sinnvoll, da neue Wege der Zusammenarbeit zu finden. Leider sind wir davon derzeit noch ziemlich weit entfernt.

Das Interview führten Joachim Staron und Sylke Tempel