Florian Peil zur Industriespionage durch Verbündete

„Wir müssen aufwachen – und wichtige Informationen besser schützen"

Nebeneffekt der öffentlichen Aufregung über das mit hoher Wahrscheinlichkeit von der NSA abgehörte Partei-Handy der Kanzlerin ist, dass nun auch offen über die Möglichkeit von Wirtschaftsspionage durch westliche Partner diskutiert werden kann. Im Gespräch mit Florian Peil, Head of Intelligence bei der deutschen Sicherheitsberatung Riskworkers, haben wir nach möglichen Konsequenzen gefragt*.

Bei einer Umfrage des BDI im Juli dieses Jahres hatten 78% der befragten Unternehmen geäußert, die NSA-Abhörmaßnahmen betreffen die deutsche Wirtschaft „hoch oder sehr hoch". Wie plausibel ist es, dass nicht nur die „üblichen Verdächtigen", etwa russische oder chinesische Dienste, die deutsche Wirtschaft im Fokus haben?

Florian Peil: Das ist durchaus plausibel. Was jedoch NSA und GHCQ angeht, so haben wir dafür bislang keinen handfesten Beweis. Wir warten immer noch auf eine offizielle Antwort der NSA, wen und was sie hier in Deutschland ausgespäht hat. Aber die Hinweise sind eindeutig. Man muss sich nur einmal die Statuten der beiden Dienste anschauen, dann wird schnell klar, dass es da nicht nur um Terrorismusabwehr geht. Das „economical well-being" Großbritanniens zum Beispiel wird da explizit genannt. Häufig wird das Spionieren auch damit begründet, dass man die Korruption bekämpfen müsse. So werden Unternehmen etwa besonders bei der Auftragsvergabe unter die Lupe genommen.

Staatliche Wirtschaftsspionage oder auch die private Konkurrenzspionage sind keine neue Erfindung, worin liegt – abgesehen von der Erregung, dass es sich bei den Angreifern um „Partnerdienste" handelt – das Besondere der NSA und GCHQ-Aktivitäten?

Florian Peil: Das Besondere ist das geradezu obszöne Ausmaß, mit der das Ganze seit Jahren betrieben wird. NSA und GHCQ haben den Status des Sammelns ja längst hinter sich: Sie speichern schlicht das gesamte Netz – und das Tag für Tag.

Florian Peil, Head of Intelligence bei der deutschen Sicherheitsberatung Riskworkers GmbH und ehemaliger Mitarbeiter eines deutschen Nachrichtendienstes, geht davon aus, dass auch die nachrichtendienstlichen Massendatensammlungen, wie sie jetzt von NSA und GHCQ bekannt wurden, die aber auch die russischen und chinesischen Geheimdienste betreiben, direkt oder mittelbar für die Industriespionage genutzt werden. Awareness und konkrete Informationsschutzmaßnahmen seien insbesondere im Mittelstand nötig.
Kontakt: florian.peil@riskworkers.com

Was die Aufregung über die Aktivitäten unserer sogenannten „Partner" angeht – die ist schlicht naiv. Ich bezweifele, dass die USA Deutschland jemals als ernstzunehmenden Partner gesehen haben. Die Freundschaft ist da eher einseitig. Wir müssen endlich aufwachen und akzeptieren, dass auch unsere Verbündeten uns ausspionieren – selbst wenn wir so anständig sind, das nicht zu tun. „Partnerschaft" heißt eben überall etwas Anderes. Empörung hilft da wenig.

Muss ein Unternehmen heute also davon ausgehen, dass Telefonkonferenzen, der Mail-Verkehr mit Anwälten, die Buchhaltungs- und Mitarbeiterdaten ... – eigentlich alles was an Informationen den Weg über öffentlich zugänglich Leitungen findet, auch in einigen Jahren bei leistungsfähigen Nachrichtendiensten noch gespeichert und auswertbar ist?

Florian Peil: Ja, damit müssen die Unternehmen rechnen. Sämtliche Daten können zeitlich unbegrenzt gespeichert werden. Bei der NSA gibt es keine Aufbewahrungsfrist, weil die amerikanischen Datenschutzgesetze nur für US-Bürger gelten. Die Briten speichern alle Daten aktuell immerhin 30 Tage lang. Besonders aufschlussreich im Hinblick auf die Aktivitäten eines Unternehmens sind zum Beispiel internationale Finanzdaten oder auch Reisedaten.

Dabei sind sowohl Verbindungsdaten wie auch Inhalte für die Angreifer interessant. Aus den Verbindungsdaten können sie sehr viel über die Aktivitäten eines Unternehmens lernen, etwa mit wem wann wo gesprochen wird, welche Gelder an wen fließen etc. Sind Spione indes auf konkrete Technologien aus, dann geht es natürlich um Inhalte.

Das Interview wurde am 20.11.2013 geführt.

Bild: Ministry of Defence

Der Komplex des Government Communications Headquarters (GCHQ) in Cheltenham (GB)

An diese Kronjuwelen kommen die Angreifer allerdings oft nur durch klassische Methoden wie der Aufklärung durch menschliche Quellen – HUMINT. Diese lassen sich durch Technik nicht ersetzen. Liegen die wichtigsten Informationen nicht als Dateien vor, sondern nur auf Papier im Panzerschrank, dann kommt ein Nachrichtendienst nur daran, wenn er Mitarbeiter anwirbt oder einschleust.

Wie muss man sich das vorstellen, wenn Nachrichtendienste im Interesse der nationalen Wirtschaft spionieren?
Florian Peil: Wenn Nachrichtendienste nicht nur abhören, sondern gezielt angreifen, dann auf zwei Schienen: entweder über die IT oder über das Personal. Dienste könnten versuchen, Trojaner in das Zielsystem einzuschleusen. Auf diese Weise können sie später die infizierten Systeme fast beliebig steuern oder Informationen entwenden. Insbesondere Smartphones sind da sehr anfällig. Skepsis ist mitunter geboten, wenn ein neuer Geschäftskontakt aus dem Ausland entsteht, der schwer einzuschätzen ist. Wenn dieser dann eine Präsentation vorführen will und zu diesem Zweck seinen USB-Stick an Ihren Computer anschließt – dann ist das System danach vielleicht schon infiltriert. Auch der Einsatz von Praktikanten oder Gaststudenten aus dem Ausland ist nach wie vor sehr beliebt. Die haben, gerade in kleineren Unternehmen, schnell überall Zugang. Kaum einer fragt nach, wenn die Neuen bevorzugt am Wochenende arbeiten oder abends erst als letzte gehen. Da sollten die Alarmglocken schrillen. Heute ist eine sorgfältige Überprüfung von Geschäftspartnern und auch neuer Mitarbeiter, gerade aus dem Ausland, durch entsprechende Due-Diligence-Recherchen und Background Checks wichtiger denn je.

Aber warum betreibt ein Nachrichtendienst diesen sehr speziellen Aufwand, wenn ihm ohnehin die gesamte Kommunikation und deren Inhalte live oder als Aufzeichnung zur Verfügung stehen?
Florian Peil: Ein Nachrichtendienst weiß ja nie mit Sicherheit, ob er die gesamte relevante Kommunikation mitbekommt. Das ist äußerst unwahrscheinlich. Kommunikation gibt es ja glücklicherweise auch immer noch von Angesicht zu Angesicht, und nicht immer können die Gesprächspartner dabei abgehört werden. Mit einigen simplen Maßnahmen können Abhörversuche unterlaufen werden.

Was die neuen Möglichkeiten des Scannens und Speicherns riesiger Datenmengen angeht, so bieten diese potentiellen Angreifern heute einfach mehr Zeit für die Auswertung – auch rückwirkend. Sie haben nun alle Zeit der Welt, um die Teile eines Puzzles zusammenzusetzen. Früher wären diese Informationen einfach verloren gewesen. Da hätten sie vielleicht gar nicht erkennt, dass sie ein Puzzle vor sich haben.

Ich sehe die Datenflut aber nicht nur als Gefahr, sondern auch als Chance: Erstmals in der Geschichte stehen die Nachrichtendienste vor dem Problem, dass sie an Informationen zu ersticken drohen. Je mehr die Dienste sammeln, desto mehr Kapazitäten brauchen sie zur Auswertung. Da stößt man irgendwann an die Grenzen. Die besondere Herausforderung für die Dienste besteht daher heute mehr als früher darin, Sinn aus den gesammelten Informationen zu generieren.

Die NSA, die bei ihrer Datensammlung allein in den USA täglich bis zu 29 Petabytes an Daten speichern soll, das sind mehr als 10.000.000 Terabyte Material pro Jahr, scheint damit kein Problem zu haben. Reichen die aktuellen Big-Data-Technologien schon aus, um „live" oder nachträglich in zwangsläufig heterogenen Daten gewünschte Informationen zu extrahieren?
Florian Peil: Da widerspreche ich. Die Auswertung bleibt auch für die NSA die große Herausforderung, auch wenn sie technisch sicherlich ganz vorne ist. Und erst die Auswertung schafft aus Daten Wissen. Entscheidend bleibt der Mensch, der hinter der Technik steht, der die richtigen Fragen formulieren und relevante Informationen als solche erkennen muss. Was nun die aktuellen Technologien angeht, so lassen sich damit bereits unterschiedlichste Informationen auffinden, Muster erkennen und Zusammenhänge herstellen. Dazu brauchen Sie aber nicht die NSA. Im kleineren Maßstab steht diese Möglichkeit auch Unternehmen offen. Entsprechende Software gibt es bereits auf dem Markt.

Nachrichtendienste sind ja normalerweise im Auftrag ihrer Regierung unterwegs. Es kann wohl kein CEO bei der NSA anrufen und diese beauftragen, die Entwicklungen eines deutschen Wettbewerbers auszuspähen – oder?
Florian Peil: Wenn wir Abläufe dieser Art kennen würden, dann hätten diese Nachrichtendienste versagt. Derartige Verbindungen, sofern sie überhaupt offiziell bestehen, werden ja nicht offen kommuniziert.

Was den militärischen Bereich angeht, so wissen wir etwas mehr. Grundsätzlich ist hier die Zusammenarbeit zwischen privaten Unternehmen und den staatlichen Stellen sehr eng. Zudem berührt dieser Bereich die nationale Sicherheit: Natürlich wollen die USA wissen, welche Technologien auf der Welt entwickelt werden. Die Aktivitäten von EADS zum Beispiel sind für die Amerikaner hoch interessant. Und da kommen dann die Nachrichtendienste zum Einsatz.

Frankreich hat kürzlich übrigens offen zugegeben, Wirtschaftsspionage zu betreiben. China und Russland wiederum haben ihrer kommunistischen Vergangenheit wegen in dieser Hinsicht eine andere Tradition. Die Verflechtungen zwischen Wirtschaft und den Diensten

sind enger. Russische Dienste sind zum Beispiel gesetzlich verpflichtet, auch wirtschaftlich relevante Daten zu sammeln. Und auch Indien ist da zunehmend aktiv.

Also sollte jedes Unternehmen, das von einem relevanten US-amerikanischen, britischen, französischen, indischen, russischen oder chinesischen Unternehmen als nennenswerter Wettbewerber wahrgenommen werden könnte, mit nachrichtendienstlich unterstützter Ausspähung rechnen?
Florian Peil: Ja, damit müssen diese Unternehmen rechnen. Entweder ihre Wettbewerber beobachten sie ganz genau – oder sogar der jeweilige Nachrichtendienst interessiert sich für sie und ihre Aktivitäten. Unser Rat an die Unternehmen ist deshalb: Machen Sie sich bewusst, dass Inhalte und Kommunikationsdaten sofort oder auch erst in einigen Monaten oder Jahren zu Ihren Wettbewerbern gelangen können. Seien Sie wachsam!

Und wie ist das mit der Compliance: Dürfen Unternehmen solche – aus nationaler Sicht von ihren Nachrichtendiensten legal gesammelte und für sie ausgewertete Informationen auch erhalten oder nutzen?
Florian Peil: In Deutschland ist eine solche Zusammenarbeit undenkbar. Der Verfassungsschutz dient zwar als Ansprechpartner bei Hinweisen auf Wirtschaftsspionage, aber eine Bereitstellung von Informationen ist untersagt. Wollen die Unternehmen Informationen, beispielsweise über Mitbewerber, so müssen sie eigene Intelligence-Abteilungen aufbauen. Im Sinne einer legalen Informationsbeschaffung sind sie dabei allerdings auf das Sammeln und Auswerten offener Quellen beschränkt, der sogenannten Open Source Intelligence – der OSINT.

Ist das in USA und Großbritannien anders?
Florian Peil: Das Verhalten insbesondere der USA ist ja paradox. Die USA versuchen weltweit ihre Compliance-Vorstellungen durchzusetzen und üben in diesem Zusammenhang massiven Druck auf ihre Handelspartner aus, diese Vorgaben ebenfalls umzusetzen. Demgegenüber stehen die massiven Aktivitäten der eigenen Nachrichtendienste – die häufig vorgeblich nur aufklären, um Fälle von Korruption aufzudecken. Da entsteht in der Regel ein hübscher Beifang, der nicht ungenutzt bleibt.

Dann müsste man ja damit rechnen, dass US-Unternehmen auf diesem Weg erworbenes Wissen auch in Deutschland nutzen?
Florian Peil: Ausschließen würde ich das nicht.

Die Cyber-Spionage der NSA wird unterstützt von einer Vielzahl von privaten Unternehmen. Muss man nicht davon ausgehen, dass diese ihr Know-how und eventuelle auch ihre Zugänge legal oder illegal auch direkt im privaten Markt anbieten?
Florian Peil: Davon ist auszugehen. Gerade in den USA hat sich nach dem 11. September eine ganze Industrie rund um das Thema Intelligence gebildet. Dabei sind die Grenzen oft fließend. Mitarbeiter, die heute bei der NSA arbeiten, wechseln morgen zu einem privaten Dienstleister und gehen anschließend wieder zurück. Allein der NSA arbeiten ja mehr als 5.000 Privatfirmen zu.

Im Umkehrschluss könnte man davon ausgehen, dass letztlich jeder, der genügend dafür zahlt, den NSA-Datenschatz nutzen kann?
Florian Peil: Auch das ist nicht auszuschließen. Rund 1,5 Millionen Menschen arbeiten allein für die amerikanischen Dienste. Dass die nicht wirklich zu kontrollieren sind, zeigt das Beispiel von Edward Snowden, der sagte, dass ihm mehr als 20 Mitarbeiter ihre Passwörter verraten hätten. Er hatte ihnen lediglich gesagt, er brauche diese Passwörter für die Erfüllung seiner Aufgaben. Wenn so wenig Sicherheitsbewusstsein auch bei der NSA an der Tagesordnung ist, dann könnten einzelne Mitarbeiter nebenbei einen schwunghaften Handel mit Informationen betreiben.

Know-how-Schutz-Maßnahmen unterliegen oft wirtschaftlichen Zwängen. Gibt es angesichts der Potenz der Nachrichtendienste hinsichtlich finanzieller Mittel, Manpower und Zugriffsmöglichkeiten noch Möglichkeiten, dass Firmengeheimnisse zumindest nicht ganz so einfach aus den Kommunikationsströmen herausgelesen werden? Was sind Ihre Vorschläge für eine Reduzierung der Gefährdung?
Florian Peil: Innovative Unternehmen stehen grundsätzlich vor dem Problem einer möglichen Ausspähung. Die individuelle Gefährdung ist am besten durch eine entsprechende Risikoanalyse festzustellen. Die Gefahr ist unterschiedlich von Land zu Land und je nach Branche. Unterstützung bieten ja auch die deutschen Sicherheitsbehörden im In- und Ausland. Ich empfehle, stets vom worst case ausgehen und sich darauf vorzubereiten.

Entscheidend ist die Etablierung eines ganzheitlichen Informationsschutzes – und der muss dann auch gelebt werden. Für den Fortbestand des Unternehmens wichtige Informationen dürfen erst gar nicht die Firma verlassen. Im Extremfall heißt das: Wichtige Dokumente ausdrucken und nach Gebrauch wieder in den Panzerschrank legen, anstatt sie auf einem Computer zu speichern, der auch noch Zugang zum Internet hat. Neben einer robusten IT-Sicherheitsarchitektur müssen die Unternehmen zudem ihre Prozesse sichern. Von entscheidender Bedeutung aber ist die Sensibilisierung der eigenen Mitarbeiter für potenzielle Sicherheitslücken und Angriffe. Der Know-how-Schutz in jedem Unternehmen steht und fällt mit den Mitarbeitern. Die größte Gefahr geht hier vom Social Engineering aus. Denn oft ist es für Angreifer leichter und schneller, einen Mitarbeiter dazu zu bringen, ihm das Passwort zu verraten, anstatt es selber zu hacken.

Und wie gut sind Sie vorbereitet? Auch Ihr Unternehmen kommt ja mit sensiblen, möglicherweise für Spionage attraktive Kundendaten in Kontakt.
Florian Peil: Kundendaten befinden sich ausschließlich auf Computern ohne Verbindung zum Internet. Daneben kommt deutsche Verschlüsselungssoftware zum Einsatz. Alle unsere Mitarbeiter sind zudem sicherheitsüberprüft und für die Gefahr durch Spionage-Angriffe sensibilisiert. Und schließlich sind da noch unsere Compliance-Regeln.