Archiv

Innere Sicherheit, Informationsschutz

Ausspähung und Konkurrenzspionage durch Profis und Ex-Geheimdienstler bei ausländischen Sicherheitsberatungsfirmen

Von: Stefan Bisanz

Über die Hälfte aller deutschen Unternehmen ist bereits Opfer von Industriespionage geworden. Das ist das Ergebnis der Studie „Industriespionage 2012“ der Sicherheitsberatung Corporate Trust. Im Fokus stehen mittelständische Unternehmen, die mit 23,5 Prozent am meisten geschädigt wurden. Mit 18,5 Prozent folgen große Konzerne, danach sind Kleinunternehmen mit 15,6 Prozent am dritthäufigsten im Visier der Angreifer.

Der deutschen Wirtschaft entsteht durch Industriespionage jährlich ein Gesamtschaden von ca. 4,2 Milliarden Euro, und die Schäden steigen weiter an. Einerseits werden die Unternehmen geschädigt durch Wirtschaftsspionage als staatlich gelenkte oder gestützte Ausforschung von Betrieben durch fremde Nachrichtendienste; anderseits durch Industrie- bzw. Konkurrenzspionage als Ausforschung, die Wettbewerber oder private Sicherheitsdienstleister in deren Auftrag betreiben. Folgende Abgrenzungen sind vorzunehmen:

Abb. 1 – Informationsgewinnung mit wirtschaftlicher Zielsetzung

	legale Beschaffung	illegale Beschaffung
staatlicher Akteur	Wirtschaftsaufklärung	Wirtschaftsspionage
privater Akteur	Business Intelligence/ Competitive Intelligence	Konkurrenzspionage

(Quelle: P. Harbich, Die wachsende Bedeutung privater Akteure im Bereich der Intelligence, Universität Köln, 2006, S. 16)

Die wesentlichen Auftraggeber bei Spionagefällen gegen Unternehmen sind zu 39 Prozent Konkurrenten, zu 19 Prozent Kunden, zu 9 Prozent Zulieferer und zu 7 Prozent Geheimdienste. Spioniert wird von eigenen Mitarbeitern, privaten Spionagefirmen, bezahlten Hackern und Profis der Geheimdienste. Die Methoden der Informationsgewinnung umfassen grundsätzlich das gesamte Geheimdienst-Repertoire und -personal, darunter Agenten aus Residenturen, Wirtschaftsjournalisten, Praktikanten, technische Informationsgewinnung etc. Wirtschaftsspionage ist dabei keine Frage der Unternehmensgröße, sondern der

Attraktivität von Firmendaten und -informationen. Das Risiko von Wirtschaftsspionage wird in Deutschland deutlich unterschätzt. Kleine und mittelständische Unternehmen sind besonders im Forschungs- und Entwicklungsbereich sehr innovativ, machen sich jedoch noch zu selten Gedanken über den Schutz ihrer Forschungsergebnisse und Produktideen.

Ausspioniert werden die Unternehmen fast immer von Profis – entweder von Mitarbeitern ausländischer Geheimdienste oder von privaten Sicherheitsfirmen. Der Täterkreis muss dabei nicht unbedingt unterschiedlich sein, denn viele frühere Mitarbeiter von Sicherheitsbehörden machen sich nach dem Ausscheiden aus dem aktiven Dienst selbstständig. Ihr Know-how und ihre Netzwerkkontakte nehmen sie mit; und machen ihre Fähigkeiten in der Privatwirtschaft zu Geld. Das Phänomen „Private Intelligence Services“ hat besonders nach dem Ende des Kalten Krieges rasant zugenommen; und das aus gutem Grund: Die Staaten in West und Ost gingen daran, ihre Nachrichtendienste zu reorganisieren und teilweise signifikant zu verkleinern. Damit suchte auch eine Vielzahl hochqualifizierter und professioneller Ex-Geheimdienstler nach zukünftigen Wirkungsmöglichkeiten und fand diese in (selbst gegründeten) privaten Sicherheitsunternehmen, wo sich die erlernten Fähigkeiten nahtlos fortführen ließen.

Nachrichtendienstliche Aktivitäten: Spionage unter Freunden
Weltweit setzen zahlreiche Staaten ihre Dienste permanent auf ausländische Unternehmen an, vor allem auf deren Patente, Geschäfts- und Betriebsgeheimnisse. Es werden Computer, Telefone und Faxgeräte interessierender Firmen „angezapft“ oder Agenten geschickt. Diese Entwicklung hat bewirkt, dass dem Thema Wirtschaftsspionage mittlerweile größere Aufmerksamkeit zuteil wird und dass die Problematik auch politisch aufgegriffen wird.

Mittlerweile spähen staatliche Geheimdienste immer öfter private Unternehmen aus. Der Schaden, der dadurch für deutsche Firmen entsteht, wird von Fachleuten auf 20 bis zu 50 Milliarden Euro pro Jahr geschätzt. Diese Schwankungsbreite erklärt sich aus den Schwierigkeiten, die durch Spionage verursachten Schäden detailliert aufzuklären. Viele Spionageaktionen bleiben unbemerkt, vor allem wenn der Datenabfluss über elektronische Netze erfolgt.

Werden sie jedoch registriert, scheuen sich betroffene Unternehmen oft aus Imagegründen, dies öffentlich zu machen und bevorzugen lieber eine „stille Bereinigung“ der Schäden.

Wirtschaftsspionage staatlicher Geheimdienste wird in Behördenpublikation zumeist China, Russland, dem Iran oder Korea zugeschrieben; mithin den üblichen Verdächtigen. Dies ist zwar grundsätzlich richtig, aber dennoch gefährlich unvollständig. Denn es gibt viele, auch westliche, befreundete Staaten, die in Deutschland Wirtschaftsspionage betreiben. Dazu gehören allen voran die USA, Frankreich, Großbritannien oder Israel. Es ist stets zu berücksichtigen, dass es im jeweiligen nationalen Interesse der Sicherung von Arbeitsplätzen ist, derartige Wirtschaftsspionage zu betreiben.

Die USA sind mit großem Abstand der aggressivste Faktor in der globalen Wirtschaftsspionage. US-Abhörsatelliten selektieren Telefonate, Gespräche und E-Mails und geben die gesammelten Informationen und Daten sehr zeitnah an amerikanische Unternehmen weiter. Kostproben der amerikanischen Spionage-Effizienz bekamen nicht nur Volkswagen, Siemens, BASF, sondern auch Opel zu spüren. Die Schwerpunkte hierbei sind forschungsintensive Industriesektionen wie Computerproduktion, Pharmaentwicklung, Mikroelektronik und jede Form der Kommunikationstechnologie. Gefährdet sind aber nicht nur Großkonzerne, sondern seit geraumer Zeit auch staatliche Forschungseinrichtungen und kreative mittelständische Unternehmen. Durch die anhaltenden US-Finanz- und Wirtschaftskrise haben sich die gezielten Angriffe auf den deutschen Mittelstand verdreifacht. Über eine im Washingtoner Handelministerium angesiedelte Schaltstelle namens 'Office of Intelligence Liaison' gehen die gesammelten Informationen über die ausländische Konkurrenz direkt an führende Wirtschaftsunternehmen der Vereinigten Staaten. Häufig

genannt werden hierbei Unternehmen wie Lockheed, Boeing, McDonnell-Douglas usw., denen es ungewöhnlich häufig gelang, aus Ausschreibungen als Sieger hervorzugehen, weil sie in letzter Minute „modifizierte“ Angebote abgaben. Als offenes Geheimnis gilt darüber hinaus, dass US-Software-Entwickler und Chiphersteller wie Microsoft, Netscape und Intel eng mit der „National Security Agency“ (NSA), dem technischen Geheimdienst der USA, kooperieren, was den Verdacht nahe legt, dass sie in ihre Produkte sogenannte „Trap Doors“ (Hintertüren für staatliche Stellen) einbauen, um staatlichen Wirtschaftsspionen ihre Arbeit zu erleichtern.

Doch auch andere sind sehr aktiv: Im Bereich des Abhörens von Telekommunikation hat der französische Geheimdienst nur für Wirtschaftsspionage momentan 3.400 Mitarbeiter auf befreundete Staaten angesetzt. Die Briten hören ausländische Handys ab, sobald sie ins Vereinigte Königreich gelangen.

Die Frage, ob auch deutsche Nachrichtendienste im befreundeten oder verbündeten Ausland Wirtschaftsspionage betreiben, muss differenziert betrachtet werden. Traditionell ist der Bundesnachrichtendienst sehr zurückhaltend in den meisten „befreundeten Staaten“, was ihm aus Unternehmerkreisen zuweilen den Vorwurf eingebracht hat, ein Standort- und Wettbewerbsnachteil für Deutschland zu sein. In den USA sind keine deutschen Nachrichtendienste aktiv. In anderen Staaten aber ist der BND in wirtschaftlicher Hinsicht sehr wohl aktiv. Zu erkennen war dies z.B. an seiner erste Analyse über Geldwäsche in Liechtenstein und den Daten-CDs mit den Namen deutscher Steuersünder, die dem BND regelmäßig aus Lichtenstein und der Schweiz angeboten wurden.

Die Methoden der Profis

Die Spionagemethoden befreundeter Nachrichtendienste in Deutschland sind sehr unterschiedlich. Die Japaner zum Beispiel betreiben zu 90 Prozent nur offene Aufklärung: Sie werten Prospekte aus, sind auf Messen unterwegs und machen dort Fotos von neuen Produkten, oder sie kaufen etwas ein und zerlegen es dann. Die US-Dienste dagegen gehen aggressiver und auch mit verdeckten Mitteln vor. Das reicht vom Einsammeln von Papiermüll von Unternehmen bis hin zur technischen Spionage, bei der in Computersysteme oder Netzwerke eingedrungen wird. Auch die Swift-Daten werden vom US-Geheimdienst nicht nur zur Terrorabwehr genutzt, sondern auch, um Geldströme der Wirtschaft in Europa nachvollziehen zu können. Für die technische Spionage hat die NSA das Monopol. Die CIA hingegen setzt auf Spionage mit menschlichen Quellen.

Alte Geheimdienst-Tricks sind auch im Internet-Zeitalter noch aktuell. Spionage 2.0 funktioniert genauso wie Spionage 1.0 mit einigen technischen Verbesserungen. Statt spezieller Miniaturkameras verwenden Agenten heute ein Smartphone, um die vom staatlichen Auftraggeber gewünschten Information zu fotografieren. Für die Übermittlung wird aber aus Sorge um Enttarnung in elektronischen Netzen, häufig immer noch ein „toter Briefkasten“ eingesetzt. Auch der „lebende Briefkasten“ hat noch nicht ausgedient – damit bezeichnet man die aus Agentenfilmen bekannte Übergabe von Informationen von Person zu Person.

Die Nachrichtendienste verbinden auch in weiteren Bereichen traditionelle Methoden mit neuen Verfahren. Die Verbindungsmethode schlechthin ist immer noch der ungerichtete A3-Agentenfunk auf Kurzwelle. Die Information über die Frequenz wird ebenfalls meist über einen toten Briefkasten ausgetauscht. Ergänzend zur Kurzwelle werden Informationen auch oft über Satellit übertragen, da eine Schüssel vor allem in Westeuropa auf Grund von deren Anzahl in Privathaushalten völlig unverdächtig erscheint. Wenn digitale Technik bei der Übermittlung von Informationen eingesetzt wird, dann ist es meist die Steganografie, das verborgene Speichern von Informationen in einer äußerlich unauffälligen Bilddatei. Beim Versand solcher Dateien wird ein offenes WLAN bevorzugt, um die eigene Identität zu verbergen. Soll ein Treffen mit dem Kontaktmann vereinbart werden, werden meist bestimmte Code-Begriffe verwendet: Die Mitteilung kann entweder in einer ganz normalen E-Mail verschickt oder auch in bestimmten Chatrooms oder Blogs versteckt

werden. Jeder Nachrichtendienst hat diesbezüglich seinen eigenen Modus Operandi, den er bevorzugt anwendet.

Es ist anzunehmen, dass es für alle Verschlüsselungstechniken in den USA eine „Trap Door“ (Hintertür für staatliche Stellen) gibt. Bei Attacken auf fremde Rechner kommt im Netz aber dennoch das ganze technische Repertoire zum Einsatz. Dabei bedient man sich auch Hacker-Methoden zum Aufspüren und Ausnutzen von Sicherheitslücken. Westliche Nachrichtendienste setzen gern Freiberufler ein, die oft besser qualifiziert sind als festangestellte Mitarbeiter. Sie erhalten dann genaue Zielvorgaben, in welchen Rechner sie eindringen sollen.

Geheimdienst-Profis mit neuem Arbeitgeber

Im Bereich der Sicherheit verschwinden vertraute Grenzziehungen. Das private Sicherheitsgewerbe boomt: Neben dem privaten Objekt- und Personenschutz übernehmen private Sicherheitsdienste zunehmend auch öffentliche Sicherheitsaufgaben. Im Jahr 2010 waren in der Bundesrepublik über 170.000 Personen bei fast 4.000 Sicherheitsunternehmen beschäftigt. Wenn ein Unternehmen Informationen von einem Wettbewerber oder lästigen Kritikern abgreifen will, liegt es nahe, damit Profis zu betrauen, die sich mit Methoden und Verfahren bestens auskennen und bereits zuvor jahrelang in diesem Metier tätig waren. Da trifft es sich gut, dass sich immer mehr frühere Mitarbeiter von Sicherheitsbehörden selbstständig machen; um ihr jahrelang erworbenes Können und Wissen lukrativ einzusetzen.

In den letzten beiden Jahrzehnten ist besonders die wachsende Bedeutung international tätiger Unternehmen (vom Großkonzern bis zum Mittelständler) als eigenständige Akteure in der internationalen Politik hervorzuheben und, damit einhergehend, das Aufkommen privater Sicherheitsdienstleister. Für international tätige Unternehmen ist es für den Geschäftserfolg von entscheidender Bedeutung, die jeweiligen landesspezifischen kulturellen, politischen und sozialen Bedingungen, aber auch die Märkte und Konkurrenten genau zu kennen. Hiermit werden oft ortansässige oder global tätige private Sicherheitsdienstleister betraut.

Kaum ein Unternehmen dieser Branche hat heutzutage keine Ex-Geheimdienstler oder ehemalige Mitglieder von Spezialkommandos in seinen Reihen und vertraut privaten Sicherheitsdienstleistern als Vertragspartner. Sie bringen natürlich nicht nur Wissen auf aktuellem Stand mit, sondern auch Netzwerkkontakte. Es wäre naiv anzunehmen, dass frühere Geheimdienstmitarbeiter im Streit mit ihren Kollegen und Organisationen ausgeschieden sind und hernach sämtliche Kontakte gekappt haben. Zudem wäre ein Nichtverwenden so erworbenen Wissens und so etablierter Kontakte auch geschäftsschädigend, denn gerade das ist ihr Wettbewerbsvorteil. Und Auftraggeber aus dem In- und Ausland bedienen sich gerne ihrer Dienste, denn hier wissen sie, was sie bekommen: Vollprofis mit Krakenarmen.

So sind in den letzten Jahren einige Fälle von Ex-Sicherheitsbehördlern auf der Payroll privater Auftraggeber in aller Welt bekannt geworden:

- Thierry Lorho, Ex-Geheimdienstmitarbeiter des französischen Nachrichtendienstes DGSE, wurde nach seinem Ausscheiden aus dem Dienst Chef der Sicherheitsfirma „Kargus Consultants“, die im Auftrag des französischen Atomkonzerns EDF die unliebsamen Kritiker von Greenpeace ausspähte. Gestohlene Laptops, abgehörte Telefone – die Spionageaffäre um EDF und Greenpeace gleicht einem Thriller. Mittendrin: Lorho und Kargus Consultants. Die französische Staatsanwaltschaft ermittelte 2009, dass Kargus Consultants im Auftrag von EDF zum Beispiel illegal in den Computer des damaligen Greenpeace-Chefs Yannick Jadot eingedrungen ist. Thierry Lorho gab freimütig zu, dass er im Auftrag von EDF, das zu 85 Prozent in französischem Staatsbesitz ist, zu Hacker-Methoden gegriffen hat. Er wurde dafür zu drei Jahren Haft auf Bewährung verurteilt.

- Im Juni 2001 spionierte der britische „Private Intelligence Service“ Hakluyt, der enge Verbindungen zum britischen Auslandsgeheimdienst MI6 hat, NGOs im Umweltbereich für BP und Shell aus. Eine mögliche Verbindung könnte dabei BPs Director of Government and Public Affairs, John Gerson, gewesen sein, der zuvor ein Kandidat als Chef des MI6 war. Die Gründer von Hakluyt waren 1995 ehemalige Mitarbeiter des MI6.

- Das Sicherheitsunternehmen „Group 4“ wurde 2003 von der britischen Regierung mit dem Schutz von umstrittenen Straßenbauarbeiten beauftragt. Group 4 kaufte daraufhin vom privaten Sicherheitsunternehmen R&CA Publications verdeckt gewonnene Informationen über Protestierer. R&CA Publications wurde 2003 von Evelyn Le Chene geleitet, die enge Kontakte zu den britischen Geheimdiensten pflegen soll. Die Firma besitzt zudem ein Netzwerk von Agenten, um eine große Datenbank über linke Aktivistengruppen zu unterhalten. Deren Namen sollen von Le Chene auch an Unternehmen verkauft worden sein.

Die Gefahren, die mit Private Intelligence Services verbunden sein können, liegen auf der Hand, wie – als ein Beispiel von vielen – die Brillstein Security Group auf ihrer Homepage ausführt: „Ein Problem: Wem können Sie in Sachen der Spionagebedrohung trauen? Behörden? Ex-Geheimdienstbeamten? Leider ist es so, dass ja Behörden vielfach mit ausländischen Diensten kooperieren, welche wiederum z.B. in Deutschland und gegen deutsche Unternehmen spionieren! ‚Freelancer’, also die berüchtigten ‚Ex-Nachrichtenleute’, sind ‚Freischaffende’ ohne jede Kontrolle in Bezug auf Loyalität und Können. (...) Es ist wenig ratsam, mit freischaffenden Ex-Geheimdienstleuten zu arbeiten, weil diese zumindest potenziell exakt mit den Gegnern und Spionagequellen zusammen kooperiert haben, die Sie jetzt bedrohen". (Quelle: **http://www.deutschland.eubsa.com/konkurrenzspionage.htm**)

Besser hätte es ein kritischer, unabhängiger Analyst nicht ausdrücken können. Die Gefahr ist auch für deutsche Unternehmen nicht zu unterschätzen, wenn sie mit ausländischen privaten Sicherheitsdienstleistern zusammenarbeiten. Die vermeintlichen Vorteile können sich dann schnell in Nachteile verwandeln, wenn solche ausländischen Sicherheitsanbieter – wovon auszugehen ist – Ex-Mitarbeiter ausländischer Nachrichtendienste beschäftigen. Erstens verfügen sie in der Regel noch über Kontakte und Netzwerke in die jeweiligen ausländischen Dienste, was dann besonders heikel ist, wenn diese Dienste Wirtschaftsspionage gegen deutsche Unternehmen betreiben. Zweitens richtet sich die Loyalität nicht selten am Honorar aus, was Tätigkeiten für mehrere Auftraggeber mit unterschiedlichen (entgegenlaufenden) Interessen erlaubt. Diese Gefahr ist auch bei einheimischen (deutschen) privaten Sicherheitsdiensten nicht auszuschließen, aber dennoch deutlich kleiner.

Denn auch die oben angeführte Brillstein Group mit ihrer treffenden Homepage-Analyse verhält sich branchenüblich und beschäftigt Ex-Mitarbeiter von Sicherheitsbehörden: „In den frühen 1980ern startete der Nachrichtendienst- und Anti-Terrorismus Experte Arik Brillstein seine eigene kleine Sicherheitsfirma, nachdem er etliche Jahre in diversen offiziellen Sicherheits- und Anti-Terrorismuseinheiten diente. Zusammen mit Ex-Kollegen und anderen professionellen von verschiedenen Diensten aus der ganzen Welt (…) begann Arik und sein Team weltweite Sicherheitsdienste anzubieten“ (Quelle: **www.brillstein-security-group.de/about.htm**) Heißt auf deutsch: Auch bei der Brillstein Security Group sind ehemalige Mitarbeiter von Sicherheitsbehörden am Werk, die ihr in früheren Tätigkeiten erworbenes Wissen kommerziell verwerten. „Es ist wenig ratsam, mit Ex-Geheimdienstleuten zu arbeiten“, meint die Brillstein Security Group, es sei denn, es sind die eigenen!

Ein ganz aktuelles Beispiel ist in der neuesten Ausgabe (März/April 2/2013) der SECURITY insight nachzulesen. Gerald Moor, Geschäftsführender Direktor, stellt sein Unternehmen „The Inkerman Group“ aus England vor. Er selbst war lange im Nachrichtendienst der Britischen Armee tätig. Er weist in diesem

Interview außerordentlich auf die bestehenden Kontakte zu Behörden hin, insbesondere auch zum US-Geheim-dienst und den Special Forces (Zitat: „ … wie kaum ein anderer.“) Er möchte mit dem Hinweis auf seine besonders guten Kontakte einen Wettbewerbsvorteil erzielen. Aber was bedeutet die Aussage wirklich? Bedeuten diese Kontakte vielleicht, dass der US-Geheimdienst für die englische Firma „The Inkerman Group“ mehr erwirkt als für andere Gefährdete? Und wenn das so ist, verlangt der US-Geheimdienst etwas dafür? Aber was hätte die Firma „The Inkerman Group“ anzubieten, außer Informationen über ihre (deutschen) Auftraggeber vielleicht? Die wären für die US-Amerikanische Wirtschaft wirklich sehr interessant.

Kein Einzelfall, sondern in der Branche die Regel:

Name	Büros weltweit	Mitarbeiter mit nachrichtendienstlichem Hintergrund	Private Kunden	Staatl. Kunden	Sitz
Control Risks	23	+	✓	✓	London, GB
Stratfor	2	+	✓	✓	Austin, USA
Kroll & Associates	65	+	✓	✓	New York, USA
Diligence	8	++	✓		Washington, USA
Economist Intelligence Unit	40		✓	✓	London, GB
Oxford Analytica	4		✓	✓	Oxford, GB
Crises Group	20			✓	Brüssel, B
International Risk	6	+	✓		Hongkong, CH
CTC Internal Group Inc.	1	++	✓		Palm Beach, USA
Global Options	10	++	✓	✓	Washington, USA
Intern. Intelligence Ltd.	4	+	✓		Cotswold, GB
ATHENA GS3 Sec. Impl.	3	++	✓	✓	Herzliya, ISR
Infosphere	1		✓	✓	Stockholm, SWE
Global Source LLC.	3	++	✓		Fairfax, USA
Global Risk Assessment	1	++	✓	✓	Riverside, USA
SmithBrandon International	1	++	✓		Washington, USA
Eurasia Group	3		✓	✓	New York, USA
Exclusive Analysis	1	+	✓	✓	London, GB
Sentigence Inc.	1	++	✓		USA
The Scowcroft Group	1	++	✓	✓	Washington, USA

(Quelle: P. Harbich, Die wachsende Bedeutung privater Akteure im Bereich der Intelligence, Universität Köln, 2006, S. 71)

Weitere Beispiele Siehe Peter Harbich, Die wachsende Bedeutung privater Akteure im Bereich der Intelligence – Private Akteure als Quellen, Abnehmer, Konkurrenten und Kooperationspartner staatlicher Nachrichtendienste, Arbeitspapiere zur Internationalen Politik und Außenpolitik, AIPA 03/2006, Universität Köln, S. 74.:

- Shabtai Shavit, der von 1989 bis 1996 Direktor des israelischen Geheimdienstes Mossad war und zum Chairman der israelisch?amerikanischen ATHENA GS3 Security Implementations Ltd. wurde;
- Frederick W. Rustmann, Jr., der 1990 nach 24jähriger Beschäftigung bei der CIA ausschied und zum Chairman des Executive Committee der amerikanischen CTC International Group Inc. wurde;
- James Woolsey (Direktor des CIA von 1993 bis 1995), William H. Webster (Direktor des CIA von 1987?1991 und Direktor des FBI von 1978?1987) und William S. Sessions (Direktor des FBI von 1987?1993), die zu Beratern für die amerikanische Global Options Inc. wurden; sowieGerard Burke, früherer Assistant Director der NSA und Executive Director des Foreign Intelligence Advisory Board von Präsident Nixon, der nach Gründung eines eigenen Private Intelligence Service namens Parvus nun Direktor von Global Source LLC wurde.

Fazit
Der Trend zu „altem Qualitätswein in neuen Schläuchen“ wird sich verstärkt fortsetzen. Dies muss nicht negativ sein, sondern führt dann zu mehr Sicherheit, wenn angreifende Profis verteidigenden Profis gegenüber stehen. Negativ könnte sich auswirken, wenn sich die Loyalität privater Sicherheitsfirmen mit Ex-Geheimdienstleistern nicht nur auf den einen Auftraggeber fokussiert, sondern sie z.B. innerhalb einer Branche den Vertragspartner wechseln bzw. konkurrierende Unternehmen bedienen oder alte Seilschaften zu den Diensten noch greifen. Denn auch in diesem Gewerbe gilt: Niemals geht man so ganz! Und für deutsche Unternehmen gilt: Augen auf bei der Partnerwahl im Security-Segment, denn die internationale Zahl trojanischer Pferde wird nicht kleiner.

consulting *plus*
Beratung GmbH
Girardetstraße 1-5
45131 Essen
Tel.: +49 201 27 90 40