Sicherheit – interdisziplinäre Perspektiven

Christian Vogt · Christian Endreß
Patrick Peters *Hrsg.*

Wirtschaftsschutz in der Praxis

Positionen zur Unternehmenssicherheit und Kriminalprävention in der Wirtschaft

Springer

Sicherheit – interdisziplinäre Perspektiven

Reihe herausgegeben von
Thomas Jäger, Universität zu Köln, Köln, Deutschland
Nicole Krämer, Universität Duisburg-Essen, Duisburg, Nordrhein-Westfalen, Deutschland
Norbert Pohlmann, Institut für Internet-Sicherheit, Westfälische Hochschule, Gelsenkirchen, Deutschland

Sicherheit ist zu einer Signatur unserer Zeit geworden. Technische und gesellschaftliche Veränderungen transformieren dabei die Bedingungen, unter denen Sicherheit erlangt werden soll, kontinuierlich. Die Herausforderungen und Risiken liegen auf allen Gebieten der gesellschaftlichen, wirtschaftlichen und politischen Ordnung. Bedrohungen und Bedrohungswahrnehmungen haben sich in den letzten Jahren verschärft und scheinen keinen ordnungspolitischen Rahmen zu haben. Soziale, ökologische, ökonomische, innere und äußere Sicherheit, Fragen der Organisation von Sicherheitsinstitutionen, Prozesse des Normwandels und der Diskursgestaltung, unterschiedliche Ausprägungen von Kommunikation mit vielfältigen Akteuren sowie die Verzahnung verschiedenster Herausforderungen greifen ineinander über. Analysen und Darstellungen, die über einen spezifischen Fachbereich hinausreichen und verschiedene Bereiche des gesellschaftlichen Lebens einbeziehen oder unterschiedliche analytische Zugänge vereinen, finden durch die interdisziplinäre Buchreihe „Sicherheit“ den Zugang zu den Lesern unterschiedlicher Fächer.

Weitere Bände in der Reihe http://www.springer.com/series/13807

Christian Vogt · Christian Endreß ·
Patrick Peters
(Hrsg.)

Wirtschaftsschutz in der Praxis

Positionen zur Unternehmenssicherheit und Kriminalprävention in der Wirtschaft

Springer

Hrsg.
Christian Vogt
CLAAS KGaA mbH
Harsewinkel, Deutschland

Christian Endreß
Geschäftsführung, ASW NRW e. V.
Düsseldorf, Deutschland

Patrick Peters
Mönchengladbach, Deutschland

ISSN 2510-0963 ISSN 2510-0955 (electronic)
Sicherheit – interdisziplinäre Perspektiven
ISBN 978-3-658-24636-5 ISBN 978-3-658-24637-2 (eBook)
https://doi.org/10.1007/978-3-658-24637-2

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Springer ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Wirtschaftsschutz in der Praxis: eine Einführung

Cyber-Risiken, Entführungen von Mitarbeitern sowie generell eine Verschärfung der Sicherheitslage in vielen Weltregionen, Ausspähversuche und Wirtschaftsspionage, globaler Terrorismus: In den vergangenen Jahren haben vielfältige Gefahren Gesellschaft und damit auch die Wirtschaft erreicht, die der weniger kundige Beobachter eher in Hollywood als in Berlin und Hamburg, London und Paris, Amsterdam und Mailand vermuten würde.

Aber: Die Gefährdungslage wird mittlerweile immer umfassender. Unternehmen werden Opfer von Cyber-Attacken oder Wirtschaftsspionage, in manchen Regionen dieser Welt sind ihre Mitarbeiter Risiken wie gezielter Entführung ausgesetzt, und durch den zunehmenden Terrorismus in Europa ist auch die Wahrscheinlichkeit gestiegen, von einem Terroranschlag betroffen zu sein. Jeden Tag werden kritische Vorfälle gemeldet, die Zahlen gehen Jahr für Jahr in Tausende, Tendenz permanent steigend. Allein in der Cyber-Kriminalität belaufen sich die Schäden für die deutsche Wirtschaft aktuell auf geschätzte 55 Mrd. EUR jährlich.

Apropos Terrorismus: Bei einer Umfrage der Wirtschaftsprüfungsgesellschaft Deloitte unter 2000 Top-Führungskräften weltweit gaben zuletzt 36,4 % an, von allen Risiken auf das Terrorismusrisiko am schlechtesten vorbereitet zu sein. Dabei ist diese Gefahr mehr als real. Die Innere Sicherheit hat sich in der Bundesrepublik Deutschland (auch medial) zu dem bedeutsamsten Politikfeld der heutigen Zeit entwickelt. Das resultiert unter anderem aus dem internationalen, islamistischen Terrorismus, der mittlerweile in Europa und auch speziell in Deutschland angekommen ist. Die Sicherheitsbehörden verzeichnen seit dem Jahr 2000 bislang eine Anzahl von 71 Anschlägen und Anschlagsversuchen – davon alleine 17 in Deutschland (an zweiter Stelle nach Frankreich mit einer Anzahl von 26). Vollendet wurden 44 Anschläge. 24 % wurden von Terrorkommandos oder Terrorzellen begangen. Die oft erfolgreiche Arbeit der Behörden hat eine weit größere Anzahl verhindern können.

Dabei stellt sich die Frage: Wie steht es um die Gefahrenabwehr in deutschen Unternehmen? Und was tun insbesondere kleine und mittlere Unternehmen und Konzerne gleichermaßen, um ihre Organisationen und damit die Geschäftszielerfüllung zu schützen sowie wirtschaftliche Weiterentwicklung dauerhaft bei einer umfassend reduzierten Risikoexponierung möglich zu machen?

Gerade vor dem Hintergrund der Digitalisierung ist dies eine höchst relevante Fragestellung. Die deutsche Wirtschaft befindet sich mitten im Prozess der digitalen Transformation. Für den Mittelstand stellt dies teilweise eine enorme Herausforderung dar. Die Bedrohungslage hat sich trotz großer Anstrengungen seitens der Wirtschaft, der Wissenschaft und des Staates verschärft: Abwehrmaßnahmen und die Sicherheitsinformationstechnologie haben nicht Schritt gehalten mit der hohen Varianz von Cyberangriffen. Für Kriminelle wie für fremde Nachrichtendienste sind Cyberangriffe über das Internet hochattraktiv, da eine Vielzahl von Schwachstellen in Softwareprodukten permanent neue Ansatzpunkte für die Entwicklung von Schadprogrammen liefern. Dabei ist Cybersicherheit ein entscheidender Erfolgsfaktor, da nur ein notwendiges Maß an Sicherheit für Anwender und Kunden notwendiges Vertrauen in Digitalisierung schafft.

Kurzum: Die globalen Bedrohungslagen sind allgegenwärtig und können jeden treffen – und das täglich. Da ist der Mittelständler, der auf einer Messe eine nahezu perfekte Kopie seines wichtigsten Produkts am Stand eines internationalen Wettbewerbers findet. Da ist der Konzern, der Mitarbeiter in eine Krisenregion entsendet, die dann Opfer von Bedrohungen oder Entführungen werden. Jüngste Angriffe auf IT-Netzwerke zeigen eine Vielzahl an Szenarien mit Auswirkungen auf die Verfügbarkeit von zentralen Infrastrukturen und lebensnotwendigen Leistungen (Gesundheitsvorsorge, Kommunikation, Zahlungsmittel, Lebensmittel, Wasser usw.) auf.

Der vorliegende Band *Wirtschaftsschutz in der Praxis* befasst sich aus verschiedenen Blickwinkeln mit dem immer akuter werdenden Aspekt des Wirtschaftsschutzes. Die Publikation richtet sich vorrangig an die mittelständische Wirtschaft, aber zugleich auch an die öffentliche Hand, politische Akteure, Berater, Wissenschaftler, Studierende, Journalisten und gemeinnützige Organisationen, die – auch aus internationaler Perspektive – mit Sicherheit befasst sind. Ansatz ist es, mit *Wirtschaftsschutz in der Praxis* eine Grundlagensammlung zum großen Komplex „Wirtschaftsschutz“ aus diversifizierten Perspektiven heraus zu erreichen. Der Band soll praxisnahe Einblicke geben, aber auch als Benchmark für die künftige Beschäftigung mit dem Thema dienen.

Das Konzept des „Wirtschaftsschutzes“ prägt den gesamten Gedanken und zieht sich als roter Faden durch die Beiträge, die aus der Feder renommierter Experten der jeweiligen Fachbereiche stammen. Doch was ist „Wirtschaftsschutz“

eigentlich? Zwar wird der Begriff in Fachdiskussionen und einschlägigen Veröffentlichungen seit langem genutzt, und auch viele Unternehmen, Fachleute der öffentlichen Hand und die Sicherheitsbehörden wissen um dessen Bedeutung. Allein, eine allgemeingültige Definition existiert nicht.

Einen ersten Anhaltspunkt bietet die Broschüre „Einführung in den Wirtschaftsgrundschutz“ (2016) des Bundesamts für Verfassungsschutz und des Bundesamts für Sicherheit in der Informationstechnik.

> Unbestritten haben Wirtschaftsspionage, Sabotage und Konkurrenzausspähung durch die Globalisierung und Digitalisierung zu neuen und komplexeren Sicherheitsherausforderungen für Staat und Wirtschaft geführt. Allerdings finden diese entgegen dem medialen Echo auch im 21. Jahrhundert nicht ausschließlich unter Ausnutzung von Lücken in der IT-Infrastruktur statt. Ein umfassender Schutz muss daher nicht nur alle relevanten Unternehmenswerte berücksichtigen, sondern darauf basierend neben informationstechnischen Maßnahmen auch physische, personelle, prozessuale und organisatorische Aspekte der Sicherheit adressieren. Der Wirtschaftsgrundschutz verfolgt die Idee eines ganzheitlichen Schutzmodells und beschränkt sich dabei nicht auf den Schutz digitaler Informationen innerhalb der Informations- und Kommunikationstechnik (IKT), da diese lediglich einen Teil der zu schützenden Werte darstellen.

Und weiter heißt es:

> Schwerpunkt des Wirtschaftsgrundschutzes sind somit all diejenigen Maßnahmen, die den Schutz der Unversehrtheit von Leib und Leben, geistigem und physischem Eigentum, nicht auf der IKT basierenden Informationen und weiteren von der Institution definierten Werten zum Ziel haben. Durch den einheitlichen Ansatz und die vergleichbare Denkweise sollen die Grenzen zwischen IT- und non-IT-sicherheitspezifischen Themen aufgelöst und die Verantwortlichen dadurch in die Lage versetzt werden, übergreifende Sicherheitskonzepte auf Basis bewährter Verfahrensweisen zu implementieren.

Daran wollen wir uns orientieren. Wirtschaftsschutz in der Praxis bedeutet die Summe aller Maßnahmen, die Einrichtungen jedweder Art ergreifen, um Mitarbeiter und Vermögenswerte zu schützen und eine prosperierende ökonomische Entwicklung möglich zu machen. Wirtschaftsschutz ähnelt in seiner Ausprägung der aus Vermögensverwaltung und Financial Planning bekannten Asset Protection, also der Absicherung von liquidem und illiquidem Vermögen durch bestimmte Maßnahmen gegen innere und äußere Einflüsse. Wirtschaftsschutz umfasst das Unternehmen in allen seinen Facetten, dezidiert auch die Mitarbeiter und stellt eine tragfähige Lösung zur Verfügung, sämtliche Ressourcen bestmöglich vor internen und externen Risiken zu schützen. Auf diese Weise entsteht

ein stabiles Gebilde, das auch Krisenszenarien standhält und dem Management in jeder Situation (auch einer unbekannten) alle Entscheidungswege offenhält. Wirtschaftsschutz versichert einer Organisation das Funktionieren im Rahmen eines sicherheitsrelevanten Vorfalls, da Kompetenzen und Verantwortlichkeiten definiert sind und ein Maßnahmenpaket zur Verfügung steht, das dazu geeignet ist, auf Vorfälle schnell, präzise, mit der gebotenen Professionalität zu reagieren. Wirtschaftsschutz entwickelt durch protektive Maßnahmen optimale reaktive Möglichkeiten.

In diese Richtung zielt dementsprechend der erste Band *Wirtschaftsschutz in der Praxis*. Die darin gesammelten Aufsätze entsprechen den Herausforderungen von Organisationen im Alltag und stellen Ansätze und Szenarien im Wirtschaftsschutz vor, die für Unternehmen und andere Einrichtungen hohe Relevanz haben. Als Sicherheitsverband werden wir die weitere Entwicklung genau beobachten und bewerten.

Wir danken allen Autorinnen und Autoren für die Mitwirkung an diesem Sammelband.

Die Herausgeber
Christian Vogt
Christian Endreß
Patrick Peters

Inhaltsverzeichnis

Herausgeber- und Autorenverzeichnis

Über die Herausgeber

Christian Vogt (Dipl. Verwaltungswirt, KHK a. D.) ist Absolvent der Fachhochschule des Bundes und seit 30 Jahren in den unterschiedlichsten Bereichen der öffentlichen und privaten Sicherheit präsent. Er ist Absolvent der Mitteleuropäischen Polizeiakademie mit dem Ausbildungsschwerpunkt Vorbeugung und Bekämpfung der internationalen organisierten Kriminalität. Er ist Certified Information Security Manager (ISACA) und ausgebildeter Datenschutzauditor. Aktuell leitet er den Bereich Konzernsicherheit und Konzerndatenschutz des international aufgestellten Landtechnikkonzerns CLAAS. Ehrenamtlich ist Christian Vogt Vorstandsvorsitzender der Allianz für Sicherheit in der Wirtschaft Nordrhein-Westfalen e. V.

Dr. Christian Endreß (Politikwissenschaftler) begann seine berufliche Laufbahn bei einer Bundesbehörde. Anschließend arbeitete er als wissenschaftlicher Mitarbeiter am Lehrstuhl für Sicherheitsforschung an der Universität Witten/Herdecke und wechselte dann in die Privatwirtschaft. Heute ist er Geschäftsführer der Allianz für Sicherheit in der Wirtschaft Nordrhein-Westfalen e. V. und seit Januar 2019 kommissarischer Geschäftsführer des ASW-Bundesverbands. Christian Endreß ist Herausgeber und Autor zahlreicher Fachpublikationen sowie Mitglied im Gesprächskreis Innere Sicherheit NRW und des Programmbeirats der Cyberakademie.

Dr. Patrick Peters (Dr. Patrick Peters – Klare Botschaften) übernimmt als Berater für Unternehmenskommunikation, Strategie und Redaktion die Strukturierung und Umsetzung der Public Relations von Unternehmen, Verbänden, Vereinen und Stiftungen. Besonders liegt sein Fokus auf unabhängigen Vermögensverwaltern, Privatbanken, Finanzdienstleistern, Rechtsanwälten, Steuerberatern, Wirtschaftsprüfern, Versicherungsunternehmen und M&A-Beratern sowie der gesamten Bau- und Gesundheitswirtschaft. Für Family Office, Vermögensverwalter, Stiftungen, Privatbanken und Investmentsfonds bietet Dr. Patrick Peters zudem ausgewählte, strategische Beratungsleistungen an. Er ist Pressekoordinator der Allianz für Sicherheit in der Wirtschaft Nordrhein-Westfalen e. V.

Autorenverzeichnis

Marc Brandner ist Partner der SmartRiskSolutions GmbH und Leiter Krisenmanagement. Er war sechs Jahre als Offizier in den Einsatzkräften des Kommando Spezialkräfte (KSK) tätig, zuletzt als kommissarischer Leiter des Ausbildungs- und Versuchszentrums. An der UniBw München hat er Wirtschafts- und Organisationswissenschaften studiert. Er war zertifizierter Leiter Sicherheits- und Krisenmanagement bei EUPOL Afghanistan. Seit 2003 berät er erfolgreich Unternehmen, Internationale Organisationen und NGO zum Sicherheits- und Krisenmanagement. Er ist bestellter Krisenberater eines Krisenreaktionsteams einer Versicherung. Dabei berät er weltweit bei Entführungen, Erpressungen, Produktschutzfällen, Cyberkriminalität und terroristischen Bedrohungslagen. Er hat unter anderem bei einer international aufsehenerregenden terroristischen Geiselnahme in Nordafrika 2013 aktiv einen Firmenkrisenstab beraten.

Dirk Fleischer (LL.M., M.A.) ist Absolvent der Deutschen Hochschule der Polizei und seit mehr als 30 Jahren in den unterschiedlichen Bereichen der privaten und öffentlichen Sicherheit präsent. Als Kriminologe und Wirtschaftsjurist wendet er sich vor allem Fragen der Entstehung von Wirtschafts- und Cyberkriminalität sowie den Präventionsmöglichkeiten durch ganzheitliche Sicherheitsmanagement- und Compliancemanagementsysteme zu. Er ist Autor diverser Veröffentlichungen und berät als freier Berater Personen, Unternehmen und Organisationen. Er ist Mitglied im Gesprächskreis Innere Sicherheit NRW und des Programmbeirats der Cyberakademie.

Burkhard Freier ist Jurist und trat 1985 in den Dienst des Landes NRW ein. Ab 1991 bekleidete er verschiedene Führungsfunktionen im NRW-Innenministerium, zwischenzeitlich war Burkhard Freier von 2001 bis 2006 Stellvertreter der Landesbeauftragten für Datenschutz und Informationsfreiheit NRW. Seit 2012 ist Burkhard Freier Leiter des Verfassungsschutzes NRW.

Dr. Christoph Georgi ist Forschungsdirektor für Sicherheit & Innovation am Strascheg Institute for Innovation, Transformation & Entrepreneurship (SITE) der EBS Business School. Sein BWL-Studium schloss er 2006 als Diplom-Kaufmann ab und promovierte 2009 im Bereich Supply Chain Management. Christoph Georgis Forschungsinteresse liegt im Bereich des strategischen Sicherheitsmanagements, dem er sich insbesondere mit qualitativen Methoden und aus Perspektive der Zukunfts-, Organisations- und Verhaltensforschung nähert.

Uwe Gerstenberg, geboren 1961 in Berlin, ist seit fast 30 Jahren in der privaten Sicherheitswirtschaft in führenden Positionen tätig. Seit 1997 leitet er als Mitgründer die consulting plus Unternehmensgruppe. Uwe Gerstenberg ist unter anderem Mitglied im Security Beirat der Messe Essen und vertritt in zahlreichen Fachverbänden die Interessen der Sicherheitswirtschaft. Des Weiteren ist er Herausgeber des Security Explorers und Autor zahlreicher Buchbeiträge und Fachartikel.

Dr. Jürgen Harrer ist Forschungsdirektor für Security & Management am Strascheg Institute for Innovation, Transformation & Entrepreneurship (SITE) der EBS Business School. Nach Erst- und Zweitstudium und mehreren beruflichen Stationen als Berater und als Führungskraft in einem DAX-Unternehmen promovierte er im Bereich Security Controlling. Jürgen Harrers Forschungsinteressen liegen in der Operational Excellence im Security Management und insbesondere im Security Performance Measurement.

Dr.-iur Trygve Ben Holland, LL.M., Jahrgang 1974, Studium der Rechtswissenschaften in Hamburg und Tansania, Master-Studium Europarecht am Europa-Institut Saarbrücken, Promotion zu einem europa- und wettbewerbsrechtlichen Thema an der Universität Saarbrücken, seit 2005 Lehrbeauftragter an der HfÖV Bremen und Leiter mehrerer Forschungsprojekte im Institut für Polizei- und Sicherheitsforschung IPoS der HfÖV.

Sarah Holland, Jahrgang 1990, Studium der Betriebswirtschaft in Hamburg und San Diego, IPMA-zertifizierte Projekt- und Prozessmanagerin im Institut für Polizei- und Sicherheitsforschung IPoS der Hochschule für Öffentliche Verwaltung Bremen.

Prof. Dr. Gabriele Jacobs ist Professorin für Organisationsverhalten und Kultur am Institut für Organisations- und Personalmanagement der Rotterdam School of Management, Erasmus University (RSM). Gabriele Jacobs ist Co-Direktorin des Centre of Excellence on Public Safety Management (CESAM), das sie 2014 mitbegründete. Neben der Präsentation ihrer Arbeit auf internationalen Konferenzen publiziert sie in zahlreichen wissenschaftlichen Fachzeitschriften sowie in Fachzeitschriften mit anwendungsorientiertem Schwerpunkt. Sie leitet verschiedene EU-Projekte und nationale Projekte im Bereich Sicherheit, beziehungsweise ist in sie als Partnerin involviert. Derzeit koordiniert sie die Erasmus+ Knowledge Alliance zum Thema „International Security Management", deren Ziel es ist, nachhaltige und konkrete Ressourcen und Strukturen zur Förderung internationaler Sicherheitskooperationen zu schaffen und die Entwicklung eines Executive Master für Führungskräfte aus dem privaten und öffentlichen Sektor.

Dominique Lapprand ist ehemaliger französischer Gendarmerie-Oberoffizier, Absolvent der Militärakademie Saint Cyr, des FBI NA und des französischen nationalen Instituts für Sicherheitsstudien. Er hat auch einen Master-Abschluss in Organisationsdynamik. Sowohl national als auch international hat er umfassende Erfahrung in den Bereichen Polizei und Sicherheit aufgebaut. Er leitete das strategische Forschungszentrum der Gendarmerie und arbeitete auch mit der Direktion für Strafrechtspflege des französischen Justizministeriums zusammen. Er war vier Jahre in der Europäischen Kommission als nationaler Entsendeexperte tätig. In den letzten Jahren hat er in acht afrikanischen Ländern an Projekten zur Reorganisation des Sicherheitssektors und der Polizei gearbeitet und parallel dazu arbeitet er mit dem Privatsektor an Informationssystemen und dem Kampf gegen den illegalen Handel. Derzeit ist er in der Erasmus+ Knowledge Alliance zum Thema „International Security Management" involviert.

Florian Lindemann ist Mitglied der Geschäftsleitung der Cyber Akademie GmbH, einem unabhängigen Schulungs- und Beratungsunternehmen der Informationssicherheitsbranche. Im Rahmen seiner Tätigkeit befasst er sich unter anderem mit rechtlichen, technischen und organisatorischen Fragen der Digitalisierung und der Cyber-Sicherheit.

Pascal Michel ist Geschäftsführer der SmartRiskSolutions GmbH. Er war 17 Jahre lang bei einer bundesdeutschen Sicherheitsbehörde im operativen Einsatz und als Ausbildungsleiter tätig. Seit 2008 berät er Unternehmen im Bereich der Reisesicherheit, in der Sicherheit von Großprojekten in risikoreichen Regionen sowie im Krisenmanagement. Für Unternehmen und NGOs hat er unterschiedliche Trainingsformate im Bereich der Reisesicherheit und des

Krisenmanagements entwickelt. Für eine weltweit führende Versicherung ist er als Krisenberater Teil eines multinationalen Krisenreaktionsteams. Seine Erfahrung umfasst die Krisenreaktion bei Entführungen, unter anderem in Mexiko, Libyen, Nigeria und DR Kongo, wo er als Krisenberater sowohl Krisenstäbe als auch das lokale Notfallmanagement beraten hat. Er ist Absolvent der Fachhochschule des Bundes und hat vier Jahre in Westafrika gelebt.

Valentina Nieß, LL.M. (Berkeley) ist Rechtsanwältin und Counsel der Sozietät Noerr LLP. Sie ist spezialisiert im Bereich Gewerblicher Rechtsschutz und Wettbewerbsrecht und berät ihre Mandanten umfassend unter anderem im Zusammenhang mit dem Aufbau von Marken- und Designportfolios, der Rechtsdurchsetzung und Prozessführung – insbesondere bei der Bekämpfung von Produktpiraterie – sowie der Durchführung von Produkteinführungen und Werbekampagnen.

Dr. Harald Olschok ist seit 1992 Hauptgeschäftsführer des Bundesverbandes der Sicherheitswirtschaft (BDSW) und der Bundesvereinigung Deutscher Geld- und Wertdienste (BDGW). Seit April 2018 ist der Diplom-Betriebswirt zudem geschäftsführendes Präsidiumsmitglied des BDSW. Als Chefredakteur betreut er das Magazin DSD – Der Sicherheitsdienst. Mitglied ist er unter anderem im Messebeirat der security in Essen, in der Vertreterversammlung und im Hauptausschuss der Verwaltungs-Berufsgenossenschaft in Hamburg sowie im Fachbeirat Masterstudiengang Sicherheits-Management an der Hochschule für Wirtschaft und Recht (HWR) Berlin.

Dr. Armin Sieber ist Managing Partner des Beratungsunternehmen Sieber Advisors in München. Er berät seit Jahren Unternehmen und Top-Manager in Fragen der Selbstdarstellung, Unternehmens- und Krisenkommunikation. Ein besonderer Schwerpunkt liegt im Bereich der Litigation PR in komplexen Rechtsauseinandersetzungen. Sieber hatte zahlreiche Führungspositionen in Wirtschaft und Beratung inne. Er forscht und unterrichtet im Bereich Medienwissenschaft an der Universität Regensburg.

Janina Wortmann geb. Voogd, LL.M. (Cape Town) ist Rechtsanwältin und Assoziierte Partnerin der Sozietät Noerr LLP. Sie berät nationale und internationale Unternehmen in allen Bereichen des Marken- und Designrechts. Darüber hinaus berät sie im Wettbewerbs- und Vertriebsrecht. Sie ist spezialisiert auf die Durchführung gerichtlicher Streitigkeiten einschließlich einstweiliger Verfügungsverfahren. Janina Wortmann geb. Voogd ist Lehrbeauftragte für Marken- und Designrecht an der AMD Akademie Mode & Design in München.

Volker Wagner ist Vice President Security bei der BASF SE. In den letzten Jahren lag sein beruflicher Schwerpunkt auf der Entwicklung und Umsetzung von Sicherheitsstrategien für den Wirtschaftsschutz in Deutschland. Er ist seit 2012 Vorstandsvorsitzender des ASW Bundesverbandes und war auch mehrere Jahre Vorstandsmitglied der ASW NRW und im Unterausschuss Wirtschaftsschutz des BDI. International engagiert er sich in der ASIS International. Er verfügt über mehr als 20 Jahre Führungserfahrung bei der Deutschen Telekom.

Jan Wolter war von Januar 2014 bis Dezember 2018 Geschäftsführer des ASW Bundesverbandes. In dieser Funktion befasste er sich mit den unterschiedlichsten Facetten des Themas Wirtschaftsschutz. Er ist Initiator und einer von drei Autoren der Studie #Desinformation, die im November 2017 auf dem Deutschen Sicherheitstag veröffentlicht wurde. Der Diplompolitologe ist seit über zwölf Jahren im Verbandsgeschäft tätig. In seinem Studium befasste sich Wolter vor allem mit den Themen Staatszerfall und Bürgerkriegsökonomien.

Peter Zawilla ist Geschäftsführer der von ihm 2004 gegründeten FMS Fraud & Compliance Management Services GmbH. Er beschäftigt sich seit über 20 Jahren mit der praxisorientierten Gestaltung beziehungsweise dem Aufbau von wirksamen und mehrwertschöpfenden Compliance beziehungsweise Fraud Management Systemen. Zudem hat er sich auf die professionelle Aufdeckung von Unregelmäßigkeiten, die Umsetzung von Präventionsmaßnahmen sowie die Implementierung und Optimierung von Compliance in Unternehmen spezialisiert. Er ist Autor zahlreicher Publikationen und Mitherausgeber mehrerer Fachbücher.

Dieter Zeller arbeitete 28 Jahre im Bereich der Sicherheit der Deutschen Telekom in verschiedenen Aufgabenschwerpunkten wie Frauddetection, Fraudinvestigation, Fraudprevention, Emergency- and Crisismanagement. Aktuell ist er als Senior Experte für das Corporate Crisismanagement im Pharmakonzern Boehringer Ingelheim verantwortlich. Die Bewältigung von Incidents im Konzern und die Weiterentwicklung des nationalen- wie internationalen Krisenmanagement zählten zu seinen Aufgaben im Konzern Deutsche Telekom. Seit 1999 steht der Mitautor des Buches „Fraud Management“ als Chairperson in der Verantwortung für das Deutsche Fraud Forum (gegen Telekommunikationskriminalität in Deutschland). In dieser Funktion vertrat Herr Zeller das DFF im Vorstand des ASW Bundesverbandes.

Teil I

Die Privatwirtschaft im Gefüge der Inneren Sicherheit

Wirtschaftsspionage in Nordrhein-Westfalen

Burkhard Freier

1 Wirtschaftsspionage – eine reale Gefahr für Unternehmen in Nordrhein-Westfalen

Nordrhein-Westfalen ist ein exportstarkes und innovatives Hochtechnologieland. Das Bruttoinlandsprodukt des Jahres 2018 spiegelt eine Wirtschaftsleistung von 705 Mrd. EUR wieder. Nordrhein-Westfalen (NRW) ist damit das wirtschaftsstärkste Bundesland. Würde man es als eigenständigen Staat betrachten, stünde es im internationalen Ranking der stärksten Wirtschaftsnationen an 19. Stelle hinter der Türkei und vor der Schweiz (vgl. www.statista.com).

NRW ist unter den Bundesländern auch der bedeutendste Investitionsstandort in Deutschland. Hier haben neben 19.000 ausländischen Unternehmen (www.nrwinvest.com) auch 18 der 50 umsatzstärksten deutschen Firmen (vgl. www.nrwinvest.com) und rund 717.000 kleine und mittlere Betriebe (NRW. INVEST GmbH 2016) ihren Sitz. Letztere bilden das wirtschaftliche Rückgrat Nordrhein-Westfalens. NRW ist zudem ein ausgewiesener Hochschul- und Forschungsstandort. Neben 70 Hochschulen haben dort mehr als 50 außeruniversitäre Forschungseinrichtungen ihren Sitz (vgl. www.wirtschaft.nrw).

Die Dynamik der globalen Digitalisierung prägt auch den nordrhein-westfälischen Wirtschafts- und Forschungsstandort. Der wirtschaftliche und gesellschaftliche Fortschritt ist abhängig von leistungsfähigen digitalen Prozessoren. Sie sichern und steuern Betriebs- und Geschäftsabläufe, Forschungsergebnisse sowie die industrielle Produktion, den Kapitalverkehr, beinahe die gesamte Kommunikation, aber auch den Betrieb sensibler Versorgungssysteme,

B. Freier (✉)
Ministerium des Innern NRW, Düsseldorf, Deutschland
E-Mail: wirtschaftsschutz@im1.nrw.de

C. Vogt et al. (Hrsg.), *Wirtschaftsschutz in der Praxis,* Sicherheit – interdisziplinäre Perspektiven, https://doi.org/10.1007/978-3-658-24637-2_1

sogenannter „Kritischer Infrastrukturen“, wie sie etwa im Energie-, Wasser- oder auch im Gesundheitswesen zu finden sind.

Die Zukunft des Wirtschafts- und Forschungsstandorts NRW hängt deshalb wesentlich davon ab, wie verantwortungsbewusst mit den Daten und Informationen, dem geistigen Eigentum und dem betrieblichen Wissen umgegangen wird, die für den Bestand und den Erfolg eines Unternehmens, einer Forschungseinrichtung oder einer Hochschule existenziell sind.

Der Schutz von betrieblichem Wissen und geschäftlichen Geheimnissen vor Angriffen von innen wie von außen, ob analog oder virtuell, ist zu „einer komplexen Sicherheitsherausforderung geworden“ (Bundesamt für Verfassungsschutz 2016). Er rückt in der globalisierten Welt immer mehr in den Fokus auch staatlicher Sicherheitsbehörden, etwa der Spionageabwehr und des Wirtschaftsschutzes als Aufgabenfelder des Verfassungsschutz des Landes Nordrhein-Westfalen (Ministerium des Innern des Landes Nordrhein-Westfalen 2016). Die nordrhein-westfälischen Unternehmen sind von zwei Seiten bedroht: Nationale und internationale Konkurrenten haben ein gesteigertes Interesse, über Ausspähung des wettbewerblichen Mitstreiters zu erfahren, wie der Konkurrent seinen wirtschaftlichen Erfolg erlangt hat, sichert und ausbaut, um diese Erkenntnisse für sich zu nutzen. Zudem sind fremde Staaten und deren Nachrichtendienste immer intensiver mit staatlich legitimierter Wirtschaftsspionage aktiv.

Das hat gravierende negative Auswirkungen für die bundesdeutsche Volkswirtschaft. Einer Studie des Digitalverbandes BITKOM aus dem Jahr 2017 zufolge sind in den letzten Jahren mehr als die Hälfte der in Deutschland ansässigen Unternehmen Opfer von Wirtschaftsspionage, Sabotage oder Datendiebstahl geworden. Dabei ist ein jährlicher Schaden von rund 55 Mrd. EUR entstanden (vgl. www.bitkom.org). Geht man von der üblichen, auf die Bundesländer bezogenen Verteilung entsprechender Zahlen aus, lässt sich ein Schaden in Höhe von mehr als zehn Milliarden Euro für Nordrhein-Westfalen hochrechnen.

Nach einer im Juli 2017 durchgeführten repräsentativen Telefonbefragung von 450 Führungskräften deutscher Unternehmen zum Thema Wirtschaftsspionage erwarten fast alle Unternehmen steigende Gefahren in diesem Bereich. Zwei von drei Großunternehmen rechnen sogar mit einer Verschärfung der Lage bei Cyber-Angriffen und Datenklau (Ernst und Young 2017). Wirtschaftsspionage konzentriert sich jedoch nicht ausschließlich auf Cyber-Angriffe. Übliche Methoden reichen vom Diebstahl von IT- und Kommunikationsgeräten über digitale Sabotage bis hin zum Social Engineering. Beim Social Engineering werden menschliche Eigenschaften wie Hilfsbereitschaft, Vertrauen, Angst oder Respekt

vor Autorität ausgenutzt, um Personen geschickt zu manipulieren. Der Angreifer täuscht sein Opfer dabei über seine Identität und seine kriminellen Absichten, um es dazu zu verleiten, im guten Glauben für das Unternehmen schädliche Handlungen auszuführen – etwa vertrauliche Informationen preiszugeben, Sicherheitsfunktionen auszuhebeln oder Schadsoftware auf einem Computer im Firmennetzwerk zu installieren.

Vielen Unternehmen mangelt es schon an ausreichenden Detektionsmöglichkeiten. Nur ein Viertel der Betriebe verfügt über ein Cyber-Sicherheitsmonitoring zur Kontrolle von Cyber-Angriffen und wertet Log-Dateien regelmäßig und systematisch aus (BSI 2018). Deshalb bleiben diesen Unternehmen derartige Angriffe häufig verborgen. Angriffe werden statistisch gesehen erst nach ungefähr 120 Tagen erkannt.

Werden Angriffe oder andere relevante Tatbestände von Wirtschaftsspionage erkannt, werden Sicherheitsbehörden nicht immer eingeschaltet oder informiert. Lediglich jedes dritte betroffene Unternehmen wendete sich nach Erkenntnissen der BITKOM-Studie an staatliche Stellen. Hauptmotiv dafür ist die Angst vor einem Imageschaden.

Nordrhein-westfälische Unternehmen mit Weltmarktniveau sowie kleine und mittlere Betriebe mit innovativen Techniken und Produkten sowie mit hervorragenden globalen Marktstrategien und Auslandskontakten bleiben weiterhin ein Ziel der Wirtschaftsspionage.

Wirtschaftsspionage ist mehr als der allgegenwärtige Cyber-Angriff. Denn es gibt auch Ausspähungen, die bei personellen Beziehungen ansetzen, physische Materialien wie Konstruktionspläne und Formeln betreffen oder beispielsweise organisatorische Schwachstellen ausnutzen. Dabei geht es nicht allein um einen möglichen finanziellen Schaden für das betroffene Unternehmen. Ausgespähtes und gestohlenes Know-how kann für die Konkurrenzfähigkeit eines Unternehmens wesentlich sein. Ein Diebstahl von Konstruktionsplänen für ein neues Bauteil kann im schlimmsten Fall beispielsweise zur Insolvenz des ausspionierten Unternehmens führen, wenn ein Dritter das Produkt dadurch vor dem „Erfinder“ auf den Markt bringt. Erwartete Gewinne bleiben aus, die Kosten für die Entwicklung können nicht refinanziert werden, und es fehlt das Kapital für zukünftige Investitionen. Die Wettbewerbsfähigkeit einer ganzen Branche kann beeinträchtigt werden, mit der möglichen Folge, dass auch der Allgemeinheit durch den Wegfall von Arbeitsplätzen und geringere Steuereinnahmen ein Schaden entsteht.

Grundsätzlich sind sämtliche Unternehmen und Branchen von Wirtschaftsspionage bedroht, die erfolgreich im nationalen und vor allem globalen

Wettbewerb stehen. Besonders betroffen sind bundesweit Forschungs- und Entwicklungsabteilungen von Unternehmen aus den Bereichen Rüstung, Luft- und Raumfahrt, Satellitentechnik, Maschinenbau, Medizin- und Mikrotechnologie, erneuerbare Energien wie Windkraftanlagen und Sonnenkollektoren, Biotechnologie und Chemie. Neben großen Unternehmen stehen in Nordrhein-Westfalen sogenannte Hidden Champions besonders im Fokus. Dies sind hoch innovative kleine und mittlere Unternehmen, die in ihrer Branche auf dem Weltmarkt eine Spitzenstellung einnehmen, in der breiten Öffentlichkeit aber in der Regel nicht sehr bekannt sind. Sie stellen beispielsweise elektronische Bauteile wie Steckverbindungen her oder Zubehörteile für Autos oder für Rüstungsgüter. Im Visier von Spionage sind aber auch Verfahren zur Lebensmittelproduktion und Produkte für die Landwirtschaft. Von großem Interesse sind vor allem kleine Unternehmen mit neuen Marktideen („Start-ups“) und einem Potenzial für große Marktchancen. Angriffe richten sich zudem gegen Universitäten und Fachhochschulen, Forschungseinrichtungen sowie die in Nordrhein-Westfalen zahlreich anzutreffenden Technologie- und Gründerzentren.

Die Interessen fremder Nachrichtendienste richten sich nicht nur auf Produkte, sondern beispielsweise auch auf

- Fertigungstechniken, Herstellungsverfahren, Konstruktionsunterlagen,
- Spezialwerkzeuge und Steuerungssysteme,
- Forschungsergebnisse, Produktideen, Patente,
- Personaldaten, Kunden- und Lieferantendaten,
- Verkaufsstrategien, Absatz- und Vertriebswege,
- Budgetplanungen, Kalkulationsunterlagen;
- Marktanalysen und Investitionsvorhaben,
- Unternehmensstrategien und
- digitale Kommunikationsdaten.

Um hier zu sensibilisieren und zu schützen, bietet ein präventiver Informationsaustausch zwischen Unternehmen, Wissenschaft und den relevanten Sicherheitsbehörden wie dem Verfassungsschutz des Landes Nordrhein-Westfalen hingegen die Chance,

- potenziell gefährdete Unternehmen frühzeitig zu sensibilisieren,
- Angreifer, Angriffsmethoden zu erkennen und Angriffsziele zu ermitteln sowie
- wirksame Schutzmaßnahmen zu entwickeln.

2 In Nordrhein-Westfalen aktive ausländische Nachrichtendienste

Unter dem Begriff „Wirtschaftsspionage“ verstehen die deutschen Sicherheitsbehörden eine staatlich gelenkte oder gestützte Ausforschung von Wirtschaftsunternehmen oder Forschungseinrichtungen durch ausländische Nachrichtendienste. Bei der sogenannten Industrie- oder „Konkurrenzspionage“ handelt es sich hingegen um die Ausspähung von Unternehmen durch Wettbewerber (Ministerium des Innern des Landes Nordrhein-Westfalen 2017).

Da es sich bei staatlich gelenkter Wirtschaftsspionage durch Nachrichtendienste um eine geheimdienstliche Tätigkeit für eine fremde Macht handelt (§ 3 Abs. 1 Nr. 2 Verfassungsschutzgesetz NRW), hat der Verfassungsschutz NRW zur Bekämpfung dieses Phänomens die gesetzliche Aufgabe, im Zusammenhang damit stehende Informationen zu sammeln und auszuwerten. Die Bekämpfung von Industrie- beziehungsweise Konkurrenzspionage ist hingegen Aufgabe der Strafverfolgungsbehörden.

In der Praxis ist eine eindeutige Zuordnung entweder als Fall nachrichtendienstlich gesteuerter Wirtschaftsspionage oder als Fall von Konkurrenzausspähung häufig jedoch nicht problemlos möglich. Eine Abgrenzung zwischen diesen beiden Formen der illegalen Know-how-Abschöpfung ist schwierig, weil in beiden Fällen das Zielobjekt und die Methoden weitgehend identisch sein können. Die Herkunft und Verbindungswege der Ausspähmaßnahme werden regelmäßig mit hohem Aufwand verschleiert. Selbst bei entsprechenden Hinweisen lassen sich fremde Nachrichtendienste kaum als mögliche Auftraggeber von Wirtschaftsspionage identifizieren.

Sicher ist also: Wirtschaftsspionage ist ein reales Betätigungsfeld ausländischer Nachrichtendienste. In einigen Staaten haben die dortigen Dienste sogar den ausdrücklichen gesetzlichen Auftrag dazu. Nach dem Gesetz der russischen Föderation über die Auslandsaufklärung hat beispielsweise der russische Auslandsnachrichtendienst die Aufgabe, „die wirtschaftliche Entwicklung und den wissenschaftlich-technische Fortschritt des Landes durch Beschaffung von wirtschaftlichen und wissenschaftlich-technischen Informationen durch die Organe der Auslandsaufklärung zu fördern“ (vgl. Art. 5 des Gesetzes der russischen Föderation über die Auslandsaufklärung).

In anderen Staaten wie etwa in der Volksrepublik China weist bereits die Zahl der Angehörigen der Nachrichtendienste (mehrere Hunderttausend) und der organisatorische Aufbau der Nachrichtendienste auf die Zielrichtung der Aufklärung

ausländischer Volkswirtschaften hin. Es gibt jeweils eigene Arbeitsgebiete für die verschiedenen Aufklärungsbereiche und Wirtschaftsräume, zum Beispiel „Westeuropa“ und damit auch Deutschland.

3 Angriffsmethoden der Wirtschaftsspione

Wirtschaftsspionage erfolgt im Wesentlichen durch drei Methoden:

3.1 OSINT

Open Source Intelligence, OSINT abgekürzt, ist die häufigste und einfachste Methode. Fremde Nachrichtendienste sammeln die erforderlichen Informationen durch intensives Abschöpfen von offen zugänglichen Quellen:

Auf diese Weise gelangen sie an wirtschaftlich wertvolle Daten, die in wachsender Anzahl unbeschränkt zur Verfügung stehen, beispielsweise über Internetauftritte der Unternehmen, über Preisgabe von Unternehmensinterna in sozialen Netzwerken durch Mitarbeiterinnen und Mitarbeiter, über Gespräche auf Messen, Symposien oder bei Empfängen in Botschaften und Konsulaten sowie über personenbezogene Angaben in Visaanträgen wie zum Beispiel die Funktion im Unternehmen oder die Gehaltshöhe.

Der Wert dieser offen erhobenen Daten wird häufig unterschätzt, weil eine Einzelinformation in der Regel nicht sehr aussagekräftig erscheint. Durch systematische Verknüpfung einer Vielzahl von Einzeldaten ergibt sich für einen fremden Nachrichtendienst jedoch ein Gesamtbild, aus dem sich selbst sensible Unternehmensdaten ablesen lassen.

3.2 HUMINT

Menschliche Quellen werden ebenfalls zur Informationsbeschaffung genutzt. Nachrichtendienste sprechen von Human Intelligence (HUMINT).

In diesem Bereich gibt es vielfältige Ansätze. Nachrichtendienste stützen sich unter anderem gezielt auf Agenten. Hierzu zählen zum Beispiel statuswidrig abgetarnte Diplomaten, die aus ihren Botschaften und Konsulaten heraus nachrichtendienstlichen Tätigkeiten nachgehen. Der gezielte Einsatz von ausländischen Praktikanten oder Doktoranden ist eine weitere Möglichkeit, um unmittelbar an sensible Unternehmensdaten zu gelangen. Zu HUMINT zählt aber

auch die klassische nachrichtendienstliche Methode des Kompromats. Kompromate werden beispielsweise geschaffen, indem Beschäftigte von Unternehmen gezielt in Kontakt mit Alkohol, Drogen oder Prostitution gebracht werden. Mit der Drohung, kompromittierendes Material zu veröffentlichen, werden diese Personen anschließend zur Kooperation genötigt.

3.2.1 Social Engineering

Eine weitere sehr häufig genutzte Methode der Wirtschaftsspionage im Bereich HUMINT ist das sogenannte Social Engineering. Ein Angreifer versucht, über die „Sicherheitslücke Mensch“ an Informationen zu gelangen. Er nutzt dabei menschliche Eigenschaften wie Hilfsbereitschaft, Gutgläubigkeit oder Unsicherheit aus, um die sogenannte „menschliche Firewall“ zu durchbrechen und vertrauliche Daten zu erhalten. Der Angreifer gelangt beispielsweise an Benutzernamen und Passwörter, indem er sich am Telefon als Sicherheitsverantwortlicher oder Systemadministrator ausgibt. Durch Hinweis auf vermeintliche akute PC-Probleme, den Aufbau von Zeitdruck und dem Vortäuschen von Betriebskenntnissen, die man sich problemlos über das Internet aneignen kann, wird das Opfer so lange verunsichert, bis es die gewünschten Informationen preisgibt (Dirk Ritter-Dausend 2013a).

3.2.2 Soziale Netzwerke

Soziale Netzwerke im Internet bieten vielfältige Ansatzpunkte für Wirtschaftsspione. Die Plattformen sind darauf ausgelegt, persönliche Daten zu präsentieren, Kontakte zu fördern und Personen miteinander zu vernetzen. Für Angreifer bieten sie optimale, schnell und unkompliziert erreichbare Anknüpfungspunkte. Der Kontakt zu ausgewählten Beschäftigten von Unternehmen lässt sich sehr einfach über die Netzwerke, auch aus dem Ausland, herstellen. Spione freunden sich unter Vorspiegelung einer falschen Identität vermeintlich mit ihren Zielpersonen an und bauen ein Vertrauensverhältnis auf. Dieses nutzen sie schließlich für das Ziel aus, an sensible Informationen des jeweiligen Unternehmens zu gelangen (Dirk Ritter-Dausend 2013b).

3.3 SIGINT

Einen hohen Stellenwert hat die Informationsgewinnung durch Fernmelde- und elektronische Aufklärung. Nachrichtendienste bezeichnen dies als Signal Intelligence, (SIGINT). Die rasante Ausweitung von Kommunikationsmöglichkeiten durch das Internet bietet Nachrichtendiensten eine Vielzahl von Ansatzpunkten.

Netzwerkstrukturen und Netzknoten für die Kommunikation erstrecken sich zum überwiegenden Teil über das Ausland. Netzbetreiber leiten die einzelnen „Datenpakete“ oftmals über den billigsten Weg, auch wenn dieser geografisch länger ist und in Teilen außerhalb Deutschlands liegt. Ein Abgreifen der Daten auf im Ausland liegenden Vermittlungsstellen hinterlässt kaum Spuren. Eine dagegen eingesetzte Verschlüsselung bietet nur Schutz, wenn sie von Endgerät zu Endgerät (Ende-zu-Ende-Verschlüsselung) erfolgt und ein anerkannt sicheres Verschlüsselungsverfahren angewendet wird.

Neben solchen „passiven“ Ausspähungen setzen Staaten wie China oder Russland auch auf „aktive“ Cyber-Angriffe. Diese sind entweder breit angelegt und erfolgen automatisiert oder können speziellen Interessen folgend ein einzelnes Unternehmen beziehungsweise den Arbeitsplatz einer einzelnen Mitarbeiterin oder eines einzelnen Mitarbeiters treffen. Laut der Cyber-Sicherheitsumfrage 2017 des Bundesamtes für Sicherheit in der Informationstechnik (BSI) gaben rund 70 % der befragten Unternehmen an, in den Jahren 2016 und 2017 Opfer von Cyber-Attacken geworden zu sein. In etwa der Hälfte der Fälle waren die Angriffe erfolgreich (BSI 2018).

Zielgenaue Cyber-Angriffe sind anders als automatisierte Massenangriffe mit herkömmlichen Methoden (Firewall, Virenscanner) in den meisten Fällen nicht zu erkennen. Sie zielen beispielsweise ab auf

- die Beeinflussung der Funktionsweise von IT-Systemen,
- den direkte Datendiebstahl von Firmen-Know-how und
- die Manipulation von Internet-Auftritten (BSI 2018).

Eine große Angriffswelle traf Deutschland bereits im Jahr 2007. Neben Regierungscomputern wurden 600 Ziele bei 250 Firmen in Deutschland angegriffen. Rund 80 davon lagen in Nordrhein-Westfalen.

Cyber-Angriffe werden am häufigsten mit Malware-Infektionen (BSI 2018) ausgeführt. Übliche Infektionswege sind

- E-Mails denen sogenannte „Trojaner“ anhängen,
- Drive-by-Downloads, bei denen eine Infektion vom Anwender unbemerkt schon beim einfachen Besuch von Webseiten erfolgt,
- ein direkter Download von Schadprogrammen über einen nicht als gefährlich erkannten Weblink (BSI 2018).

Trojaner laden häufig weitere Schadsoftware nach. Hat sich eine solche Malware im Unternehmensnetzwerk eingenistet, sendet sie nach und nach

dort eingesammelte Daten an den Angreifer. Die Software kann zudem für Sabotagezwecke genutzt werden. Ein sehr bekanntes Beispiel ist die Schadsoftware Stuxnet, die das iranische Atomprogramm über ein Jahr erfolgreich sabotiert hat.

Die weiter zunehmende Digitalisierung schafft laufend neue Angriffsmöglichkeiten. Unter den Stichworten Industrie 4.0 und Internet of Things (IoT) schreitet die Vernetzung von Prozessen auch im Bereich der Produktion mit modernster Informations- und Kommunikationstechnik voran. Dies bietet Unternehmen zahlreiche neue Möglichkeiten und ist für sie unter Effizienzgesichtspunkten unverzichtbar. Diese Entwicklung schafft aber auch bisher ungeahnte Gelegenheiten für Angreifer bis hin zum direkten Eingriff in die Produktion mit den damit verbundenen Sabotagemöglichkeiten.

2016 wurden täglich ca. 350.000 neue Schadprogrammvarianten registriert. Nach dem durch die massenhafte Verbreitung von Ransomware-Trojanern geprägten Jahr 2016 zeichnet sich derzeit ein deutlicher Rückgang im Versand von Schadprogramm-Spam ab (BSI 2018). Eine Entwarnung ist jedoch nicht angebracht, denn Schadprogramme bleiben „eine der größten Bedrohungen für Privatanwender, Unternehmen und Behörden“ (BSI 2018).

3.3.1 Computer-based Social Engineering

Sogenannte HUMINT- und SIGINT-Angriffe lassen sich mittlerweile nicht mehr klar trennen. Um einen technischen Angriff vorzubereiten, wird häufig Social Engineering vorgeschaltet. In einem solchen Fall spricht man vom Computer-based Social Engineering.

Der in der Anlage einer E-Mail enthaltene Trojaner nistet sich nicht von alleine in das Netzwerk eines angegriffenen Unternehmens ein. Ein Angreifer benötigt menschliche Unterstützung, zumeist einen Unternehmensangehörigen, der eine entsprechende E-Mail in seinem Arbeitsumfeld öffnet. Die Nachricht ist dabei so angelegt, dass sie für den Empfänger unverdächtig ist und ihn durch ein interessantes Thema oder eine besondere persönliche Ansprache zum Anklicken animiert. Diese Kontaktaufnahme per E-Mail ist häufig von langer Hand vorbereitet: Der Angreifer macht über das Internet und Soziale Netzwerke Personen ausfindig, die in einem der relevanten Bereiche des anzugreifenden Unternehmens arbeiten. Es wird versucht, mit der letztlich ausgewählten Zielperson ein Vertrauensverhältnis aufzubauen, das für solche häufig erfolgreiche Angriffe ausgenutzt wird.

Neben elektronischen Nachrichten kommen zudem USB-Speichermedien zum Einsatz. Sie werden beispielsweise als Werbegeschenke verteilt oder im Unternehmensumfeld so platziert, dass sie wie verloren gegangen wirken. Manche

Angreifer versuchen, USB-Sticks zudem bei einem Besuch heimlich oder unter einem Vorwand an die Firmenrechner anzuschließen. Eine entsprechende Sensibilisierung der Beschäftigten ist daher sehr wichtig.

3.3.2 Smartphones

Ein beliebtes Angriffsziel von Wirtschaftsspionen sind Smartphones. Die meisten Menschen nutzen diese Geräte im privaten und auch im beruflichen Umfeld. Smartphones haben Funktionen klassischer Computer. Sie sind ebenso leicht, bei häufig fehlendem Schutz sogar noch leichter als Computer angreifbar. Für versierte Nachrichtendienste stellen solche Angriffe keine Herausforderung dar.

Besondere Vorsicht ist geboten, wenn über die mobilen Geräte geschäftliche Daten ausgetauscht, diese auf ihnen gespeichert oder die Smartphones sogar mit dem Unternehmensnetzwerk verbunden werden. Mit spezieller, unbemerkt aufgespielter Schadsoftware lassen sich die Geräte in „Wanzen“ verwandeln. In vertrauliche Besprechungen mitgenommen, ermöglichen sie dem Angreifer das Mithören der gesprochenen Inhalte. Auch Bilder aus allen Besprechungsräumen sind über die eingebaute Kamera auf diesem Weg abrufbar. Beim Verbinden der Geräte mit dem Unternehmensnetzwerk kann die Schadsoftware sich dort weiter ausbreiten.

3.3.3 Cloud Computing

Cloud-Dienste erfreuen sich wachsender Beliebtheit, beispielsweise um Ressourcen im eigenen Unternehmen zu sparen und einen ortsunabhängigen Zugang auf Daten zu ermöglichen. Die neuen Möglichkeiten bringen jedoch auch zusätzliche Gefahren mit sich. Unternehmen müssen sich mit den besonderen Sicherheitsanforderungen solcher Lösungen vertraut machen. Das Bundesamt für Sicherheit in der Informationstechnik hat mit dem „Cloud Computing Compliance Controls Catalogue“ (C5) einen darauf zugeschnittenen Anforderungskatalog veröffentlicht. Ein Unternehmen, das Cloud-Technik nutzen möchte, muss sich insbesondere darüber im Klaren sein, dass verteilt abgelegte Daten physikalisch nicht mehr ausschließlich auf den eigenen Rechnern und Systemen und damit im eigenen Sicherheitsbereich liegen. Dieses Risiko ist sorgfältig zu bedenken, selbst wenn der Anbieter des Cloud-Services aus Deutschland kommt und alle Anforderungen des C5 erfüllt.

4 Ansätze für einen wirksamen Wirtschaftsschutz

Das Spektrum der Methoden und Instrumente, um sich vor Wirtschaftsspionage- oder auch der Konkurrenzausspähung zu schützen, ist breit. Verantwortlichen in Unternehmen sollte aber auch klar sein: Einen 100-prozentigen Schutz gibt

es nicht. Zu spät ist es, sich um den Schutz betrieblichen Wissens erst zu kümmern, wenn man bereits Opfer von Ausspähungen geworden ist. Sich frühzeitig und richtig um den Schutz des Unternehmens zu bemühen, spart unterm Strich nicht nur Geld, sondern sichert das Unternehmen insgesamt. Betriebliche Sicherheit und Informationssicherheit als ihr integraler Bestandteil sind daher unternehmensstrategische Themen und damit eine Daueraufgabe für die Unternehmensleitung.

4.1 Ganzheitliches Sicherheitskonzept

Wirtschaftsspionage zielt nicht nur auf den digitalen Wissensbestand über den Weg der Cyber-Attacke. Die Instrumente und Ziele der offenen und konspirativen Informationsbeschaffung sind weitaus vielfältiger. Der erfolgversprechendste Ansatz zu Beginn der Entwicklung eines Sicherheitskonzeptes lautet: Ein Unternehmen identifiziert in einem ersten Schritt seine sogenannten „Kronjuwelen", das ist beispielsweise das exklusive und besonders sensible, weil für den Unternehmenserfolg relevante Know-how. In der Regel sind dies nicht mehr als rund fünf Prozent aller Unternehmensdaten. Diese Daten sollten in einem speziell gesicherten und vom Internet getrennten Bereich aufbewahrt werden. Da aber Unternehmenssicherheit mehr als reine IT- und Datensicherheit ist, sollte diese Maßnahme in ein für das Unternehmen zu erstellendes, ganzheitliches Sicherheitskonzept eingebettet werden, das nicht nur alle weiteren Daten überprüft, sondern auch andere sicherheitsrelevante Bereiche des Unternehmens umfasst.

Das bedeutet, den Blick über die technische Sicherheit der IT-Systeme und die Datensicherheit hinaus auch auf die Infrastruktur des Betriebes, etwa die Objektsicherheit, zu lenken, die Anforderungen an die Beschäftigten und die erforderlichen Ressourcen zu überdenken, bis hin zu der Organisation und den Verantwortlichkeiten für die betriebliche Sicherheit. Da Sicherheit angesichts des permanenten technologischen Wandels als Prozess verstanden werden muss, sind Sicherheitskonzepte in ein Managementsystem zu integrieren. Dazu gehören ein Risiko- und Notfallmanagement, das bei allen Maßnahmen die zu schützenden Werte, die möglichen Gefahren, die Eintrittswahrscheinlichkeiten und Schadenshöhen in Relation setzt und für den Ernstfall fertigte Pläne mit Sofortmaßnahmen bereithält.

Es geht letztlich darum, die Resilienz des Unternehmens gegen Angriffe auf den inneren Kern des betrieblichen Know-hows zu erhöhen. Neben der Aktualität von technischen und organisatorischen Sicherheitsmaßnahmen zählt dazu auch, allen Beteiligten im Betrieb die rechtlichen wie die innerorganisatorischen Regeln

und Vorschriften bewusst zu machen, sie zu sensibilisieren und auf die Einhaltung nicht nur hinzuweisen, sondern diese auch zu leben.

Ansätze für den Aufbau und die Entwicklung solcher umfassenden Sicherheitskonzepte können die Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI), die Komponenten des Wirtschaftsgrundschutzes der „Initiative Wirtschaftsschutz“ (einem Zusammenschluss aus mehreren Sicherheitsbehörden und Partnerverbänden) sowie internationale Standards wie ISO 27001 ff. bieten.

4.2 Sicherheit ist Chefsache

Sicherheit im Unternehmen kann nicht nur „nebenbei“ bearbeitet werden. Sie sollte professionell durch eine eigene, möglichst an die Geschäftsführung angebundene Organisationseinheit vorangetrieben werden. Denn Unternehmenssicherheit ist Chefsache. Alle Fäden in Bezug auf Sicherheit, unabhängig davon, ob es sich um den IT-Bereich, um Objektsicherheit oder um weitere Sicherheitsthemen handelt, sollten in dieser gebündelten Zuständigkeit zusammenlaufen.

Bedrohungslagen für Unternehmen ändern sich im Zuge des technischen Fortschrittes und der Entwicklung immer neuer Angriffsmethoden sehr rasch. Es sind moderne, kreative Abwehrmaßnahmen gefragt, die auf die Prozesse und Strukturen, die Produkte und Strategien des Unternehmens und nicht zuletzt auf die Mitarbeiterschaft und deren Arbeitsplätze zugeschnitten sind.

Bestehende Sicherheitsvorkehrungen und deren Einhaltung sind aber auch fortlaufend auf ihre Wirksamkeit zu überprüfen. Bei sensiblen IT-gestützten Verfahren bietet sich beispielsweise ein sogenannter Penetrationstest an. Mit einem solchen Test werden denkbare Angriffe simuliert und die Erkenntnisse zur Fortentwicklung des Sicherheitskonzeptes genutzt. Teil dieses Konzeptes sollten auch Regelungen zum sicheren Umgang mit mobilen Geräten sein.

4.3 Vorbereitung auf den „worst case“

Neben einem präventiven Ansatz ist für jedes Unternehmen ein Krisen- und Notfallmanagement unabdingbar. Zwar hofft jedes Unternehmen, dass der „worst case“ nicht eintritt. Es wäre jedoch fahrlässig, auf einen Krisenfall, das gehackte Netzwerk oder den erfolgreichen Spionagefall nicht vorbereitet zu sein. Ein unternehmensadäquates Krisen- und Notfallmanagement geht in der Regel mit einer besonderen Aufbauorganisation einher und umfasst viele Schritte bis hin zur Krisenkommunikation nach außen.

Sicherheit selbst ist zwar kein unmittelbar wertschöpfender Prozess, sie hat jedoch eine sehr wichtige flankierende Funktion und stellt somit einen nicht zu vernachlässigenden Wettbewerbsvorteil dar (W. Karden und A. von Freiberg 2011).

5 Angebote des nordrhein-westfälischen Verfassungsschutzes

Der Verfassungsschutz des Landes Nordrhein-Westfalen informiert in seinen jährlichen Berichten über die Gefahren der Wirtschaftsspionage. Er sensibilisiert zudem insbesondere kleine und mittlere Unternehmen vor Ort sowie beispielsweise bei Veranstaltungen von Wirtschaftsverbänden und den Industrie- und Handelskammern für die Gefahren der Wirtschaftsspionage.

Nordrhein-westfälische Unternehmen können sich vertraulich an den Verfassungsschutz NRW wenden, wenn sie Fragen zur Erstellung eines Sicherheitskonzeptes oder zu anderen Sicherheitsthemen haben. Die Experten des Wirtschaftsschutzes übernehmen dann eine Einstiegsberatung; sie können aber auch direkt für Fachvorträge vor Beschäftigten von Unternehmen oder Vertretern von Interessensverbänden angesprochen werden (wirtschaftsschutz@im1.nrw.de). Sicherheitsbevollmächtigte im Unternehmen können zudem Unterstützung bei der Durchführung von Awareness-Veranstaltungen erhalten.

Der Verfassungsschutz des Landes Nordrhein-Westfalen ist bei konkreten Verdachtsfällen für Unternehmen jederzeit ansprechbar, wie zum Beispiel bei

- dem Verdacht eines Angriffs auf Informations- und Kommunikationstechnik,
- Anhaltspunkten für Know-how-Verlust,
- Sicherheitsvorfällen in Auslandsniederlassungen und auf Geschäftsreisen,
- untypischen Einbruchsdelikten, einem Spionageverdacht gegen Mitarbeiter und Fremdpersonal,
- unerklärlichen Auftragsrückgängen oder unerklärlichem Verlust von Marktanteilen.

Vertraulichkeit wird auf Wunsch zugesichert.

In institutioneller Hinsicht repräsentiert und ergänzt die „Sicherheitspartnerschaft Nordrhein-Westfalen“ als Public Private Partnership die Aufgabenstellung, die Wirtschaft und die Öffentlichkeit über die Gefahren der Wirtschaftsspionage und Wirtschaftskriminalität aufzuklären und auf die Notwendigkeit des Schutzes betrieblicher Informationen hinzuweisen. Die Sicherheitspartnerschaft besteht schon seit dem Jahr 2001. In dieser Partnerschaft haben sich das Ministerium

des Innern des Landes Nordrhein-Westfalen (Abteilungen Verfassungsschutz und Polizei), das Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen, das Landeskriminalamt NRW, die Allianz für Sicherheit in der Wirtschaft Nordrhein-Westfalen e. V. und die Vereinigung der Industrie- und Handelskammern in Nordrhein-Westfalen zusammengeschlossen. Gemeinsam verfolgen die Partner über die Vernetzung der Akteure, einen intensiven Informationsaustausch und gemeinsame Aktivitäten die Ziele der Vertrauensbildung und Prävention, damit die Unternehmen in Nordrhein-Westfalen für Themen wie Spionage, Cyber-Attacken, Sabotage oder auch Wirtschaftskriminalität einen verlässlichen Ansprechpartner haben.

Literatur

BSI (Hrsg.). (2018). *Allianz für Cybersicherheit. Ergebnis der Cyber-Sicherheits-Umfrage 2017* (S. 18). Bonn: BSI.

Bundesamt für Verfassungsschutz, BSI, ASW Bundesverband (Hrsg). (2016). *Einführung in den Wirtschaftsgrundschutz* (S. 6). Berlin: Bundesamt für Verfassungsschutz.

Ernst & Young GmbH (Hrsg.). (2017). *Datenklau: Virtuelle Gefahr, echte Schäden. Eine Befragung von 450 deutschen Unternehmen* (S. 4).

Karden, W., & von Freiberg, A. (2011). *Praxishandbuch Unternehmenssicherheit* (S. 9). Norderstedt.

Landesbetrieb IT.NRW. (2018). *Bruttoinlandsprodukt (BIP) 2009–2018*. Düsseldorf: Landesbetrieb Information und Technik des Landes Nordrhein-Westfalen.

Ministerium des Innern des Landes Nordrhein-Westfalen. (2016). *Verfassungsschutzbericht des Landes Nordrhein-Westfalen für das Jahr 2016* (S. 244 ff.). Düsseldorf: Ministerium des Innern des Landes Nordrhein-Westfalen.

Ministerium des Innern des Landes Nordrhein-Westfalen. (2017). *Verfassungsschutzbericht des Landes Nordrhein-Westfalen für das Jahr 2017*. Düsseldorf: Ministerium des Innern des Landes Nordrhein-Westfalen.

NRW.INVEST GmbH (Hrsg.). (2016). *Neue Chancen in Nordrhein-Westfalen. Ihr Investitionsstandort Nr. 1 in Deutschland – Daten. Fakten* (S. 6). Düsseldorf: NRW. INVEST GmbH.

Ritter-Dausend, D. (2013a). Schwachstelle Mensch in der Unternehmenssicherheitsarchitektur. In FAZ Institut (Hrsg.), *Security management 2012/2013*. Frankfurt: FAZ Institut.

Ritter-Dausend, D. (2013b). *Die Kunst des Hackens; Social Engineering und Wirtschaftsspionage in IT-Sicherheit – Management und Praxis*. (Bd. 2, S. 40–42).

https://de.statista.com/statistik/daten/studie/36889/umfrage/bruttoinlandsprodukt-nach-bundeslaendern/.

https://www.nrwinvest.com/de/standort-nrw/internationale-unternehmen-in-nrw/.

https://www.wirtschaft.nrw/mittelstand.

https://www.mkw.nrw/studium/informieren/hochschulkarte-nrw/.

https://www.mkw.nrw/forschung/einrichtungen/ausseruniversitaere-forschung-in-nrw/.

https://www.bitkom.org/Presse/Anhaenge-an-PIs/2017/07-Juli/Bitkom-Charts-Wirtschaftsschutz-in-der-digitalen-Welt-21-07-2017.pdf, S. 5.

Sicherheitsarchitektur im Wandel: Der Beitrag der privaten Sicherheitsdienste für den Schutz der deutschen Wirtschaft

Harald Olschok

1 Überblick über die aktuelle politische Diskussion und die Forderungen des BDSW

Nach der Bundestagswahl am 24. September 2017 hat es fast ein halbes Jahr bis zur Bildung der neuen Bundesregierung am 14. März 2018 gedauert. Dieses lange Warten hat sich für uns gelohnt, weil in der Koalitionsvereinbarung der Großen Koalition unter anderem ausgeführt wird: „Private Sicherheitsbetriebe leisten einen wichtigen Beitrag zur Sicherheit. Durch die Neuordnung der Regelungen für das private Sicherheitsgewerbe in einem eigenständigen Gesetz werden wir die Sicherheitsstandards

Der Beitrag basiert in weiten Teilen auf dem 5. Weißbuch der CoESS, dem europäischen Dachverband der Sicherheitswirtschaft, „The new security company: integration of services and technology responding to changes in customer demand, demography and technology" (CoESS 2015). Es wurde gemeinsam von der CoESS und dem BDSW auf der Sicherheitstagung am 23. April 2015 in Berlin vorgestellt. An diesem Weißbuch haben mitgearbeitet: Martin Hildebrandt, Friedrich P. Kötter, Reinhard Rupprecht, Dr. Berthold Stoppelkamp und Silke Wollmann. Mein besonderer Dank gilt Kirsten Wiegand, Referentin für Sicherheitsforschung beim BDSW, für die kritische Durchsicht, die Korrekturen und Anmerkungen sowie die Zusammenstellung des Literaturverzeichnisses. Nicole Ernst ist für Erstellung unseres Statistiksatzes „Sicherheitswirtschaft in Deutschland" zuständig und hat die Abbildungen erstellt und in den Text eingefügt. Auch dafür vielen Dank!

H. Olschok (✉)
Zornheim, Deutschland
E-Mail: olschok@bdsw.de

C. Vogt et al. (Hrsg.), *Wirtschaftsschutz in der Praxis,* Sicherheit – interdisziplinäre Perspektiven, https://doi.org/10.1007/978-3-658-24637-2_2

in diesem Gewerbezweig verbessern und so für noch mehr Sicherheit und Verlässlichkeit sorgen“ (Bundesregierung 2018, S. 127). Damit hat der Bundesverband der Sicherheitswirtschaft (BDSW) ein wichtiges Verbandsziel erreicht. Seit Langem weisen wir darauf hin, dass das Gewerberecht bei Weitem nicht (mehr) ausreicht, der faktischen Bedeutung der privaten Sicherheitsdienste für die Innere Sicherheit in Deutschland gerecht zu werden. Wir haben in unserem Positions- und Forderungspapier vor der Bundestagswahl deutlich gemacht, welche Maßnahmen notwendig sind, um Deutschland noch sicherer zu machen (vgl. BDSW 2017).

Deutschland ist eines der sichersten Länder der Welt. Die veröffentlichten Zahlen aus der Polizeilichen Kriminalstatistik für das Jahr 2017 zeigen, dass die Zahl der in Deutschland erfassten Verbrechen im Vergleich zum Vorjahr um fast zehn Prozent gesunken ist (vgl. Bundeskriminalamt 2018). Dazu haben auch die privaten Sicherheitsunternehmen mit ihren rund 260.000 Mitarbeiterinnen und Mitarbeitern beigetragen. Sie leisten mit ihren Dienstleistungen und Produkten täglich einen wichtigen Beitrag zur Gefahrenabwehr innerhalb der Sicherheitsarchitektur Deutschlands. (Qualifizierte) private Sicherheitsdienste können zu einer wirkungsvollen Entlastung der Polizei beitragen und die objektive Sicherheit, aber auch das subjektive Sicherheitsempfinden der Bürgerinnen und Bürger, nachhaltig verbessern. Auch dazu müssen die privaten Sicherheitsdienste auf eine neue rechtliche Grundlage gestellt werden. Ziel muss es sein, die privaten Sicherheitsdienste in den Zuständigkeitsbereich der Innenbehörden zu überführen, wie dies in fast allen Mitgliedsstaaten der EU der Fall ist. Wir wissen um die damit einhergehenden juristischen, verwaltungsrechtlichen und politischen Herausforderungen.

Das im November 2016 vom Deutschen Bundestag beschlossene Gesetzespaket zur Änderung von bewachungsrechtlichen Vorschriften stellt einen Schritt in die richtige Richtung dar. Es bleibt aber hinter den Erwartungen des BDSW zurück. Die Einführung einer verschärften und regelmäßigen Überprüfung von Personal und Unternehmern, der Sachkundeprüfung für den künftigen Unternehmer und von leitenden Mitarbeitern beim Schutz von Flüchtlingsunterkünften und zugangsgeschützten Großveranstaltungen reichen nicht aus. Große Hoffnung setzen wir in das geplante „Bewacherregister“, das 2019 fertig sein soll. Dies muss die Anforderungen aus Sicht der Branche berücksichtigen und transparent und kostengünstig werden. Wichtig sind vor allem eine schnelle und unbürokratische Überprüfung von Sicherheitsmitarbeitern sowie eine Vermeidung von unnötigen und zeitaufwendigen Doppelüberprüfungen. Hierzu gehören auch die Überprüfung der waffenrechtlichen Genehmigungsverfahren für Geldtransporte sowie die Sicherheitsüberprüfungen beim Schutz von militärischen Liegenschaften oder in der Luftsicherheit.

Für einzelne Aufgabengebiete, die eine enge Zusammenarbeit mit der Polizei erfordern, sind spezialgesetzliche Regelungen zu schaffen. Das gilt für den Schutz

von Großveranstaltungen, Flüchtlingsunterkünften, des Öffentlichen Personenverkehrs und von Einrichtungen, die zu den kritischen Infrastrukturen zählen. Für den Schutz militärischer Liegenschaften, den Schutz von Atomkraftwerken und die Sicherheitsaufgaben an den Verkehrsflughäfen wurden derartige eigenständige rechtliche Regelungen bereits geschaffen. Nur in einer spezialgesetzlichen Regelung lassen sich Anforderungen an die Leistungsfähigkeit, Organisation, Qualifizierung sowie Ausstattung der privaten Sicherheitsdienste zwingend festlegen. Wichtig ist auch eine über das Gewerberecht hinausgehende erweiterte Zuverlässigkeitsprüfung. Die zahlreichen Piratenangriffe auf (deutsche) Schiffe vor rund zehn Jahren haben dazu geführt, dass im Gewerberecht die Voraussetzungen für den Einsatz bewaffneter privater Sicherheitsdienste geschaffen wurden. In diesem Fall wurden in kürzester Zeit neue rechtliche Grundlagen von der Politik geschaffen.[1]

Die Sicherheitswirtschaft und der sie vertretende BDSW sind in den letzten 15 Jahren ihrer sicherheitspolitischen Verantwortung für Deutschland gerecht geworden. Wir haben an der Entstehung mehrerer Studiengänge für privates Sicherheitsmanagement an den Polizeihochschulen in Berlin, Kiel-Altenholz und Hamburg aktiv mitgearbeitet. Das gilt auch für die beiden Ausbildungsberufe in der Sicherheitswirtschaft und für die Fortbildungsregelung zur Geprüften Schutz- und Sicherheitskraft. In zehn Bundesländern haben wir Kooperationsvereinbarungen mit den jeweiligen Landespolizeibehörden unterzeichnet. Außerdem arbeiten wir aktiv in der „Initiative Wirtschaftsschutz“ mit.

Diese Anstrengungen für noch mehr Qualität und Seriosität der Sicherheitsdienstleistungen werden nur dann nachhaltig sein, wenn – wie von der Großen Koalition vorgesehen – in der 19. Legislaturperiode die rechtlichen Rahmenbedingungen für die privaten Sicherheitsdienste auf eine neue, zeitgemäße

[1]Die zahlreichen Piratenüberfälle auf die internationale Schifffahrt haben im Sommer 2012 dazu geführt, dass die Bundesregierung beschlossen hat, künftig bewaffnete Sicherheitsdienste im Kampf gegen Piraterie zuzulassen. Deutschland ist nach Japan und Griechenland die größte Schifffahrtsnation und war deshalb von den Piraten-Überfällen in besonderer Weise betroffen. Die Forderungen der Polizeigewerkschaften, die Bundeswehr bzw. die Bundespolizei zum Transportschutz auf den internationalen Seewegen einzuführen, wurden von der Politik abgelehnt. Stattdessen wurde ein neues Zulassungsverfahren in das deutsche Gewerberecht eingeführt. Auf dieser Grundlage eines unternehmensbezogenen Ansatzes muss der Antragssteller darlegen, dass die von ihm eingesetzten Sicherheitskräfte über die erforderlichen Fähigkeiten und Kenntnisse verfügen und persönlich geeignet und zuverlässig sind. Die Zulassung erfolgt durch das Bundesamt für Wirtschaft und Ausfuhrkontrolle. In Deutschland sind derzeit sieben Unternehmen zugelassen. Es gab und gibt einen „Markt für Piratenbekämpfung“. Ziel muss es sein, diesen Markt auch für deutsche Sicherheitsunternehmen zu erweitern.