Das Thema Digitalisierung ist in aller Munde. Zum Teil führt es jedoch bereits zu Ermüdungserscheinungen. Und das, obwohl selten über eine Definition gesprochen wird. Mit dem Kompendium „Sicherheit - Gesellschaft - Digitalisierung“ trägt die TCC Verlagsgesellschaft mit Fachbeiträgen ausgewiesener Experten inhaltlich und mit Beispielen zur Diskussion über Digitalisierung und ihre Bedeutung für die Sicherheitswirtschaft sowie mögliche Auswirkungen auf gesellschaftliche Entwicklungen bei.

Sicherheit ist die Grundlage für gesellschaftliche Entwicklung. Digitalisierung ist eine Entwicklung durch die Gesellschaft. Dass mit der Digitalisierung Veränderungen stattfinden, steht fest. Wie sie definiert ist, wie sie wirkt und welche Gestaltungskraft von ihr ausgeht, beschreiben die Autoren:

Philip A. Caspari und Stephan Grinat, W.I.S. Sicherheit + Service
Matthias Clausmeyer, W.I.S. Unternehmensgruppe
Marian Meier-Andrae, MULTIROTOR
Dr. Frank Nikolaus, Nikolaus & Co. LLP
Dr. Tim Stuchtey und Dr. Johannes Rieckmann,
Brandenburgisches Institut für Gesellschaft und Sicherheit BIGS
Volker Wagner, Bundesverband ASW
Jan Wolter, Bundesverband ASW
Dirk Zundel, streamBASE

ISBN 978-3-947973-00-2

SICHERHEIT – GESELLSCHAFT – DIGITALISIERUNG

SICHERHEIT GESELLSCHAFT DIGITALISIERUNG

VERLAGS-GESELLSCHAFT

Inhalt

Günter Calaminus
Geschäftsführer
W.I.S. Unternehmensgruppe

***Günter Calaminus** ist seit Januar 2016 Geschäftsführer der W.I.S. Unternehmensgruppe mit Sitz in Köln. Seit über 25 Jahren ist er in leitenden Funktionen der deutschen Sicherheitswirtschaft auch für international operierende Sicherheitsunternehmen tätig. Zudem setzt er sich für die Entwicklung der Branche auch ehrenamtlich ein und ist u.a. im Verwaltungsrat des Brandenburgischen Instituts für Gesellschaft und Sicherheit BIGS aktiv.*

Vorwort

Sehr geehrte Damen und Herren,
liebe Leserinnen und Leser,

das Kompendium ***„Sicherheit – Gesellschaft – Digitalisierung“*** widmet sich aktuellen und künftigen Themen der Sicherheitswirtschaft und der Unternehmenssicherheit, die von ausgewiesenen Experten der Branche, von Verbänden und von der Wissenschaft aus verschiedenen Blickwinkeln und Perspektiven beleuchtet werden. Mit dem Kompendium verfolgen wir das Ziel, einen branchenübergreifenden Diskurs zum Thema Sicherheit im Zeichen der Digitalisierung – Chancen und Risiken anzustoßen.

Möglicherweise geht es Ihnen wie mir, wenn Sie mit Begriffen wie „Big Data“ oder Digitalisierung konfrontiert werden: Reflexartig möchte man sich wegducken und hofft, dass der Themenkelch an einem vorüberzieht. Der Grund, und darauf geht ***Dirk Zundel*** in seinem ***Beitrag „Digitalisierung – Keiner kann‘s mehr hören“*** ein, liegt häufig darin, dass eine klare Definition und ein eindeutiges Verständnis über Digitalisierung fehlen. Zudem wird das so bedeutsame Thema in den Medien inflationär verwendet, ohne nachhaltig in die Chancen-, Nutzen- und Risikobewertung einzusteigen.

Fest steht: das Internet hat mehr als nur neue Formen der Kommunikation und den Online-Handel gebracht. Heute sprechen wir vom „Internet der Dinge“, von Blockchain und Künstlicher Intelligenz (KI). Die Entwicklung von Hardware und Infrastruktur tun ihr übriges: Immer kleinere Prozessoren erzeugen immer mehr Leistung bis hin zum Quantencomputer. Datenautobahnen werden zu „Rennstrecken“, per Glasfaser oder „wireless“; Deutschland muss sich eher fragen, warum es in Lesotho besseren Empfang gibt als hierzulande. Zurückbleiben ist keine Option. Der Kampf um die Regelungs- und Deutungshoheit auf dem „Grid“ im Cyberspace findet seit Jahren statt. Die Datenschutzgrundverordnung (DSGVO) sei nur beispielhaft erwähnt.

Zuweilen fühlt man sich an die frühen 1980er Jahre und den Fantasy/Science Fiction Film Tron erinnert. Der Programmierer Flynn kämpft mit seinem Programm Tron gegen das alles beherrschende Master-Kontrollprogramm. Dieses hat ein gefährliches Eigenleben entwickelt und droht die Herrschaft auf dem Raster zu übernehmen. Was

damals noch „Fantasy“ war, hat sich heute zu einem ernsten und wahrhaftigen Problem entwickelt. Welche Bedeutung Bedrohungen aus dem Internet für die Wirtschaft und das Business Continuity Management sowie das geistige Eigentum und den Bestand Kritischer Infrastrukturen haben können, beleuchten der ***Vorsitzende Volker Wagner*** und der ***Geschäftsführer Jan Wolter vom Bundesverband Allianz für Sicherheit in der Wirtschaft (ASW).***

Wie es um die Sicherheitswirtschaft steht und wer zu ihr zählt, darauf gehen ***Dr. Tim Stuchtey*** und ***Dr. Johannes Rieckmann*** vom ***Brandenburgischen Institut für Gesellschaft und Sicherheit*** – kurz: ***BIGS*** – ein. In ihrem ***Beitrag „Die Vermessung der Sicherheitswirtschaft – Wachstum und Veränderung im Zeichen der Digitalisierung“*** gehen sie davon aus, dass es für eine Analyse erforderlich ist, „ein klares Verständnis von Sicherheit zu haben. Sicherheit wird am BIGS als das Ergebnis aus einer Funktion von externer Bedrohung und den Schutzleistungen einer Gesellschaft zu deren Kompensation betrachtet. Ceteris Paribus steigt also die Sicherheit, wenn der Staat oder private Wirtschaftssubjekte mehr für Schutzleistungen ausgeben oder die Bedrohung durch Kriminalität, Terrorismus oder Naturkatastrophen zurückgeht. Schutzleistungen können demnach z.B. Ausgaben für die Polizei oder private Sicherheitsunternehmen sein.“ Zudem führe die fortschreitende Digitalisierung dazu, dass sich die Sicherheitswirtschaft verändere. „Immer günstiger werdende Sicherheitstechnik bei gleichzeitig steigenden Lohnkosten führen zu einer Verschiebung von Arbeit zu Kapital, das bei der Sicherheitsherstellung zum Einsatz kommt.“

Nach Beiträgen, die grundsätzlich Chancen und Risiken aufzeigen sowie eine Zuordnung ermöglichen, sind die nachfolgenden Abhandlungen an der Praxis orientiert. Mit ihnen steigen wir auch in die Umsetzung von Digitalisierung in hochwertige Sicherheitsdienstleistungen ein. ***Stephan Grinat*** und ***Philip A. Caspari*** gehen in ihrem ***Beitrag „Predictive Analytics und Künstliche Intelligenz in der Sicherheitswirtschaft“*** u.a. der Frage nach, „warum Predictive Analytics und Künstliche Intelligenz nicht für ganzheitliche Sicherheitsarchitekturen genutzt werden und ob das derzeit vorherrschende Verständnis von Sicherheit den Anforderungen der Zukunft gewachsen sein wird“. Wie sich die Digitalisierung und der Umgang mit dem Mehrwert „Unternehmensdaten“ im Verbund mit qualifiziertem Sicherheitspersonal auf die Sicherheitswirtschaft und ihre Geschäftsmodelle entwickelt, beleuchten meine Führungskräfte. Sie sind erfahrene Spezialisten im Bereich Corporate Security und verfügen über internationale Einsatzerfahrungen bei der Bundeswehr.

Mit dem ***Beitrag „Drohnen in der Sicherheitswirtschaft“*** von ***Marian Meier-Andrea***, Geschäftsführer der bei Berlin ansässigen ***Multirotor GmbH***, richten wir den Blick in die dritte Dimension. Etwas überspitzt könnte man sagen, dass die Entwicklung der aus dem Modellbau stammenden „Flugrobotik“ und ihr Einsatz im Rahmen ziviler Sicherheitsanwendungen nahezu synchron mit der Digitalisierung verläuft. Der Beitrag veranschaulicht beispielsweise den polizeilichen Einsatz von Drohnen durch das Landeskriminalamt Berlin. Es setzt Multirotor-Systeme u. a. zur Tatortvermessung ein und hält sie inzwischen für unverzichtbar. Zudem werden interessante Alternativen zu personalintensiven Dienstleistungen bei der Objektbewachung aufgezeigt. In einer demographisch bedingt zunehmend schwierigen Personallage ein attraktives Instrument. Jedoch schildert der Autor diese Entwicklungen auch im Spiegel sich ändernder datenschutzrechtlicher Bestimmungen sowie sicherheitstechnischer Anforderungen, die für den Einsatz von Flugrobotik im Zusammenhang mit sicherheitsrelevanten Dienstleistungen unabdingbar sind.

Und dass mit der Digitalisierung herausfordernde Veränderungen einhergehen, weiß auch ***Matthias Clausmeyer***, unser Chief Financial Officer. In seinem Beitrag ***„Grundlagen der digitalen Transformation - Aus Sicht eines CFOs“*** gibt er Einblicke in Voraussetzungen und Anstrengungen, die für eine erfolgreiche digitale Transformation notwendig sind. In seinem Beitrag „werden die aufgekommenen Fragestellungen sowie die gegebenen Antworten, die eigenen Erfahrungen und die hoffentlich gezogenen Lehren… skizziert, wobei diese Ausführungen auf keinen Fall als vollumfänglich anzusehen sind“. Dennoch bieten sie dem geneigten und an einer digitalen Transformation interessierten Leser realistische und wegweisende Einblicke in diesen Prozess.

Abschließend beleuchtet ***Dr. Frank Nikolaus*** in seinem Beitrag ***„Blockchain: Ein Fall für die Sicherheitswirtschaft?“*** die zahlreichen Facetten der Blockchain/Distributed Ledger Technologie und ihre Auswirkungen auf die Sicherheitswirtschaft. „Es lässt sich feststellen, dass sowohl erhebliche Potenziale in der Schaffung zusätzlicher Sicherheit für Menschen und Daten in der Technologie wohnen, sie aber zugleich neue Bedrohungsszenarien schafft, die einer professionellen Absicherung und Verteidigung durch Unternehmen der Sicherheitswirtschaft erfordern.“

Mit den Beiträgen in unserem ersten Kompendium unter dem ***Titel „Sicherheit – Gesellschaft – Digitalisierung“*** haben wir mit der W.I.S. Unternehmensgruppe Neuland betreten. Mit diesem Schritt beabsichtigen wir, einen inhaltlichen Beitrag zur Diskussion über den Digitalisierungsprozess in der zivilen Sicherheitswirtschaft zu leisten. In einer Zeit, in der private Sicherheitsakteure in Deutschland quantitativ und qualitativ immer bedeutsamere Partner für behördliche Sicherheitsakteure werden, setzen wir uns als TOP 10 Sicherheitsdienstleister, führender Technikintegrator und Spezialist für Corporate Security an die Spitze einer inhaltsgetriebenen Entwicklung.

Mein Dank gilt den Autoren dieses Kompendiums, die mit großer Begeisterung und Engagement das Projekt inhaltlich möglich gemacht haben. Zudem danke ich den im Hintergrund arbeitenden, fleißigen Händen meiner Mitarbeiter. Allen voran Maren Prill und Jan Wosnitzka-Koch, die unermüdlich die Organisation des Projektes betreut haben.

Ich freue mich, diese Entwicklung gemeinsam mit Ihnen anzugreifen und ins Gespräch zu kommen. Nun wünsche ich Ihnen viel Freude bei der Lektüre.

Mit freundlichen Grüßen /
Kind regards

Günter Calaminus

Dr. Johannes Rieckmann
Senior Research Fellow
BIGS

Dr. Johannes Rieckmann *ist seit August 2015 als Senior Research Fellow am BIGS tätig. Er beschäftigt sich unter anderem mit ökonomischen Fragestellungen von Cybersicherheit, Ordnungspolitik im Zusammenhang mit der Bereitstellung von Schutz durch öffentliche und private Dienstleister; sowie der Vernetzung von Akteuren der zivilen Sicherheit aus Forschung und Entwicklung, Produktion, Politik und praxisorientierten Anwendern im Zusammenhang mit Forschungs-Rahmenprogrammen. Dr. Rieckmann hat Wirtschaftswissenschaften in Bremen und Paris studiert, arbeitete für Unternehmensberatungen in Hamburg und Brüssel und promovierte anschließend am Lehrstuhl für Volkswirtschaftstheorie und Entwicklungsökonomik an der Universität Göttingen. Im Rahmen seiner anschließenden Tätigkeit in der Abteilung Entwicklung und Sicherheit am DIW Berlin arbeitete er an der Entwicklung des WISIND-Indikators zur Abbildung objektiver Kriminalitätslage – unter Berücksichtigung von Dunkelfeld und Schweregrad – sowie subjektiver Wahrnehmung in Deutschland. Weiterhin koordinierte er Feldforschung im Rahmen einer entwicklungsökonomischen Studie in Kirgistan.*

Dr. Tim Stuchtey
Diplom-Volkswirt
Direktor BIGS

Dr. Tim Stuchtey *ist Diplom-Volkswirt und hat an der Westfälischen Wilhelms-Universität Münster studiert und an der Technischen Universität Berlin im Fachgebiet Wirtschafts- und Infrastrukturpolitik promoviert. Er war zunächst persönlicher Referent des Präsidenten der TU Berlin bevor er für einen Spitzenverband der deutschen Wirtschaft im Bereich Wirtschaftspolitik arbeitete. 2001 wechselte er an die Humboldt-Universität zu Berlin als Leiter der neu geschaffenen Stabsstelle für strategische Entwicklung und Planung und wurde später Leiter des Präsidialbereichs. An der Humboldt-Universität baute Tim Stuchtey die Humboldt Institution on Transatlantic Issues (HITI) auf und wechselte 2007 als Senior Fellow und Program Director Business and Economics an das American Institute for Contemporary German Studies (AICGS) an der Johns Hopkins University in Washington, DC. 2010 wurde er geschäftsführender Direktor des neu gegründeten Brandenburgischen Instituts für Gesellschaft und Sicherheit gGmbH (BIGS) in Potsdam. Seine Forschungsschwerpunkte liegen im Bereich der Ökonomie der Sicherheit, der transatlantischen Wirtschaftsbeziehungen und der klassischen Ordnungspolitik.*

Brandenburgisches Institut für Gesellschaft und Sicherheit gGmbH
Dianastra. 46
14482 Potsdam
Tel. + 49 (0)331 704 406 -0
E-Mail: info@bigs-potsdam.org

Die Vermessung der Sicherheitswirtschaft – Wachstum und Veränderung im Zeichen der Digitalisierung

von Johannes Rieckmann und Tim Stuchtey

Ein immer größerer Teil unseres Lebens ist durch die Digitalisierung betroffen. Dies gilt nicht nur für uns als Individuum, sondern auch für Geschäftsprozesse und die Wertschöpfung innerhalb der Volkswirtschaft. Als Konsequenz wächst die Verfügbarkeit von Daten über unser Tun und Schaffen exponentiell. Daten werden als das Öl des 21. Jahrhunderts bezeichnet und sind der Rohstoff, der die digitale Wirtschaft zum Laufen bringt. Daten stellen insofern einen erheblichen Wert dar und diesen Datenschatz gilt es, adäquat zu schützen.

Diese Entwicklung wurde von der Polizei bislang nicht mit gleicher Geschwindigkeit mitverfolgt. Der Cyberraum als neue Dimension für Leben, Wirtschaften sowie illegales Handeln ist polizeilich kaum erschlossen. Wer käme schon auf die Idee, einen durch Ransomware befallenen Computer zur nächsten Polizeistation zu tragen und dort Hilfe zu verlangen. Der Mangel an staatlichem Schutz bei gleichzeitiger Nachfrage nach eben diesem durch private Wirtschaftssubjekte führt dazu, dass sich ein weites Feld für private Sicherheitsdienstleistungen ergibt, durch die diese Lücke zumindest teilweise geschlossen werden kann.
Die Digitalisierung verändert aber auch die Sicherheitswirtschaft selbst. Immer günstiger werdende Sicherheitstechnik bei gleichzeitig steigenden Lohnkosten führen zu einer Verschiebung von Arbeit zu Kapital, das bei der Sicherheitsherstellung zum Einsatz kommt. Gleichzeitig fallen durch die unterschiedlichen Sicherheitstätigkeiten privater Sicherheitsunternehmen selbst eine erhebliche Menge an Daten an. Dieser Datenpool kann erschlossen werden um daraus einen Mehrwert für die Unternehmen selbst und besser noch ihre Kunden zu schaffen. In welchem Umfang dies erfolgt wollen wir mit diesem Beitrag analysieren.

Für die Analyse ist es erforderlich, ein klares Verständnis von Sicherheit zu haben. Sicherheit wird am Brandenburgischen Institut für Gesellschaft und Sicherheit (BIGS)

als das Ergebnis aus einer Funktion von externer Bedrohung und den Schutzleistungen einer Gesellschaft zu deren Kompensation. Ceteris Paribus steigt also die Sicherheit, wenn der Staat oder private Wirtschaftssubjekte mehr für Schutzleistungen ausgeben oder die Bedrohung durch Kriminalität, Terrorismus oder Naturkatastrophen zurückgeht. Schutzleistungen können demnach z.B. Ausgaben für die Polizei oder private Sicherheitsunternehmen sein.

Übergeordnete Veränderungsprozesse

Die Sicherheitswirtschaft in Deutschland durchlebt seit einigen Jahren einen dynamischen Änderungsprozess. Als Sicherheitswirtschaft wird an dieser Stelle die Gesamtheit der in Deutschland ansässigen Anbieter von physischen Sicherheitsprodukten, Sicherheitsdienstleistungen sowie des sich dieser Trennung teilweise entziehenden Bereiches der Anbieter von „IT in der Sicherheit“ und „Sicherheit in der IT“ betrachtet.

Neben Änderungen in der Lohnhöhe und –Struktur mit den ersten (allgemeinverbindlichen) Tarifverträgen und später mit der Einführung des Mindestlohns im Jahr 2015, sowie in der Wettbewerbs- und Personallage durch regulatorische Änderungen und EU-Erweiterungen waren in den vergangenen Jahren vor allem zwei Entwicklungen von Bedeutung: die Flüchtlingskrise und die bereits angesprochene Digitalisierung.

Mit der Flüchtlingskrise gab es einen Sondereffekt, dessen Bedeutung vorerst wieder nachgelassen hat. Mit dem sprunghaften Anstieg des Zustroms schutzsuchender Kriegsflüchtlinge sowie von Armutsmigranten nach Europa und hier besonders nach Deutschland im Jahr 2015 und 2016, stieg die Nachfrage nach klassischen Sicherheitsdienstleistungen ebenfalls an. Bei diesem Nachfrageanstieg ging es vor allem um die Bewachung von Flüchtlingsunterkünften nach außen, und um den Ordnungsdienst innerhalb der Unterkünfte. Mittlerweile hat der Zustrom von Migranten nachgelassen und damit ist auch die zusätzliche Nachfrage nach entsprechenden Sicherheitsdienstleistungen wieder entfallen. Ob diese Entwicklung von Dauer sein wird, hängt von vielerlei Faktoren ab, die zu einem großen Teil außerhalb Deutschlands liegen, jedoch von der deutschen sowie europäischen Außenpolitik mitgestaltet werden.

Dieser in Politik und Gesellschaft stark beachtete Effekt lässt leicht vergessen, welchen übergeordneten Trend wir seit Jahren in der Sicherheitswirtschaft beobachten können. Die Digitalisierung dürfte für die Branche von noch größerer Bedeutung sein und deutlich langfristiger wirken. Schließlich betrifft sie eine qualitative Veränderung und auch Erweiterung der Arbeit vor allem von Sicherheitsdienstleistern, und mittelbar auch der Hersteller von Sicherheitsprodukten und Vorleistungen. Denn klassische Sicherheitsdienstleistungen werden durch Informationstechnologie-Sicherheitsdienstleistungen ergänzt (Komplementäreffekt), verändern sich im Rahmen der Digitalisierung, und werden teilweise sogar ersetzt (Substitutionseffekt).

Ein Beispiel für einen solchen Komplementäreffekt wäre die Unterstützung der Sicherheitsfirma eines Shopping Centers durch „intelligente“, auf Algorithmen basierende Videoanalyse z.B. im zugehörigen Parkhaus. Diese kann automatisiert auf Auffälligkeiten hinweisen, wie beispielsweise das mehrfache Umsetzen desselben Fahrzeuges innerhalb des Parkhauses von einem Stellplatz zum nächsten – etwa immer näher heran an einen tragenden Pfeiler oder eine bestimmte Tür.

Ein Substitutionseffekt läge vor, wenn durch auf Algorithmen basierende Videoanalyse die Stelle des menschlichen Bildschirmbeobachters weitgehend oder gar gänzlich entfiele. Ein solcher Substitutionseffekt bedeutet eine Änderung der Kombination aus Inputfaktoren (Humankapital/Arbeit und Kapital /Technik) zur Produktion des gleichen Outputs. Arbeit wird teilweise und zusehends durch Kapital ersetzt. So ermöglichen nicht nur Anlagen für automatisierte Videoüberwachung und Bildauswertung einen geringeren Personaleinsatz in der Leitzentrale. Drohnentechnik ermöglicht Perimeter-Überwachung in Echtzeit, und damit eine Reduktion der herkömmlichen Streifentätigkeit sowie verbesserte Reaktionszeiten für Interventionskräfte.
Es zeigt sich, dass einige Sicherheitsunternehmen die neuen technischen Möglichkeiten bei der Erstellung ihrer Dienstleistungen annehmen und für Veränderungsprozesse offen sind. Andere Branchenteilnehmer halten an der herkömmlichen nahezu vollständig auf dem Faktor Arbeit beruhende Dienstleistung fest. Somit spaltet sich die Branche in zwei Gruppen: Zum einen gibt es auch weiterhin die „klassischen“ Wachschutz- und Sicherheitsunternehmen, welche relativ wenig komplexe Dienstleistungen verkaufen. Diese zeichnen sich durch vergleichsweise geringe Arbeitsproduktivität und Innovationskraft aus, und betreiben oft nicht einmal eine Website. Digitalisierung spielt hier voraussichtlich in den kommenden Jahren nur eine begrenzte Rolle.
Die andere, innovativere Gruppe von Sicherheitsunternehmen passt sich den neuen technischen Möglichkeiten dahingehend an, dass sie nicht mehr primär Mann- oder besser Personenstunden verkaufen. Vielmehr werden vermehrt in-

tegrierte Sicherheitslösungen vermarktet. Ein ergebnisorientierter Ansatz tritt hier an die Stelle eines prozessorientierten.

Technischer Wandel – schleichend bis disruptiv

Sicherheit ist nach unserem Verständnis eine Funktion aus zwei Faktoren, nämlich Bedrohung einerseits und Schutz andererseits. Bedrohungen können dabei natürlicher Art sein (z.B. Sturmflut) oder vom Menschen bewusst herbeigeführt (z.B. Kriminalität oder Terrorismus). Während die erstgenannte sich durch vom Menschen geschaffene Schutzleistungen nicht verändert, ist letztere dynamisch und anpassungsfähig. Kriminelle und Terroristen sind anders als Naturereignisse in der Lage, ihre Taktik auf Grund von neuen oder veränderten Schutzleistungen anzupassen. Daher stehen die Schutzleistungen grundsätzlich in einem Wettbewerb mit der Bedrohung. Das Ergebnis dieses Wettbewerbs ist das Maß an erreichter Sicherheit.
Mit der Digitalisierung unseres Wirtschafts- und Privatlebens erwächst auch die Notwendigkeit, den Cyberraum vor neuen Bedrohungen zu schützen. So haben sich im Zuge des technischen Fortschritts ab den 80er- und 90er Jahren[1] vermehrt Produkte und Dienstleistungen zum Schutz von IT-Systemen entwickelt und etabliert. Zugleich aber haben sich durch die Technik auch Sicherheitsdienstleitungen und -Produkte in vormals rein physisch geprägten Bereichen verändert. So sind einige Felder heute schlichtweg überholt, bereits obsolet geworden oder verschwinden nach und nach vom Markt.

Andere Dienstleistungen bestehen weiter, haben sich aber in ihrer Form mehr oder minder stark verändert. Dazu gehören beispielsweise die Gepäck- und Fluggastkontrollen. Früher wurden Haupt- und Handgepäck meist stichprobenartig geöffnet und einer optischen und haptischen Kontrolle unterzogen – und ggf. auch einer olfaktorischen, mit Hilfe von Spürhunden. Die Passagiere wurden stichprobenartig einer Leibesvisitation unterzogen, ab den 1970er-Jahren kamen Metalldetektoren hinzu.

Heute dagegen sieht die Kontrolle an Flughäfen anders aus: Jedes Gepäckstück und jeder Passagier wird kontrolliert, allerdings jetzt mit elektronsicher Hilfe. Metalldetektoren, Röntgen- oder Terrahertz-Scanner und Analysesoftware zur Unterstützung der Kontrolleure gestalten den Prozess effizienter und effektiver. Stichprobenartig kommen zusätzlich Ionen-Mobilitäts-Spektrometer zum Einsatz, diese erschnüffeln Spreng- und Kampfstoffe sowie andere unerlaubte Substanzen wie illegale Drogen. Der Spürhund kommt jetzt erst beim Auftreten eines Verdachtsmoments zum Einsatz.

Die Elektronisierung und Digitalisierung hat hier also die Natur der Schutzleistung – eine eingehende Suche nach potenziell gefährlichen Gegenständen und Substanzen – nicht verändert, wohl aber ihre Effizienz – insbesondere die Geschwindigkeit – und ihre Effektivität – insbesondere die Genauigkeit und Unempfindlichkeit gegenüber Ermüdung und Manipulation – erhöht. Gleichzeitig empfinden viele der einer solchen Kontrolle unterzogenen Fluggäste die Kontrollen im Vergleich zu den früheren Verfahren als weniger invasiv, belästigend und willkürlich.
Ein weiteres Beispiel für veränderte Tätigkeiten ist der Betrieb von Videoüberwachungs-Leitstellen. Intelligente Videoanalyse erkennt automatisiert verdächtiges und überprüfungswürdiges Verhalten und besondere Vorkommnisse, wie weiter oben bereits am Parkhaus-Beispiel kurz angerissen wurde. Die entsprechenden, im Algorithmus hinterlegten Kriterien können beliebig programmiert werden: Plötzliche Gruppenbildung oder Aufteilung von Menschen kommt genauso in Frage wie Stürze, Schlägereien, Rennen, oder die Übergabe von Gegenständen. Hin- und Hergehen in bestimmten Bereichen bei konstanter Blickrichtung, räumliches Trennen von Personen von ihren Gepäckstücken über bestimmte Entfernungen oder Zeiträume hinaus, Kleidungswechsel bei identischem Gangmuster, Vermummung, „unrunde“ Gangmuster (die Hinweis auf verdecktes Tragen einer Waffe oder eines Sprengstoffgürtels sein könnten), sichtbare Feuerwaffen etc. können ebenfalls von Interesse sein.
Weitere Felder gab es früher zumindest in der heutigen Form gar nicht, sie sind im Zuge der Digitalisierung neu hinzugekommen bzw. haben ihren Charakter so stark verändert, dass es sich um neue Tätigkeiten handelt. Hier wäre beispielsweise die Absicherung von Geländen, Veranstaltungen oder seltener Einzelpersonen gegenüber Bedrohungen durch unbemannte Fluggeräte anzuführen. Früher war es schlicht nicht möglich, einen wirksamen Schutz gegenüber Bedrohung durch beispielsweise ferngesteuerten Modellflugzeugen mit Sprengstoff zu gewährleisten. Allerdings war dies auch ein weniger relevantes Thema als heute (obwohl es beispielsweise schon 1977 Pläne der Roten Armee Fraktion gab, auf den damaligen bayerischen Ministerpräsident, Franz Josef Strauß ein entsprechendes Attentat zu verüben[2]). Heute sind

[1] Die erste bekannte hacking-Attacke wurde bereits 1903 durchgeführt, als der Londoner Zauberkünstler Nevil Maskelyne eine Morse-Vorführung von Guglielmo Marconi störte und eigene, beleidigende Nachrichten einschleuste. Der Begriff wurde jedoch erst Mitte der 50er am Massachusetts Institute of Technology geprägt, und an Bedeutung gewannen hacker erst ab den späten 80er Jahren.

[2] WELT (2008) „RAF wollte Strauß mit einem Modellflugzeug töten.“ https://www.welt.de/politik/article2480440/RAF-wollte-Strauss-mit-einem-Modellflugzeug-toeten.html Veröffentlicht am 23.09.2008, letzter Abruf 05.10.2018.

Abbildung 1: Neue Möglichkeiten und Herausforderungen durch Technologie. Nicht das Produkt von Boston Dynamics, aber ein möglicher Ersatz für einen Sicherheitsdienstmitarbeiter auf Streifengang.

die entsprechenden Fluggeräte unvergleichlich manövrierfähiger und dabei leichter zu bedienen, billiger, und können höhere Nutzlasten transportieren. Die Programmierbarkeit der Flugbahnen in Kombination mit Global Positioning Systems (GPS) eröffnet neue Bedrohungsszenarien beispielsweise für den zivilen Luftverkehr. Auch die Miniaturisierung der Kameratechnik hat hier neue Missbrauchsmöglichkeiten eröffnet.

Gab es nun bis vor wenigen Jahren nur eingeschränkte Detektions- und vor allem physische Abwehrmöglichkeiten (etwa Flintenschützen auf Tagungsgebäuden, auf die Beizjagd auf Fluggeräte dressierte Raubvögel, Drohnen mit Fangnetzen), so hat sich hier ein ganz neues Geschäftsfeld eröffnet. Kombinierte Sensorik nutzt heute Radartechnik, Mikrofone und Audioanalyse, Videokameras, Infrarot- und Frequenzscanner. Sie ermöglicht Früherkennung von Fluggeräten bereits beim Kopplungsvorgang der Fernbedienung mit dem Fluggerät (pairing) beziehungsweise – falls dies außerhalb der Überwachungsreichweite vollzogen wird – ihrer Annäherung über größere Entfernungen.

Störsender – mittlerweile auch in portablen Versionen als sogenannte Drohnengewehre - erlauben die Lähmung oder sogar die Übernahme der Steuerung mittels Funk, oder eine Störung oder Verfälschung (spoofing) des GPS-Signals und damit eine Manipulation der Navigationsfähigkeit der Drohne. Sogar sogenannte Netzwerfer, Laser oder elektromagnetischer Puls können als Wirkmittel zum Einsatz gebracht werden, allerdings besteht hier die Gefahr eines unkontrollierten Absturzes. Bei einer Störung des Steuerungssignals oder der Navigation verhalten sich Drohnen entsprechend ihrer Programmierung und Einstellung – vom Rückkehren zum Ausgangsort über Verharren am Platz oder kontrolliertem senkrechten Landen bis hin zu Fortsetzen der letzten Aktion – unterschiedlich, stürzen aber im Gegensatz zu den ersten am Markt erhältlichen Modellen mittlerweile nicht mehr ab.

Ein weiteres Beispiel für ein neu hinzukommendes, brandaktuelles Thema – mit potenziell erheblichem Regulierungs- und Technikfolgeabschätzungsbedarf – ist die annähernd erreichte Marktreife von geländegängigen und weitgehend autonom agierenden Maschinen. So wäre es etwa denkbar, bislang übliche Personenstreifen im Wachschutz teilweise durch „Roboterhunde“ zu ersetzen, wie sie etwa die Firma Boston Dynamics im Juni 2018 auf der Technikmesse Cebit in Hannover vorstellte und ab kommendem Jahr unter dem Produktnamen „SpotMini“ (siehe Abbildung 1) für jedermann zu verkaufen plant. Diese könnten dann etwa ermüdungsfrei Treppenhäuser oder bei Wind und Wetter weitläufige Firmengelände ablaufen und mit Kameratechnik überwachen.

Datenschatz braucht Datenschutz

Der technische Wandel innerhalb der Sicherheitswirtschaft führt letztlich auch zu einem stärkeren anfallen digitaler Daten in diesen Unternehmen. Auch in der Vergangenheit gab es Kundendaten oder Einträge (auch mit personenbezogenen Daten) in Wachbüchern, die es galt „gut weg zu schließen“. Heute fallen diese Daten digital an und können einen Mehrwert für das Unternehmen und seine Kunden bringen. Sie können dem Unternehmen aber auch, wenn sie in die falschen Hände fallen, erheblichen Schaden zufügen. Es gilt, gegenüber (potenziellen) Kunden sowie Politik, Verwaltung, Presse und Bürgern glaubhaft zu machen, dass mit diesen sensiblen Daten sorgsam und den rechtlichen Vorschriften entsprechend umgegangen wird. Die Daten dürfen also nur für die vorgesehenen und vereinbarten Zwecke verwendet werden, und müssen gegen kriminellen Missbrauch hinreichend abgesichert werden.

Verschärfend wirkt hier der Umstand, dass einerseits sich entwickelnde Analysemöglichkeiten großer Mengen unstrukturierter Daten – Stichworte big data und Metadaten-Analyse – manche Unternehmen in der öffentlichen Wahrnehmung in die Lage versetzen, Zusammenhänge und Verbindungen möglicherweise effektiver erken-

nen zu können, als manche Sicherheitsbehörden. Diese Wahrnehmung, die durchaus in Misstrauen der Öffentlichkeit umschlagen kann, betrifft derzeit vor allem Unternehmen aus dem Bereich der Telekommunikation, Soziale Netzwerke, Email-Anbieter, Handelsplattformen usw., aber auch Krankenversicherungen, Banken, und zukünftig möglicherweise eben auch Sicherheitsunternehmen. Hier ist also insbesondere in Bezug auf personenbezogene Daten ein solides und auch nach außen kommuniziertes Datenschutzmanagement von elementarer Bedeutung.

Fachkräftemangel, Personalwerbung und Anreizstrukturen

Der vermehrte Technikeinsatz und die Digitalisierung in der Sicherheitswirtschaft führen dazu, dass die Anforderungen an die Fähigkeiten und Ausbildung des Personals in dieser Branche ansteigen. Diese verstärkte Nachfrage nach mehr Humankapital trifft am Arbeitsmarkt auf den langfristigen demographischen Trend immer kleiner werdender Geburtenjahrgänge und auf eine lang anhaltende konjunkturelle Wachstumsphase der deutschen Volkswirtschaft. Insbesondere beim Angebot von Menschen mit besonderen IT-Kenntnissen besteht schon heute ein erheblicher Fachkräftemangel. Die Folge ist ein sich zusehendes verschärfender Wettbewerb nicht nur um die besten Talente, sondern um alle verfügbaren Fachkräfte. Besonders zu spüren bekommen diese neuen Rahmenbedingungen die einschlägigen Sicherheitsbehörden im Bereich Informationstechnik. Dies gilt umso mehr, da sie eingeschnürt im Korsett der Tarifverträge des öffentlichen Diensts sind und mit beschränkten Anreizmöglichkeiten um dieselben Fachkräfte werben müssen wie die Privatwirtschaft.

„Das Wams des Beamten ist eng, aber es wärmt“, soll Friedrich II. gesagt haben. In näherer Zukunft wird er in diesem Arbeitsfeld vergleichsweise wohl von vielen als vor allem eng empfunden, was eine handfeste Herausforderung für die behördliche Personalwerbung darstellt. Hier eröffnet sich allerdings auch ein neues oder zumindest stark erweitertes Geschäftsfeld für die Sicherheitswirtschaft. Als Berater und Auftragnehmer werden zusehends Unternehmen im Bereich Informationstechnik von Behörden in die Sicherheitsarchitektur eingebunden.

Struktur der Sicherheitswirtschaft mit engerem Digitalisierungsbezug

Neben der Unterscheidung zwischen digitalisierten Sicherheitsunternehmen einerseits und klassischen Sicherheitsunternehmen andererseits ist auch eine Differenzierung zwischen Produktherstellern und Dienstleistern von Aussagekraft für die Veränderungen auf dem Markt der Sicherheitswirtschaft. Das BIGS führt seit dem Jahr 2012 regelmäßig Befragungen der Sicherheitswirtschaft durch, die empirisch ausgewertet werden. Hieraus lassen sich über die Zeit aufschlussreiche Entwicklungen und strukturelle Verschiebungen ableiten. Nachfolgend sollen insbesondere solche Veränderungen näher betrachtet werden, die einen Bezug zur Digitalisierung in der Sicherheitswirtschaft aufweisen.

Kaum überraschend ist, dass knapp 80 Prozent der 2014 erfassten IT-Sicherheitsunternehmen erst nach 1990 gegründet wurden – 2017 waren es sogar 86 Prozent. Dies korreliert vermutlich auch mit der starken Zunahme von Computern in privaten Haushalten sowie in den Unternehmen, die ab Mitte der 90er Jahre Computer in den Betriebsalltag integriert haben. Aufmerken lässt, dass fünf Unternehmen, die vor 1949 gegründet wurden in der Umfrage angeben, hinsichtlich ihres Produktportfolios reine IT-Sicherheitsunternehmen zu sein. Dies lässt sich wohl nur so interpretieren, dass es einigen traditionellen Unternehmen gelungen ist, sich erfolgreich an den technischen Wandel anzupassen. Zudem zeigt die detailliertere Betrachtung dieser fünf Datensätze, dass fast alle Unternehmen Sicherheitsberatungen und -dienstleistungen zur IT-Sicherheit anbieten. Zudem sind diese Unternehmen über ihren eigenen Standort hinaus und teilweise deutschlandweit tätig.
Die Größe der Unternehmen nach Umsatz und Mitarbeiter variiert je nach Marktsegment erheblich. Bei der Analyse der IT-Sicherheitsunternehmen konnte festgestellt werden, dass es sich bei diesen insgesamt um eher kleinere Unternehmen mit einem verhältnismäßig geringen Umsatz handelt. In den Marktsegmenten Sicherheitsdienstleistungen und –technologie sind hingegen überwiegend größere Unternehmen tätig.

Das Produktsegment IT-Sicherheit wurde 2014 von ca. 21 Prozent der nicht nur ausschließlich im zivilen, sondern auch im militärischen Sektor aktiven Unternehmen angeboten. Interessant ist zudem, dass die Hälfte dieser Unternehmen auf dem internationalen Markt aktiv ist – 2017 waren es sogar alle der entsprechenden in der Umfrage erfassten Unternehmen. Dieser Anteil liegt erheblich über dem Durchschnitt.

Die Verteilung der Produktportfolios der Sicherheitsunternehmen variiert teilweise beträchtlich über die Bundesländer. In Bayern sind laut Angaben der Teilnehmer der Befragung insbesondere IT-Sicherheitsunternehmen dominierend, während in Nordrhein-Westfalen vor allem Anbieter von Sicherheitsprodukten und -techni-

ken ihren Hauptstandort haben. Mit Standorten in Baden-Württemberg sind IT-Sicherheitsunternehmen fast so häufig vertreten, wie Unternehmen von Sicherheitsprodukten und -techniken. Interessant ist zudem, dass in Berlin vor allem traditionelle Sicherheitsdienstleister am häufigsten angesiedelt sind. Bei den meisten Bundesländern hingegen war zumindest bis 2015 eine Dominanz der IT-Sicherheitsunternehmen oder der Unternehmen, die Sicherheitsprodukte und -techniken anbieten, zu erkennen.
Die traditionelle Unterteilung einer Volkswirtschaft in die drei Sektoren Landwirtschaft, Industrie und Dienstleistungen spielt zunehmend eine geringe Rolle. Neben der immer geringeren Bedeutung der Landwirtschaft führt besonders die Digitalisierung von Wirtschaftsprozessen vermehrt dazu, dass die Grenzen zwischen den einzelnen Sektoren undeutlicher werden. Dieser Prozess ist auch bei den Unternehmen der Sicherheitswirtschaft zu beobachten, deren Produktmix sich verändert. Wo neue Unternehmen in den Markt eintreten, ist deren Angebot häufig nicht mehr eindeutig als Technikprodukt oder als Dienstleistung zu klassifizieren.

Interessant ist die Entwicklung der Tätigkeitsfelder von Unternehmen der Sicherheitsbranche, in denen es in den letzten Jahren auch unabhängig von der Digitalisierung zu erheblichen Verschiebungen gekommen ist, und vermutlich auch in den kommenden Jahren Änderungen geben wird. Diese bewegen sich dabei durchaus nicht nur in eine Richtung, sondern unterliegen teilweise äußeren Einflüssen – in erster Linie gewissermaßen der innen- und sicherheitspolitischen „Großwetterlage“ sowie technischen Einflüssen.
Waren in den ersten Befragungsjahren keine signifikanten Verschiebungen zwischen den Gruppen über die Zeit zu beobachten, so zeichnete sich danach ein dynamischeres Bild. Während sich 2012 mehr als die Hälfte der befragten Unternehmen noch vorrangig als Produkthersteller bezeichnete, waren es 2015 nicht einmal mehr 30 Prozent der Unternehmen, welche sich in erster Linie als solche sahen. Diese Entwicklung war nur zum Teil auf Veränderungen in der Befragungsgesamtheit zurückzuführen.
Insbesondere nahm der Angebotsmix mit maßgeblichem Bezug zu IT-Technik sowohl bei den Produkten als auch den Dienstleistungen stark zu, hier spielten also eine Ergänzung und auch qualitative Änderung bestehender Angebote durch die Digitalisierung eine Rolle. Diese Verflechtung muss Berücksichtigung finden, wenn man sich die Wachstumswerte der Teilbereiche ansieht. Nach 2015 und in engem Zusammenhang mit der Flüchtlingskrise allerdings ist der relative Anteil der non-IT-Dienstleistungsunternehmen an der Gesamtzahl der deutschen Sicherheitsunternehmen stark angestiegen. Wir beobachten hier mithin eine zeitlich begrenzte Trendumkehr, die in deutlichem Gegensatz zur Entwicklung im Produktbereich steht.

In den Jahren 2013 und 2014 zeigte ein genauerer Blick auf die Tätigkeitsfelder der Unternehmen, dass knapp die Hälfte klassische Sicherheitsprodukte und -techniken entwickelten, produzierten oder vermarkteten. Je rund ein Drittel war im Bereich der klassischen Sicherheitsdienstleistungen, der IT-Sicherheitsprodukte und IT-Sicherheitsdienstleistungen tätig. Eine durchaus große Zahl an Unternehmen war dabei auch in mehreren Bereichen aktiv – boten also beispielsweise sowohl Sicherheitsprodukte und -dienstleistungen an („Klassiker“) oder waren gleichermaßen in den Bereichen IT-Sicherheit und klassischer Sicherheitsangebote tätig (allrounder). Wie die Struktur der befragten Sicherheitsunternehmen zeigte, waren die Verknüpfung von Sicherheitsprodukten und -dienstleistungen bei Unternehmen, die ausschließlich im Bereich klassischer Sicherheitsprodukte und -techniken tätig sind, allerdings geringer ausgeprägt.

Unter den IT-Sicherheitsprodukten nimmt seit fünf Jahren Software wenig überraschend eine herausragende Rolle ein, u. a. Anti-Viren-Programme, firewalls, tracking- und Wiederherstellungsprogramme. Unter Zubehör fallen Server-Schränke, Schlösser für Computer sowie Systemlösungen für Hardware-Sicherheit. Verschlüsselung und Kryptographie umfassen die Herstellung und den Vertrieb von Software und Hardware und wurden ebenfalls von vielen der befragten Unternehmen als Geschäftsfeld genannt. Die IT-Technologie wird heute immer mehr ein Bestandteil von Anwendungen im klassischen Bereich der Sicherheitsprodukte und -dienstleistungen, die entsprechend von immer mehr Unternehmen angeboten wird. Die Bereiche Software, IT-Zubehör und Kryptographie nehmen ähnlich starke Positionen ein. IT-Sicherheit muss aufgrund ihrer zunehmenden Bedeutung als sektorübergreifende Transformationstechnologie aufgefasst werden.

Es gibt zahlreiche Beispiele für Sicherheitsprodukte mit integraler digitaler Informationstechnik. Bereits vor fünf Jahren zeichnete sich die zunehmende Bedeutung von Kontrollsystemen in der Sicherheitswirtschaft ab. Zutrittskontrollsysteme spielen hierbei eine Schlüsselrolle. Sie umfassen den Zugang zu Gebäuden und Geländen sowie die Verkehrsinfrastruktur und elektronische Ausweisesysteme sowie Schloss- und Schließanlagen, und wurden in den Befragungswellen häufig genannt. Mit einer geringeren Anzahl von Nennungen folgten Authentifizierungssysteme durch Biometrie und die Kategorie Vi-

deosysteme sowie Einbruchmelde- und Alarmanlagen, sodann Brand- und Explosionsschutzsysteme.

Letztere umfassen Produkte wie Rauchmelder, Feuerlöscher, Feuerschutztüren sowie Gaswarneinrichtungen. In der Kategorie mechanische Zutrittskontrolle sind Schlösser, Schließanlagen, Beschläge und Schranken vertreten, während Identifikationssysteme RFID und Funketiketten ebenfalls ein zahlenmäßig bedeutsames Feld bildeten. Weiterhin werden Leitzentralen und Lagezentren bereitgestellt, bisweilen auch vollständige Kommunikationssysteme. Nur für einzelne Unternehmen spielen bildgebende Verfahren (inklusive Röntgengeräten und Computertomographie), Aufgaben der Gefahrenstofferkennung im Bereich CBRN (also bezogen auf chemische, biologische, radioaktive und nukleare Gefahren) oder die entsprechende Aus- oder Umrüstung von Fahrzeugen und Schutzbekleidung für Polizei, Feuerwehr, Technisches Hilfswerk und andere Sicherheitsdienstleister eine größere Rolle.

Entsprechend der Umfrage-Ergebnisse bedeutsame IT-Sicherheitsdienstleistungen umfassen Datensicherung, Netzwerksicherheit, Betriebssystemsicherheit, Datenwiederherstellung sowie IT-Sicherheitsmanagementprogramme. Es folgt IT-Sicherheitsberatung, dies umfasst die Erstellung von Sicherheitsmodellen und -konzepten, Risikoanalysen sowie Sicherheitsschulungen. IT-Sicherheits-Audit beinhaltet die Überprüfung von bestehenden Sicherheitssystemen und -prozessen, während Digitale Forensik die Untersuchung von verdächtigen Vorfällen im Zusammenhang mit IT-Systemen, die Feststellung des Tatbestandes und der Täter durch Erfassung, Auswertung und Analyse digitaler Spuren beinhaltet. Unternehmen, die Zertifizierungen im Bereich IT-Sicherheit sowohl nach Standards der International Organization for Standardization (ISO) als auch anderen Normen anbieten, bilden die kleinste Kategorie in dieser Gruppe.

Ein genauerer Blick auf die Beschäftigungssituation nach Produktportfolio zeigt, dass mehr als ein Drittel der Mitarbeiter bei Sicherheitsprodukt- und Sicherheitstechnikunternehmen beschäftigt sind. Fast 30 Prozent der Beschäftigten waren vor 2014 Jahren nach unserer Hochrechnung im traditionellen Sicherheitsdienstleistungsbereich angestellt, 2015 und 2016 waren es deutlich mehr. 2017 näherte sich die Struktur wieder den vorherigen Relationen an. Die wenigsten Mitarbeiter waren mit einem Anteil von unter 20 Prozent im reinen IT-Sicherheitsbereich tätig. Die gesonderte Betrachtung der Beschäftigtenstruktur in der IT-Sicherheitsbranche zeigte, dass fast 60 Prozent der spezialisierten IT-Sicherheitsunternehmen maximal neun Mitarbeiter beschäftigen.

Umsatzentwicklung und Wachstum

Von den zahlenmäßigen Anteilen der Unternehmen an der Branche sowie von Belegschaftsgrößen gesondert zu betrachten sind Zahlen und Trends zur Umsatzentwicklung, die aussagekräftige Hinweise auf das Wachstum der Branche in den vergangenen und kommenden Jahren geben.

Auffällig war noch vor einigen Jahren, dass insbesondere die IT-Sicherheitsunternehmen – für das Jahr 2011 – das geringste Umsatzwachstum angaben. Mittelfristig gesehen erwarteten diese damals jedoch im Vergleich zu den anderen Branchen für die nächsten drei bis fünf Jahre für ihr eigenes Unternehmen ein Umsatzwachstum von 5,1 Prozent. Diese Kennzahl lag somit etwas höher als die durchschnittliche Einschätzung der eigenen Umsatzentwicklung aller Unternehmen, die für die kommenden 3 bis 5 Jahre auf ca. 4,7 Prozent geschätzt wurde. Insbesondere die IT-Sicherheitsunternehmen prognostizierten ein hohes Umsatzwachstum für die Sicherheitswirtschaft in Deutschland.

Darauf deutete auch der unterdurchschnittliche Umsatz je Mitarbeiter der 2012 befragten IT-Sicherheitsunternehmen hin. Die steigende Nachfrage nach IT-Sicherheitsprodukten zeigte damals, dass es hier – womöglich auch in Folge einer Sensibilisierung durch prominente Fälle von Cyberkriminalität –zu einer neuen Dynamik kam. 2013 zeigte dann eine separate Analyse der IT-Sicherheitswirtschaft, dass sich dieses Teilsegment der Sicherheitswirtschaft durch überdurchschnittlich hohe Wachstumskennzahlen auszeichnete. Die befragten Unternehmen der IT-Sicherheitswirtschaft rechneten mit einem Umsatzwachstum von durchschnittlich 6,3 Prozent, für die Folgejahre sogar von 6,9 Prozent.

Eine detailliertere Aufschlüsselung der Wachstumsentwicklungen in der IT-Sicherheitswirtschaft – im Vergleich zu den Erwartungen der traditionellen Sicherheitsunternehmen – ergab, dass der Umsatz im Jahr 2012 bei knapp 35 Prozent der IT-Unternehmen sogar um mindestens zehn Prozent gestiegen war. Selbst in einem vergleichsweise wachstumsschwachen Jahr lag der Anteil besonders wachstumsstarker Unternehmen in der IT-Wirtschaft damit deutlich über dem gesamtwirtschaftlichen Durchschnitt. Für die Folgejahre erwarteten stolze 38 Prozent der IT-Sicherheitsunternehmen ein Umsatzplus von mehr als 10 Prozent und in mittelfristiger Perspektive betrug der Anteil der Optimisten sogar 40 Prozent.

Im Hinblick auf die Umsatzentwicklung wurde 2014 bereits bei der ersten Auswertung deut-

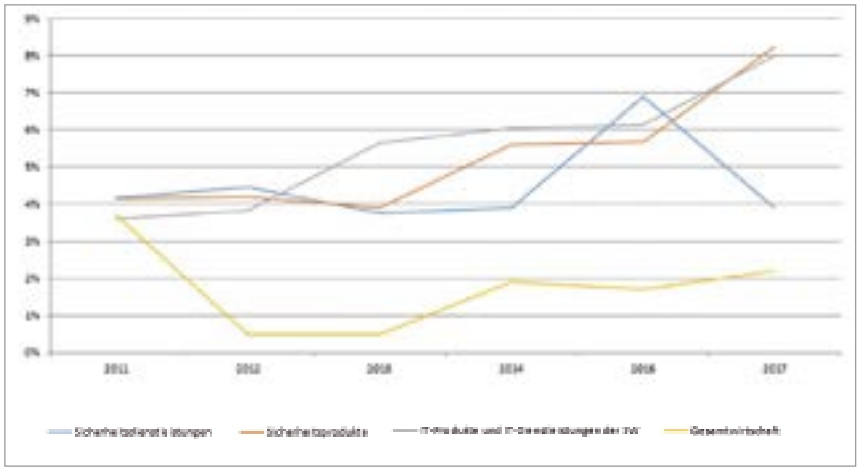

Abbildung 2: Angaben zu Wachstums-Entwicklung bis und -Erwartung für 2017, nach Angebotsportfolio, im Vergleich zur Gesamtwirtschaft

Wie aus der Zeitreihe ersichtlich ist, wächst der Umsatz der Sicherheitswirtschaft mit Bezug zu IT und Digitalisierung seit Jahren ungebrochen und deutlich stärker als das reale Bruttoinlandsprodukt. Der starke Anstieg im Bereich der Sicherheitsdienstleistungen ab 2015 ist ein Sondereffekt, der auf die Flüchtlingskrise zurückzuführen ist. Hier zeichnet sich bereits wieder eine deutliche Normalisierung ab. Ausreißer bei Angaben zu Wachstumserwartungen konservativ bei 10% gekappt. Quelle: BIGS 2011-2017, Statista 2018.

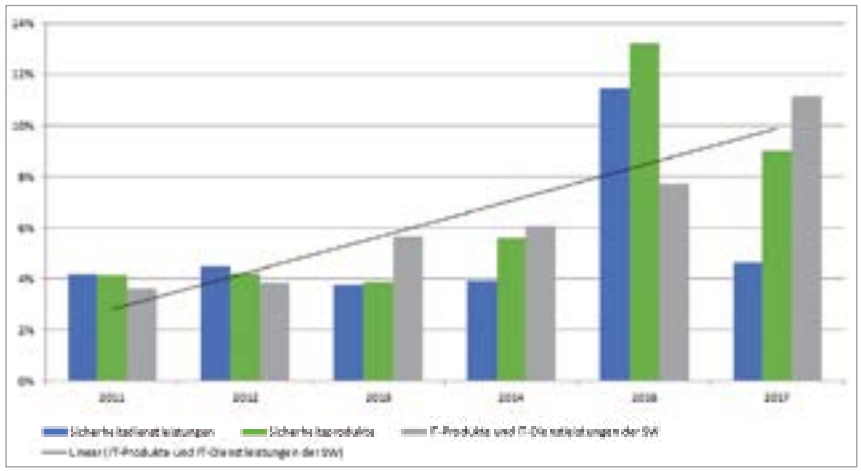

Abbildung 3: Wachstumstreiber Digitalisierung

IT-Produkte und –Dienstleistungen der Sicherheitswirtschaft erweisen sich seit 2011 als Wachstumstreiber. Besonders optimistische (pessimistische) Erwartungs-Angaben für das während der Befragung noch laufende Geschäftsjahr 2017 wurden im Gegensatz zur vorhergehenden Abbildung nicht bei 10% gekappt, sondern immer noch konservativ mit 16 (Antwort: „Über 15 %“) bzw. 26 („Über 25%) Prozent inkludiert. Quelle: Eigene Darstellung, Datengrundlage BIGS 2011-2017.

lich, dass die Unternehmen das Wachstum auf dem gesamten Sicherheitsmarkt in Deutschland für 2013 höher einstuften als das eigene Wachstum, sich selbst also als unterdurchschnittlich prosperierend empfanden. Bei der differenzierten Betrachtung nach den jeweiligen Produktportfolios bestätigte sich dieses Selbstbild.

Für das Jahr 2014 erwarteten IT-Sicherheitsunternehmen 2013 einen Wachstumsschub von 5,4 Prozent. Im Jahr 2014 erwarteten sie für den gleichen Zeitraum ein Wachstum von 5,9 Prozent. Das realisierte Umsatzwachstum lag nach den Befragungswerten von 2015 bei Unternehmen mit IT-Bezug bei 6,1 Prozent. Auch Unternehmen ohne IT-Bezug konnten wiederum mit hohem Wachstum aufwarten. Hier lag der durchschnittliche Umsatzanstieg 2014 bei 4,8 Prozent.
2014 waren insbesondere Unternehmen höherer Umsatzklassen – solcher von mehr als fünf Millionen Euro im Jahr - Hersteller von Sicherheitsprodukten und –techniken. Dieses Bild hatte auch 2017 noch Bestand, wenngleich sich hier je nach Verbandszugehörigkeit der Unternehmen auch eine „Verschiebung“ in den Dienstleistungsbereich ergab. Das Produktsortiment der Unternehmen wurde vor allem durch elektronische Zutrittskontrollsysteme, Videosysteme sowie Einbruchmelde- und Alarmanlagen dominiert. IT-Sicherheitsunternehmen waren die drittgrößte Portfoliogruppe in der 2014er-Marktstudie und setzten insgesamt ungefähr fünf Milliarden Euro um.
Die Umsatzstruktur der IT-Sicherheitsunternehmen zeigte 2014, dass fast die Hälfte dieser Unternehmen überwiegend kleinere Betriebe waren, da sie sich selbst in der ersten Umsatzkategorie (weniger als 250.000 Euro) verorteten. Reine IT-Sicherheitsunternehmen waren mehrheitlich als Kleinstunternehmen einzustufen und vor allem in der Sparte IT-Sicherheitsprodukte gab es viele „Zwerge“ und einige wenige „Riesen“ – aber nur wenige Unternehmen mittlerer Größe.

Mit der Befragungswelle 2015 wurden zugleich die Umsatzentwicklungen von 2014 im Vergleich zum Vorjahr erfragt. Aus vorherigen Analysen ging beispielsweise immer deutlich hervor, dass der Bereich der IT-Sicherheit nochmals dynamischer wuchs als die insgesamt schon recht wachstumsstarke Branche der Sicherheitswirtschaft. Die positiven Erwartun-

gen der Vorjahresbefragung haben sich weitestgehend als treffend erwiesen.

Das Umsatzwachstum von 2015 auf 2016 bewerteten die IT-Sicherheitsunternehmen dann unterschiedlich – von „unverändert“ bis „mehr als 15 Prozent gestiegen“ war alles ähnlich häufig vertreten, wohingegen niemand von schrumpfender Umsatzentwicklung berichtete. Im Bereich der Sicherheitsprodukte – inklusive elektronischer Produkte – wurden von einer Mehrheit der Probanden sogar mehr 25 Prozent Umsatzwachstum vermeldet. Für 2017 erwarteten die meisten teilnehmenden IT-Sicherheitsunternehmen ein Umsatzplus von 15 Prozent oder mehr, die meisten Hersteller von Produkten etwas moderater auf immer noch hohem Niveau bei 10 Prozent. Abbildung 2 zeigt, wie sich die Umsatzzuwächse der verschiedenen Zweige der Sicherheitswirtschaft in den vergangenen Jahren bei konservativer Interpretation der Daten durchschnittlich – also basierend auf den Angaben aller Umfrageteilnehmer –entwickelt haben.

Betrachtet man dezidiert IT-Sicherheitsunternehmen in jüngerer Vergangenheit, erkennt man, dass die Unternehmen höherer Umsatzklassen jetzt auch hier die Mehrheit bilden. Hier verläuft die Grenze je nach Verbandszugehörigkeit bei über einer bzw. häufiger ebenfalls bei mehr als fünf Millionen Euro Jahresumsatz. 2017 war das Bild deutlich gemischter als 2014, wobei die umsatzstärkste Gruppe (mehr als 25 Millionen Euro) sogar leicht überrepräsentiert war. Vorsichtig könnte man darauf schließen, dass die großen Firmen sich dem Thema IT-Sicherheit im Angebotsportfolio vermehrt zuwenden.

Die Trendentwicklung im Bereich des Wachstums der IT-Produkte und Sicherheitsdienstleistungen wird in Abbildung 3 durch eine Gerade noch etwas deutlicher dargestellt. Im Gegensatz zur vorhergehenden Abbildungen wurde hier zudem ein etwas weniger vorsichtiger Ansatz gewählt: Auch besonders optimistische und pessimistische Angaben von mehr (weniger) als 15 bzw. 25 Prozent Wachstum fanden Eingang in die Berechnungen. Hier kristallisiert sich ein noch deutlicheres Bild der Digitalisierung als Wachstumstreiber heraus.

Insgesamt ist es um die Entwicklung der Sicherheitsbranche und ihr Gesamtwachstum – sowie das in allen Teilbereichen – gut bestellt: Eine genauere Aufschlüsselung der Wachstumszahlen von Anbietern von IT- und non-IT-Produkten und -Dienstleistungen sowie ihre Beobachtung über die letzten Jahre zeigt, dass beide Bereiche an sich höhere Wachstumszahlen als die Gesamtwirtschaft generieren. Die Sicherheitswirtschaft insgesamt stellte sich nach mittlerweile fünf Beobachtungsjahren – also nach Abschluss der jüngsten Durchgangs der bisherigen Befragungen der Sicherheitswirtschaft durch das BIGS Ende des Jahres 2017 – als ein überdurchschnittlich wachsender und personalintensiver Bereich heraus.
Das Wachstum der IT-Sicherheitswirtschaft ist seit Jahren ungebrochen besonders ausgeprägt. Digitalisierung (auch im Produktbereich) und IT-Sicherheit haben sich – abseits von Sondereffekten ab 2015 – als Wachstumstreiber der Branche erwiesen. Die hohen Wachstumsraten der IT-Sicherheitswirtschaft sind auch Ausdruck einer nachholenden Entwicklung. Wie die Erhebung noch 2012 gezeigt hatte, wurde die IT-Sicherheitswirtschaft in Deutschland bis dahin überwiegend von Kleinst- und Kleinunternehmen dominiert, die vornehmlich im Bereich der Dienstleistungen oder des Vertriebs von IT-Sicherheitsprodukten tätig waren.

Ausgehend von der Annahme, dass die Kleinstunternehmen – mit Ausnahme womöglich weniger Start-ups – überwiegend sich keine eigene Forschung und Produktentwicklung leisten können, deutete das Bild noch 2014 darauf hin, dass sich mit Ausnahme einiger etablierter Großunternehmen in Deutschland bisher keine größere Zahl innovativer und wettbewerbsfähiger IT-Sicherheitsunternehmen etablieren konnte. Eine entwickelte, vielfältige IT-Sicherheitswirtschaft mit umfassenden Entwicklungs- und Produktionskapazitäten existierte – anders als im Bereich zum Beispiel herkömmlicher Sicherheitsprodukte – offenbar bislang erst in Teilen. „Luft nach oben“, Entwicklungs- und Wachstumspotenzial war deutlich erkennbar. Dieses Potenzial scheint seitdem vermehrt umgesetzt zu werden.

Ob allerdings diese Entwicklung tatsächlich dazu führt, dass sich Deutschland zu einem global wettbewerbsfähigen Standort für IT-Sicherheit entwickelt, um beispielsweise auch die strategischen Erfordernisse der Bundeswehr und das Ziel der digitalen Agenda zur Stärkung der „technischen Souveränität“ Deutschlands zu erreichen, ist derzeit noch offen. In Anbetracht der anhaltenden Dynamik ist eine solche Entwicklung jedoch vorstellbar und lohnt die weitere und vertiefte Beobachtung und Analyse.
Insbesondere jener Teil der Sicherheitswirtschaft, der sich mit IT-Sicherheitsprodukten und IT-Dienstleistungen beschäftigt, zeigt seit Jahren einen dynamischen Wachstumsprozess, den es bestmöglich für die deutsche Volkswirtschaft zu nutzen gilt. Das allgemeine Wirtschaftswachstum und die Beschäftigung können von der Dynamik der Sicherheitswirtschaft profitieren.

Trends

Bereits 2013 stellten technologische Faktoren die bei weitem am häufigsten genannten Trends. Daten- und IT-Sicherheit bildete hierbei das größte cluster und umfasst Angaben über den generellen Anstieg von IT-Sicherheitsanforderungen, Datenschutzanforderungen sowie Daten- und Netzwerksicherung als wichtige Wachstumstreiber. Insgesamt 44 Prozent der Antworten im diesem Feld bezeichneten IT-Sicherheit generell als einen wichtigen Trend, während 36 Prozent Datenschutz und 20 Prozent Daten- und Netzwerksicherung als wichtige Zukunftsthemen sahen.

Die nächstwichtigste Gruppe bildeten sogenannte Sicherheitssysteme, als wichtige Wachstumsfelder der Zukunft wurden damit von den befragten Unternehmern elektronische Überwachungssysteme, Zutrittskontrollen und Systemlösungen für Kritische Infrastrukturen bezeichnet. In dieser Gruppe sah eine große Mehrheit – 69 Prozent aller Antworten – Überwachungssysteme als einen bedeutenden Trend an, 22 Prozent erachteten elektronische Zutrittskontrollen und neun Prozent der Antworten Systemlösungen für Kritische Infrastrukturen als wichtig für die Zukunft.

Mit nur geringem Abstand folgte das Thema Technologisierung und Vernetzung - darunter fällt u. a. die Digitalisierung von Lebensbereichen mit Sicherheitsbezug. Hier wurde bereits damals angenommen, dass elektronische Datenverarbeitungssysteme (EDV) und Informations- und Kommunikationssysteme (IuK) Geschäftsprozesse und Gesellschaftsbeziehungen noch vermehrt durchdringen würden, so dass daraus neue Verwundbarkeiten und erhöhte Sicherheitsanforderungen entstünden. Dies sahen die Probanden sowohl für Behörden, Unternehmen wie auch Privathaushalte.

Bei den Trends registrieren viele Sicherheitsunternehmen, dass technologische Themen wie IT-Sicherheit, elektronische Sicherheitssysteme und Sicherheitslösungen aufgrund der zunehmenden Technologisierung in allen Lebensbereichen die Märkte in Zukunft prägen werden. Folgerichtig werden Datenschutz und Datensicherung sowie der Schutz von geistigen Eigentumsrechten (intellectual property, IP) zunehmend wichtig.

Innerhalb der erhobenen Trends ließ sich insgesamt feststellen, dass der IT-Sicherheit mit Abstand die größte Aufmerksamkeit beigemessen wurde. Auf Trends der IT-Sicherheit entfiel, bei insgesamt fünf möglichen Antwortoptionen, 545 Mal die Wertung „besonders wichtig“ bzw. „wichtig“.

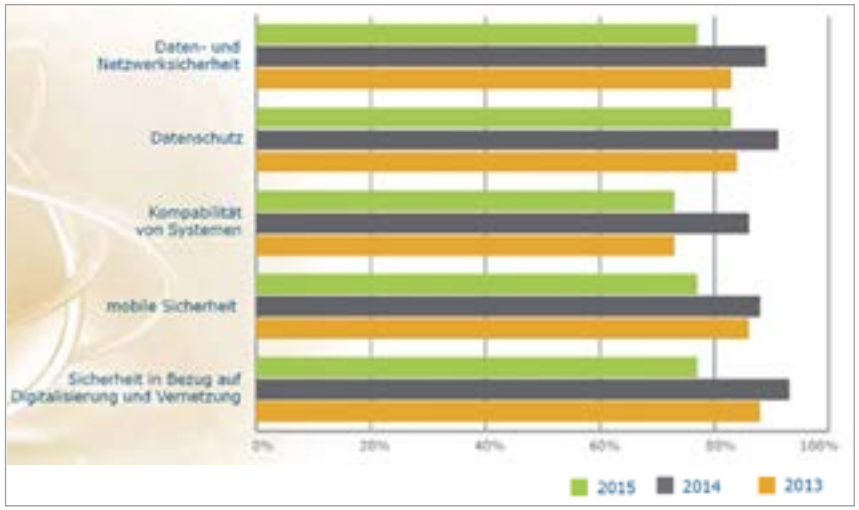

Abbildung 4: Trends in der IT – wichtigste Themen 2013 – 2015

Das Thema Datenschutz gewann bereits im Jahre 2014 an Bedeutung, und gehörte zu den am häufigsten genannten wichtigen Zukunftsthemen Spätestens seit Ablauf der zweijährigen Übergangsfrist und dem ausnahmslosen Inkrafttreten der Europäischen Datenschutz-Grundverordnung am 25. Mai 2018 sollte sich auch in Unternehmen der Sicherheitswirtschaft die Geschäftsführungsebene damit befassen, um Risiken zu begrenzen. Quelle: Gruchmann, Stuchtey (2016) Die Sicherheitswirtschaft in Deutschland 2015 - Auswirkungen der Digitalisierung und der Flüchtlingskrise auf die Sicherheitswirtschaft. BIGS Essenz, S. 7.

Nicht nur die Entwicklungen in der Flüchtlingspolitik in den vergangenen drei Jahren haben ihre Spuren hinterlassen, sondern vor allem auch die Digitalisierung der Gesellschaft. Auch 2015 zeigte sich die besondere Rolle der Digitalisierung, jetzt auch im Zusammenhang mit Industrie 4.0: Bei der Frage nach den treibenden Trends der Branche zeigt sich, dass all jene Trend, die im Zusammenhang mit Digitalisierung und IT-Sicherheit stehen, deutlich häufiger genannt wurden als „analoge“ Trends.

Im Folgenden benannte Punkte wurden bereits in den letzten Jahren innerhalb der Sicherheitswirtschaft als wichtige Nachfrage- und Wachstumsfaktoren für die Zukunft angesehen. Insbesondere der Themenbereich IT-Sicherheit fand in der Befragung außerordentliche Beachtung. Abbildung 4 zeigt eine detaillierte Auflistung innerhalb des gesamten Beurteilungsspielraums.

Kein Urteil zu den einzelnen Bereichen trauten sich im Schnitt zehn Prozent der befragten Unternehmen zu. Die Daten- und Netzwerksicherung innerhalb dieses Bereichs wurde von fast 60 Prozent der Unternehmen als besonders wichtig eingestuft. Weitere 30 Prozent hielten die Entwicklung in diesem Bereich für wichtig. Auch die Themen Digitalisierung und Vernetzung, Datenschutzanforderun-

gen und Mobilität wurden als wichtige Zukunftstrends bewertet. Es lassen sich in diesem Bereich besonders wichtige Wachstumstreiber vermuten. Lediglich die Kompatibilität von Systemen sahen nur knapp 30 Prozent der Unternehmen als besonders wichtig an. Allerdings schätzten weitere 44 Prozent die Kompatibilität als ein wichtiges Thema ein; und dieser Trend wurde somit immer noch als bedeutsamer eingeschätzt als beispielsweise die Trendentwicklung im Bereich der Sicherheitsdienstleistungen. Der Bereich der offenen Beantwortung lieferte folgende Begriffe wiederholt: business continuity management (BCM), Verschlüsselung, Weiterbildung und mobiler Hochwasserschutz.

Den Trends im Bereich der Sicherheitsprodukte wurde 2013 erkennbar weniger Bedeutung beigemessen, die Antworthäufigkeiten ging hier im Vergleich zu den Erhebungen der Vorjahre deutlich zurück. Hier wurden vor allem Integrierte Systeme als Trendprodukte der Sicherheit als besonders wichtig eingeschätzt. Auch elektronische Überwachungssysteme, Zutrittskontrollen und Systemlösungen für Kritische Infrastrukturen wurden als weitere Wachstumspotentiale gesehen, jedoch als weniger ausgeprägt betrachtet. Auffällig war, dass in dem Bereich der Sicherheitsprodukte durchgängig die Priorität „wichtig“ gegenüber der Einstufung „besonders wichtig“ favorisiert wird. Der Rückschluss einer bereits damals grundsätzlich geringeren Bedeutung von Sicherheitsprodukten außerhalb des IT-Bereichs für zukünftige Marktchancen liegt hier nahe. Individuelle Nennungen von Trends bei den Sicherheitsprodukten waren zusätzlich: Abhörsicherheit, Analysewerkzeuge, Besuchermanagement, Brandschutz, Kryptologie, sichere elektronische Identitäten, privater Bereich, Zutrittssteuerungssysteme, Brandmeldeanlagen (BMA) und Sprachalarmanlagen (SAA). Zum Teil lassen sich die genannten Produkte hier auch dem IT-Bereich zuordnen.

Konsistent zeichnet sich dieses Bild auch in den Folgejahren in den Befragungsergebnissen ab. Insgesamt dominieren bei den – als „besonders wichtig“ und „wichtig“ bzw. als „besonders wahrscheinlich“ und „wahrscheinlich“ – gesehenen Trends und Herausforderungen IT-nahe Bereiche. Nicht nur die Analysen zum Wachstum der Sicherheitswirtschaft zeigten auch 2015 die besondere Rolle der IT-Sicherheitswirtschaft. Schaut man auf die Perspektiven und wahrgenommenen Herausforderungen der Branche, bestätigte sich dies, wenn man auf die Umfrageergebnisse zu den qualitativen Trends schaute.

In der jüngsten Befragungswelle wurden als Trends im Bereich der IT-Sicherheitsdienstleistungen unter anderem Bedrohungs- und Risikoanalysen, der Betrieb von security operations centers, Beratung im Bereich der Schatten-IT, Kosten-Nutzen-Analysen von Sicherheitsinvestitionen, und Künstliche Intelligenz (KI) genannt. Der gerade nach zweijähriger Übergangsfrist in Kraft getretene Europäischen Datenschutzgrundverordnung wird ebenfalls ein bedeutender Einfluss zugetraut.

Im Bereich der IT-Sicherheitsprodukte wurden advanced persitent threats (APTs) ebenso genannt wie Kryptographie im anbrechenden Zeitalter der Quantencomputer, Zertifizierung, Cloud-Produkte, KI, kostengünstigere Lösungen für kleinere und mittlere Unternehmen, hardware security-Module sowie Bedrohungsanalyse-Systeme.
Aber auch im Bereich klassischer Sicherheitsprodukte und Sicherheitsdienstleistungen wurden Trends mit Bezügen zur Digitalisierung genannt. Neben KI und big data-Analyse wurden hier beispielsweise Alarmaufschaltungen, Brandmeldesysteme und E-Zylinder von Schließsystemen als Beispiele künftig relevanter werdender Bereiche geäußert.

Ein weiterer Trend ist die zunehmende Diversifizierung im Produktportfolio der Sicherheitsunternehmen. Hierbei steigt nicht nur die Verflechtung klassischer Anbieter von Sicherheitsprodukten und klassischer Anbieter von Sicherheitsdienstleistungen. Auch die Zahl der reinen IT-Unternehmen und die Zahl der allrounder, die Produkte und Dienstleistungen im Rahmen der IT-Sicherheit anbieten, wächst von Jahr zu Jahr. Letztlich werden also verstärkt Sicherheitslösungen angeboten, die aus einer Kombination aus Ingenieursleistung, digitaler Informationsverarbeitung und Humankapital bestehen.

Sowohl das hierfür benötigte höher qualifizierte Personal als auch die Internationalisierung dürften ursächlich dafür sein, dass zunehmend Fachkräftemangel von den befragten Unternehmen als eine Herausforderung genannt wird. Die Einführung des Mindestlohns Anfang dieses Jahres kann an dieser Stelle ein zusätzlicher Treiber in Richtung besser qualifizierter Mitarbeiter sein. Da die Sicherheitswirtschaft – sowohl bei kleineren und mittelgroßen Unternehmen als auch bei Großunternehmen – sich bislang als eine relativ personalintensive Branche darstellt, kann dieser Personalmangel ein Hemmnis für das weitere Wachstum der Branche darstellen.

Die rasante Entwicklung im Bereich der IT-Sicherheitswirtschaft ist nur eine der Ursachen für einen permanenten Bedarf an gut ausgebildeten Fachkräften. Fachkräftemängel besteht allerdings auch darüber hinaus, wie die jährliche Befragung der Sicherheitswirtschaft bereits 2012 bis 2014 zeigte. Innerhalb der gesamten Sicher-

heitswirtschaft gaben bereits 2013 65 Prozent der Unternehmen an, es bestünden Schwierigkeiten geeignetes Personal zu finden. Hierunter fallen auch sehr viele Kleinstunternehmen, die nicht auf einen großen Personalpool zur Deckung von Engpässen zurück greifen können und damit schnell in eine Existenz bedrohende Lage geraten können, sollte die Humankapitalqualifikation mittel- und langfristig hinter der Nachfrage nach gut ausgebildeten Arbeitskräften liegen.

Dass dies auf mittlere Frist gesehen bereits der Fall ist, legen die konstant hohen Zahlen über die Erhebungswellen hinweg nahe. Bereits im Jahr 2012 bemängelten 64 Prozent der Unternehmen, dass sie Probleme hätten, geeignetes Personal zu finden. Die reinen IT-Sicherheitsunternehmen sind hier erstaunlicherweise weniger stark betroffen. Von den klassischen Anbietern von Sicherheitsprodukten und -dienstleistungen gaben dagegen 72 Prozent an, bei der Besetzung ihrer Stellen mit geeignetem Personal Problemen gegenüber zu stehen. Ursachen für diese überproportional starke Betroffenheit bei non-IT-Sicherheitsunternehmen sind im Fachkräftemangel der Ingenieursberufe oder aber in gehobenen Ansprüchen der in der Branche bislang üblichen Berufsbildern zu vermuten, beispielsweise ist eine starke Internationalisierung bei den Absatzmärkten und Exportzahlen aller Sicherheitsunternehmen zu beobachten.
Bezüglich der Absatzmärkte ließ sich für IT-Sicherheitsunternehmen bereits 2014 erkennen, dass der Exportmarkt eine ausgesprochen bedeutende Rolle spielte. Etwa 25 der in der Befragung der Sicherheitswirtschaft erfassten exportorientierten Unternehmen waren IT-Sicherheitsunternehmen. Diese Entwicklung fügt sich ins Bild einer Marktraumvergrößerung über die letzten Jahre. Ausschließlich regional waren 2014 entsprechend weniger Unternehmen aktiv als noch im Jahr 2012. Während in 2012 noch regional tätige Unternehmen den Markt dominierten, war im Jahr 2014 der nationale Absatzmarkt die am häufigsten angegebene Absatzregion. Im Jahr 2017 zeigte sich die Fortsetzung des Trends – etwa zwei Drittel der befragten Unternehmen gaben eine überregionale Marktorientierung an.

Bei den Produktherstellern wie auch bei den IT-Dienstleistern stand der internationale Absatzmarkt im Vordergrund – wenig überraschend im deutlichen Gegensatz zu Anbietern klassischer Dienstleistungen, die laut Befragungsergebnis meist einen regionalen, zumindest aber allenfalls nationalen Absatzmarkt im Blick haben. Die Tendenz der Marktraumvergrößerung erscheint gleichläufig zur steigenden Diversifizierung von Produkt- und Dienstleistungsanbietern, insbesondere in dem Bereich, in denen IT-Sicherheitsprodukte und –dienstleistungen eine Rolle spielen.

Allrounder, die sowohl im IT- als auch im non-IT-Bereich Sicherheitsprodukte und Dienstleistungen anbieten, sind oft international tätig. Klassische Sicherheitsunternehmen hingegen bieten zumeist regionale Güter und Dienstleistungen an. Die reinen IT-Sicherheitsunternehmen haben dagegen am häufigsten einen nationalen Vertriebsfokus.

Schlussbetrachtungen

Bereits im Jahr 2012 konnte das BIGS eine relativ zu anderen Wirtschaftsbereichen hohe Umsatz- und Beschäftigungszahl für die Branche ermitteln, und insgesamt eine unerwartet hohe Bedeutung für Volkswirtschaft und Gesellschaft ermitteln. In den folgenden zweieinhalb Jahren stieg der Umsatz kontinuierlich an. Umsatztreiber der Sicherheitswirtschaft war in den letzten Jahren bis zur Flüchtlingskrise insbesondere die IT-Sicherheitswirtschaft, während die Sicherheitsdienstleistungen gerade im Wach- und Schutzgewerbe kaum stärker wuchsen als die Gesamtwirtschaft. (Einen besonders niedrigen Umsatz je Mitarbeiter hatten dabei vor allem viele der Kleinst- und Kleinunternehmen – auch im Bereich der IT-Sicherheit – sowie die zumeist kleinen Mischunternehmen.)
Die Wachstumsentwicklung des Wach- und Schutzgewerbes hat sich im Jahr 2015 deutlich geändert. Die Gründe hierfür sind offensichtlich: Mit der Flüchtlingskrise war der Bedarf an Sicherheitspersonal sprunghaft angestiegen. 2017 lässt sich jedoch bereits wieder ein Normalisierungseffekt beobachten, der sich auch mit den Erwartungen der weit überwiegenden Mehrheit der Unternehmer der Branche für 2018 deckt.

Die oben beschriebene Trendumkehr im Zusammenhang mit der Flüchtlingskrise – ein steiler Anstieg des relativen Anteils der non-IT-Dienstleistungsunternehmen an der Gesamtzahl der deutschen Sicherheitsunternehmen – ist aller Voraussicht nach zeitlich begrenzt. Sowohl der relative Anteil der im Produktbereich als auch im IT-bezogenen Bereich tätigen Sicherheitsunternehmen überholt nach unseren Umfrage-Ergebnissen die klassischen Dienstleister bereits wieder.
Besonders ausgeprägt war die private und öffentliche Nachfrage nach Sicherheitsprodukten und -dienstleistungen in den letzten Jahren vor Beginn der Flücht-

lingskrise im Bereich der digitalen Sicherheit. Damit setzte sich das auch im Vergleich zur übrigen Branche weit überdurchschnittliche Wachstum dieses Sektors verstärkt fort. Bereits ab dem Jahr 2014 war eine verstärkte Dynamik zu beobachten, mutmaßlich auch in Folge des „Snowden-Effekts“: Unter dem Eindruck der Enthüllungen über die Fähigkeiten und Aktivitäten der National Security Agency (NSA) im Bereich signal intelligence und Überwachung des Internet-Datenverkehrs ab Mai 2013, sowie von Presseberichten zu Aktivitäten weiterer Auslandsnachrichtendienste und prominenter Fälle von Datendiebstahl und anderer Fälle von Cyberkriminalität gaben im Jahr 2014 48 Prozent der befragten Unternehmen an, dass IT-Sicherheit zu einem entscheidenden Meta-Trend der Sicherheitswirtschaft geworden war. Im Vorjahr waren hingegen lediglich 16 Prozent dieser Auffassung.

Aus heutiger Sicht wäre es allerdings viel zu kurz gegriffen, die wachsende Bedeutung des Bereichs der digitalen Sicherheit als alleinige Folge der NSA-Affäre zu verstehen. Auch die zu verzeichnenden Zunahme und Professionalisierung von Cyberkriminalität mit arbeitsteiligem und spezialisierten Vorgehen sowie Angriffen mit baukastenartig zusammengestellter Schadsoftware tragen ihren Teil bei. Neu ist auch die Breite des „Beuteschemas“. Mit „Geschäftsmodellen“ wie der Erpressung mit verschlüsselnden Trojanern – man denke beispielsweise an die ransomware „Locky“ – werden heute auch Krankenhäuser, kommunale Behörden, kleine Unternehmen und sogar Privatpersonen angegriffen. Andere Nachrichtendienste oder ihre privatwirtschaftlichen Helfer versuchen Einfluss auf den Ausgang von Parlaments- und Präsidentschaftswahlen über die maßgeschneiderte Verbreitung von Falschmeldungen und den Einsatz von bots und sog. Trollfabriken in sozialen Netzwerken zu nehmen. Die gesellschaftliche Diskussion hierüber hat auch die Entscheider in Unternehmen dafür sensibilisiert, dass vergleichbare Kampagnen auch gegen ihr Unternehmen geführt werden können. Die erhöhte Sensibilität führt letztlich auch zur Suche nach möglichen Lösungen auf dem Markt der Sicherheitswirtschaft.

Nicht nur das Tatmittel Internet als Werkzeug von kriminellen, organisierten Verbrechen, Terroristen und Industriespionen hat an Bedeutung gewonnen. Auch ist der Angriffsvektor exponentiell am wachsen. Die fortschreitende Vernetzung im Zeitalter der Digitalisierung (Stichwort Industrie 4.0) aber auch beispielsweise die rasante Verbreitung von Sensoren (proliferation of sensors), das Aufkommen des Internet of Things mit einer zunehmenden Vernetzung von Alltagsgegenständen, der Verbraucherwunsch nach Smart Homes und die sich andeutende Marktreife autonomer Fahrzeuge stellen unsere Gesellschaft und damit auch die Sicherheitswirtschaft vor neue Herausforderungen.

Das bestätigen auch die Aussagen der Unternehmen der Sicherheitswirtschaft, die hier für sich selbst eine der wesentlichen Herausforderungen der Zukunft sehen. Der Anteil der Unternehmen, die ihr Geschäftsfeld um Aufgaben im Bereich der IT-Sicherheit verbreitern, nimmt gegenwärtig deutlich zu. Und gleichzeitig führt diese Entwicklung – in Verbindung mit einem nach Einschätzung der Unternehmen offenbar schärfer werdenden Wettbewerb – offenbar derzeit in vielen Unternehmen zu vermehrten Anstrengungen in Forschung und Entwicklung. Dies gilt auch im Bereich der „klassischen“ Sicherheitsprodukte und -techniken, die z.B. durch die Vernetzung von Überwachungssystemen oder intelligente Videoanalyse und maschinelles Lernen in ihrer Arbeit neue Möglichkeiten erhalten, aber gleichzeitig auch vor neue Herausforderungen gestellt werden. Dies gilt aber auch für Sicherheitsdienstleistungen die durch eine intelligente Analyse großer Datenmengen zusätzliche Werte für ihre Kunden schaffen können.

Diese verstärkte Rolle von Forschung und Entwicklung zeigt einen Wandel: Die Sicherheitswirtschaft in Deutschland ist – seit ihren Anfängen – von intensivem Personalbedarf und traditionsreichen Praktiken geprägt, in denen Forschung und Entwicklung (F&E) eine geringe Bedeutung besaß. Auf der anderen Seite wächst der in den letzten Jahren hinzugekommene Bereich der IT-Sicherheit sehr stark und lässt sowohl im Produkt- als auch im Dienstleistungsspektrum eine F&E-unterstützte Dynamik vermuten. Die Befragungsergebnisse zeigten schon im Jahr 2013, dass in diesem Sektor rund 32 Prozent aller Unternehmen F&E betreiben. Im Jahr 2017 betrieb die Mehrzahl der sich an der Umfrage beteiligenden Hersteller von Sicherheitsprodukten wie auch die Mehrheit der IT-Dienstleister nach eigener Auskunft F&E, wohingegen dies nur bei einem kleinen Teil der Anbieter klassischer Dienstleistungen der Fall war – und sich auch bei diesen vermutlich mehrheitlich auf andere, nebenher verfolgte Geschäftszweige bezog.

Insgesamt zeigt sich, dass die Unterscheidung zwischen Sicherheitsdienstleistern, IT Sicherheit und Anbietern von Sicherheitstechnologie immer schwieriger wird und die Grenzen verschwimmen. Die gesamte Sicherheitswirtschaft steht vor Herausforderungen bei der Rekrutierung von geeignetem Personal. Die demographische Entwicklung und der schon über mehrere Jahre andauernde konjunkturelle Aufschwung haben das relative Angebot an geeignetem Personal in allen Qualifikationsstufen reduziert. An der demo-

graphischen Entwicklung wird sich in absehbarer Zeit nichts ändern. Sollte sich auch das Wirtschaftswachstum weiter fortsetzen, ist im Sicherheitsgewerbe mit einem Anstieg der Arbeitskosten zu rechnen. Dies wird den Trend zu einem Einsatz von mehr Technik und Digitalisierung weiter verstärken.

Das gestiegene Bedürfnis der Bevölkerung nach einem höheren Sicherheitsniveau führt dazu, dass vom Staat mehr Stellen für die Polizei geschaffen werden. Auch die Polizeien haben Schwierigkeiten, geeignete Bewerber für diese neuen Stellen zu finden. Folgerichtig wird der Einsatz der Polizei bei jenen Schutzleistungen priorisiert, die von der Politik als besonders essenziell angesehen werden. In anderen Bereichen wird mehr als in der Vergangenheit der Einsatz auch von privaten Sicherheitsanbietern in Erwägung gezogen.

Während in der Vergangenheit vermeintliche Kostenersparnisse insbesondere im Bereich des Personals ein wesentlicher Grund für die von Schutzleistungen an private Anbieter waren, ist heute die Verfügbarkeit ein wichtiger Wettbewerbsfaktor. Gerade in jenen Bereichen, in denen besonders gefragte Qualifikationen des Personals erforderlich sind, ist häufig das starre Tarifgefüge des öffentlichen Dienstes ein Hindernis. Geeignete und zu rekrutierende Personen können von der Privatwirtschaft oft ein besseres Angebot erwarten als von der öffentlichen Hand. Um sich die Arbeitsleistung solcher Personen zu sichern, hilft dem Staat dann letztlich nur die Vergabe von Aufträgen an private Dienstleister oder Berater. Nur diese sind rechtlich in der Lage, den Talenten ein marktadäquates Gehalt zu zahlen.

Die hier beschriebenen Trends und Effekte werden dazu führen, dass sich das Angebot bei den Sicherheitsdienstleistungen in zwei Gruppen teilen wird. Die einen konkurrieren über den Preis und versuchen möglichst billig niedrigqualifiziertes Personal für einfache Dienstleistungsaufgaben anzubieten. Die anderen schaffen aus einem intelligenten Mix von Humankapital, Datenanalyse und dem Einsatz neuester technischer Möglichkeiten ein Dienstleistungsangebot, das sich über den Mehrwert an Sicherheit und nicht über den Preis verkauft.

Impressum

Autoren:

Philip A. Caspari und **Stephan Grinat**, W.I.S. Sicherheit + Service GmbH & Co. KG
Matthias Clausmeyer, W.I.S. Sicherheit + Service GmbH & Co. KG
Marian Meier-Andrae, MULTIROTOR GmbH
Dr. Frank Nikolaus, Nikolaus & Co. LLP
Dr. Tim Stuchtey und **Dr. Johannes Rieckmann**,
Brandenburgisches Institut für Gesellschaft und Sicherheit BIGS
Volker Wagner, ASW Bundesverband Allianz für Sicherheit in der Wirtschaft e.V.
Jan Wolter, ASW Bundesverband Allianz für Sicherheit in der Wirtschaft e.V.
Dirk Zundel, streamBASE GmbH

Bestellnummer:

ISBN 978-3-947973-00-2

Bezugs- und Verlagsanschrift:

TCC Verlagsgesellschaft
c/o W.I.S. Training + Service GmbH

Industriestraße 171
50999 Köln

E-Mail: kompendium@wis-sicherheit.de

Projektidee und -realisierung:

Oliver Arning
Suum Cuique - Medienberatung & Moderation

Kronprinzenstraße 38/40
44135 Dortmund

E-Mail: info@suum-cuique.org

Layout und Satz:

DITO
digitale Dienstleistungs-GmbH

Hängebank 3
45307 Essen

E-Mail: dito@ditogmbh.de

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