N° 2 | 2023

SPOC

Wirtschaft und Wissenschaft schützen

Wettlauf um Zukunft

Spionage in Wirtschaft und Forschung

Sicherheit versus Freiheit?
Forschungsfreiheit in Gefahr

Die Macht der Normen
Chinas Normierungsstrategie

Bundesamt für Verfassungsschutz

Liebe Leserinnen, Liebe Leser,

über drei Jahrzehnte profitierte die deutsche Wirtschaft von dem Zugang zu Märkten, Mächten und Menschen. Doch seit geraumer Zeit sind ökonomische Entflechtungstendenzen, ein verstärkter technologischer Merkantilismus sowie die Renaissance der Geopolitik unübersehbar. Eine Situation, in der sich der Handlungsspielraum für Unternehmen, die zwischen den Konfliktlinien rivalisierender Staaten agieren müssen, zunehmend fragmentiert. Geopolitik, Technologie und Sicherheit sind dabei strategische Herausforderungen, die über erfolgreiche Geschäftsmodelle und Reputation mitentscheiden.

Die vorliegende Ausgabe des SPOC-Magazins widmet sich den drängenden Themen dieser Gemengelage aus dem professionellen Blickwinkel unserer Cyber- und Spionageabwehr: Wir informieren Sie über aktuelle Risiken für die deutsche Wirtschaft und Wissenschaft, die mehr denn je im Aufklärungsspektrum fremder Mächte und ihrer Geheimdienste liegen und unterstützen Sie mit konkreten Maßnahmen bei Ihrer persönlichen Gefahreneinschätzung und effektiven Prävention.

Ihr Single Point of Contact beim BfV ist der Bereich Prävention/Wirtschaftsschutz. Auch die Landesbehörden für Verfassungsschutz stehen Ihnen als vertrauliche Anlaufstellen zur Verfügung. Unsere gemeinsame Expertise kann Ihnen im Wettlauf um Zukunft den entscheidenden Vorsprung verschaffen.

Ich wünsche Ihnen eine spannende Lektüre.

Thomas Haldenwang
Präsident Bundesamt für Verfassungsschutz (BfV)

Single Point of Contact –
SPOC

Dieses Heft wird vom Bereich Prävention in Wirtschaft, Wissenschaft, Politik und Verwaltung des Bundesamtes für Verfassungsschutz (BfV) herausgegeben.

Der Bereich, der mit Standorten in Köln und Berlin vertreten ist, bereitet die Erkenntnisse und Analysen des Hauses bedarfsgerecht für seine Zielgruppen auf und trägt so dazu bei, dass sich diese eigenverantwortlich und effektiv gegen gewaltbereiten Extremismus, Terrorismus, Spionage und Sabotage durch fremde Mächte schützen können.

Zudem ist er als Single Point of Contact jederzeit bei konkreten Verdachtsfällen und Sicherheitsanfragen für Unternehmen, Wissenschafts- und Forschungseinrichtungen sowie Politik und Verwaltung ansprechbar:

wirtschaftsschutz@bfv.bund.de
030 18792-3322

Impressum:

Herausgeber
Bundesamt für Verfassungsschutz
Merianstraße 100, 50765 Köln

Redaktionsleitung
Philip Kornberger

Art Direktion und Gestaltung
Sonnenstaub, Berlin | sonnenstaub.com

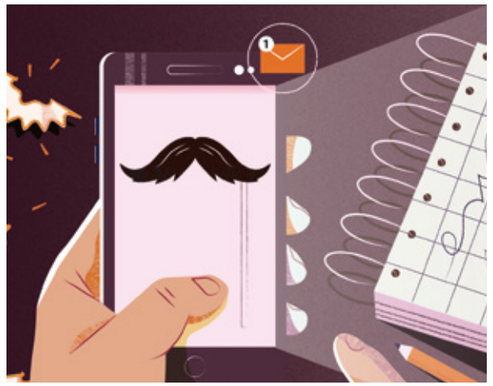
Redaktionelle Mitarbeit und Korrektorat
Agentur Sheila, Berlin | agentur-sheila.com

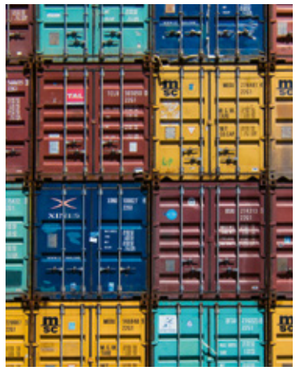
Herstellung
Spreedruck

MIX
Papier aus verantwortungsvollen Quellen
FSC® C125128

Klimaneutral
Druckprodukt
ClimatePartner.com/11669-2110-1003

Inhalt





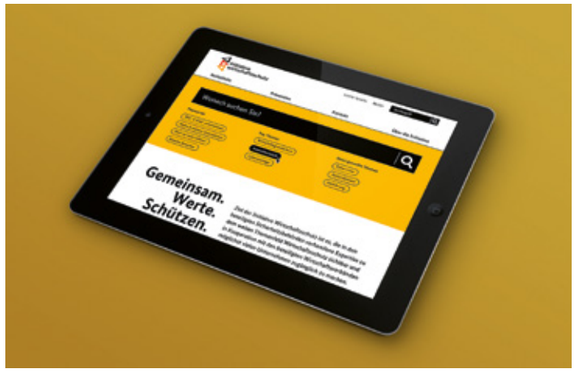
Passwortsicherheit

Seit Jahren wertet das Hasso-Plattner-Institut (HPI) die beliebtesten Passwörter der Deutschen aus, um für das Thema Passwortsicherheit zu sensibilisieren. Auch 2022 waren die Top Ten vor allem simple Zahlen- oder Buchstabenreihen wie „123456“ und „qwertz“ oder schlichte Wörter wie „passwort“, womit es Angreifende nicht besonders schwer haben.

Datengrundlage für die Auswertung ist der „Identity Leak Checker“ des HPI unter **sec.hpi.de/ilc**, mit dem Nutzerinnen und Nutzer selbst überprüfen können, ob sie Opfer eines Datendiebstahls geworden sind. Tipps zur Wahl eines neuen und sicheren Passworts bietet das HPI ebenfalls. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie die Verbraucherzentralen bieten zudem weitere Hilfestellung zum Thema.

Top Ten deutscher Passwörter 2022:

1. 123456
2. 123456789
3. 1Qaz2wsx3edc
4. 12345
5. password
6. qwertz
7. ficken
8. 12345678
9. passwort
10. Ebels123



Wirtschaftsschutz im neuen Look

Das Internetportal der Initiative Wirtschaftsschutz unter **www.wirtschaftsschutz.info** bekommt aktuell ein neues Design. Die Seite soll Unternehmen künftig noch zielgenauer dabei helfen, sich wirksam vor Gefahren zu schützen.

Unter dem Dach der Initiative Wirtschaftsschutz bündeln Sicherheitsbehörden (Bundesamt für Verfassungsschutz (BfV), Bundesnachrichtendienst (BND), Bundeskriminalamt (BKA), Bundesamt für Sicherheit in der Informationstechnik (BSI)) und Wirtschaft (Bundesverband der Deutschen Industrie, Deutscher Industrie- und Handelskammertag, Allianz für Sicherheit in der Wirtschaft, Bundesverband der Sicherheitswirtschaft) ihre breit gefächerte Expertise und stellen aktuelle Informationen zu einer Vielzahl von Themen von Cyberkriminalität über Wirtschafts- und Wissenschaftsspionage bis hin zu IT-Sicherheit bereit. Zudem bietet die Plattform die Möglichkeit, Erfahrungen auszutauschen und Kontakt mit den beteiligten Behörden aufzunehmen.

IT-SICHERHEIT IM HOMEOFFICE

Laut dem Statistischen Bundesamt war 2020 zwischenzeitlich fast ein Viertel aller Erwerbstätigen in Deutschland aus dem Homeoffice tätig. Doch nur in den wenigsten Unternehmen waren die IT-Sicherheitsmaßnahmen auf diese besondere Arbeitssituation hin ausgelegt. Das ergab die Studie „IT-Sicherheit im HOME-OFFICE“ des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Auch 2023 haben die in der Studie aufgezeigten Angriffsflächen nicht an Bedeutung verloren. Homeoffice gehört zur neuen Arbeitswelt, umso wichtiger ist es daher, dass alle Beteiligten sich mit den besonderen Sicherheitsanforderungen auseinandersetzen. Die Studie „IT-Sicherheit im HOME-OFFICE“ ist unter **www.bsi.bund.de** abrufbar.

Foto: FG Trade

Illustration: Joana Schulze

STATE OF THE PHISH

83 % der für den „State of the Phish 2022“-Report befragten Unternehmen geben an, dass sie 2021 wenigstens einem Phishing-Angriff zum Opfer gefallen sind. 2020 waren es gerade einmal 57 %. Der Urheber des Berichts, der IT-Sicherheitsdienstleister Proofpoint, führt die Entwicklung auf ein nachlassendes Aufmerksamkeitsniveau infolge von Pandemiemüdigkeit, den gesteigerten Missbrauch legitimer (speziell Cloud-)Dienste sowie eine immer schnellere Anpassung der Köder an aktuelle Thementrends zurück. Darüber hinaus hat Proofpoint Selbsteinschätzungen der Beschäftigten zu ihren Gewohnheiten beim Thema Cybersicherheit eingeholt: 42 % offenbarten riskante Verhaltensweisen wie das leichtfertige Klicken auf eventuell schädliche Links. 77 % nutzten dienstliche Geräte auch privat. 56 % erlaubten zudem Bekannten und Familienangehörigen den Zugriff. Gleichzeitig waren nur 53 % der Befragten in der Lage, den Begriff „Phishing“ richtig zu erklären.

Die Zahlen zeigen einmal mehr, dass regelmäßige Sensibilisierungen und Schulungen essenziell für den Aufbau einer effektiven Sicherheitskultur sind. Dabei hilft auch das neue Informationsblatt „Schutz vor Phishing“ des BfV.

Nur
24%
der Unternehmen üben regelmäßig, was im Falle eines Cyberangriffs zu tun ist.

58% der Unternehmen nutzen unternehmensfremde IT.

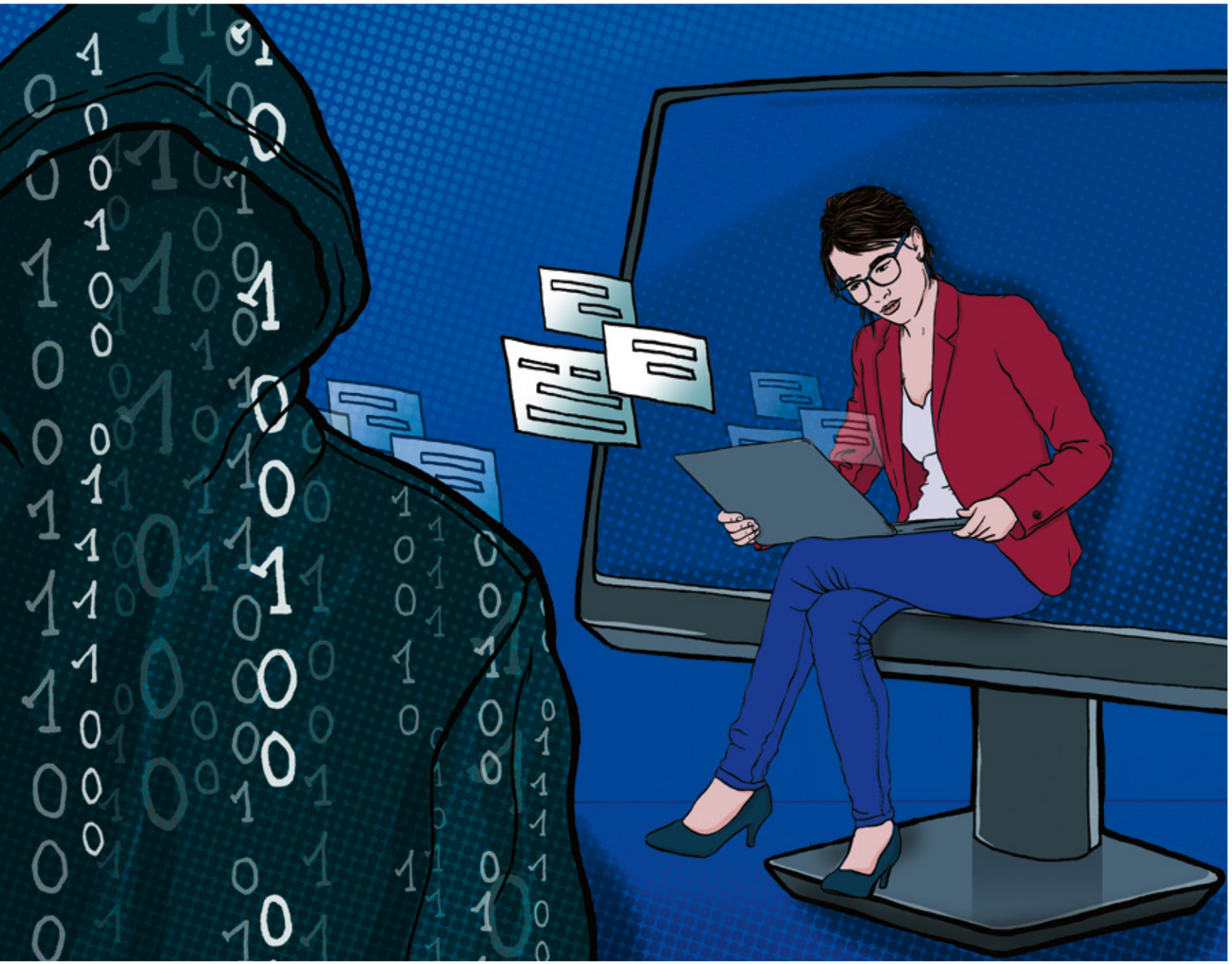
38%
der Unternehmen planen Stress- oder Szenariotests zur Optimierung der eigenen Lieferketten-Resilienz.

17
Supply-Chain-Angriffe zwischen 2020 und 2021 gehen auf das Konto von APT-Gruppierungen.

3–4-mal
so häufig wie schädliche Anhänge sind schädliche URLs.

270-mal
wurden Unternehmen durchschnittlich im Jahr 2021 digital angegriffen.

50% der schwerwiegendsten Risiken für einen Cyberangriff liegen bei Führungskräften.



INNENTÄTERSCHAFT

Wer, weshalb und was dagegen tun?

Redaktion: Wirtschaftsschutz **Illustration:** Sonja Marterner

Wer?

Im Prinzip kann vom Hausmeister bis zur Vorstandsvorsitzenden jede Person Innentäterin oder Innentäter werden. Alle Beschäftigten, aber auch Externe, die sich aufgrund individueller Zugangsmöglichkeiten Zugriff auf Unternehmens- und Forschungdaten verschaffen können und diese an unbefugte Dritte weitergeben. Auch firmenfremde Dienstleisterinnen und Dienstleister kommen somit für eine Innentäterschaft infrage. Und deutsches Know-how ist begehrt, auch bei ausländischen Nachrichtendiensten, die im Staatsauftrag Wirtschaftsspionage betreiben. Dabei bieten Innentäterinnen und Innentäter den Vorteil, dass diese direkt an der Quelle sitzen und so Informationen abziehen oder auch Cyberoperationen zur Spionage oder gar Sabotage erleichtern können.

Wichtig ist an dieser Stelle auch, zwischen Innentäterinnen und Innentätern zu unterscheiden, die mit Vorsatz und gezielt handeln, sei es durch Datendiebstahl, Sabotage oder das Einschleusen von Ransomware sowie jenen, die durch das Öffnen anonymer E-Mails oder dem Herunterladen unerlaubter Software dem Unternehmen unbewusst Schaden zufügen.

Für den Forschungs- und Universitätsbereich bedeuten Innentäterinnen und Innentäter eine besondere Herausforderung. Denn steht auf der einen Seite der im Grundgesetz (Artikel 5 GG) verankerte Grundsatz der Freiheit der Forschung – offen, vielfältig, international, auf Austausch beruhend – muss auf der anderen Seite Wissen vor missbräuchlicher Verwendung geschützt werden. So zum Beispiel vor Gastwissenschaftlerinnen und Gastwissenschaftlern, die Forschungsergebnisse an militärische Einrichtungen in ihrer Heimat weitergeben.

Weshalb?

Oft ist Unzufriedenheit am Arbeitsplatz für aktive Innentäterinnen und Innentäter Grund genug, dem eigenen Unternehmen schaden zu wollen. Aber auch finanzielle Not, Streben nach Respekt und Anerkennung, weltanschauliche Überzeugungen, psychische Ängste bis hin zu Erpressung durch externe Personen können eine Rolle spielen. Unwissenheit oder schlicht Gedankenlosigkeit können zu einer unbewussten Innentäterschaft führen.

Was dagegen tun?

Innentäterinnen und Innentäter können großen Schaden anrichten. Unternehmen inklusive kleiner und mittelständischer Betriebe sowie Forschungseinrichtungen sollten sich daher wappnen. Ein Leitfaden:

1. Identifizieren Sie schützenswerte Güter (Daten und Informationen), mögliche Angreifende und Angriffswege in einer **Risikoanalyse**. Stellen Sie sich Fragen wie: Wo liegt das größte Schadenspotenzial? Wie ist der Umgang mit sicherheitssensiblen Informationen geregelt? Wer arbeitet an sicherheitsrelevanten Stellen?

2. Leiten Sie von den Ergebnissen der Analyse entsprechende Schutzmaßnahmen ab und überführen Sie diese in ein ganzheitliches **Schutzkonzept**. Maßnahmen könnten sein:

   - Klassifizierung der Unternehmensinformationen; z. B. *offen, vertraulich, geheim*.
   - Beschränkung des Zugriffs auf Informationen nach dem „Need-to-know-Prinzip“. Dies gilt auch für Zugänge zu Räumen, Laboren und Gebäuden.
   - Etablierung einer sicherheitsorientierten Personalauswahl („Pre-Employment-Screening“) und Management von Beschäftigtenaustritten.

   Pre-Employment-Screening: Mehr Informationen zum Thema finden Sie in unserem gleichnamigen Informationsblatt, das unter **www.verfassungsschutz.de** *und* **www.wirtschaftsschutz.info** *kostenfrei zur Verfügung steht.*

   - Sensibilisierung und Training der Beschäftigten zu Gefahren und Möglichkeiten von Ausforschung und Know-how-Abfluss.
   - Berücksichtigung des Informationsschutzes bei der Zusammenarbeit mit externen Dienstleisterinnen und Dienstleistern.
   - Etablierung einer Sicherheitskultur.

3. Prüfen Sie ergriffene Maßnahmen regelmäßig auf ihre Wirksamkeit.

4. Passen Sie die Schutzmaßnahmen gegebenenfalls an.

Mehr zum Thema

Die Broschüre „Informationsabfluss aus Unternehmen – Innentäterschaft als unterschätztes Massenphänomen“ leistet mit praxisorientierten Hinweisen, Anregungen und Checklisten *Hilfe zur Selbsthilfe* und stellt darüber hinaus die Unterstützungsmöglichkeiten der Sicherheitsbehörden dar. Sie können diese von der Initiative Wirtschaftsschutz unter der Federführung des Bundesministeriums des Innern und für Heimat (BMI) herausgegebene Publikation unter **www.wirtschaftsschutz.info** kostenfrei herunterladen.

SICHERHEIT versus FREIHEIT?

Wissenschaftsschutz im globalen Wettbewerb

Redaktion: Wirtschaftsschutz BfV **Illustration:** Sonja Marterner

Um den Rang Deutschlands als führenden Innovationsstandort zu sichern, sind wissenschaftliche Erkenntnisse und Erfindungen in technischen Zukunftsbranchen elementar. Doch auch andere Länder haben großes Interesse, deutsches Know-how für den eigenen Fortschritt zu nutzen und loten so immer neue Wege aus, an dieses zu gelangen. Die Nachrichtendienste dieser Länder spielen dabei eine wichtige Rolle.

Bereits 2008 forschte Professor Changhua Hu als Gastwissenschaftler für vier Monate an der Universität Duisburg-Essen und konnte sich in dieser Zeit wichtige Forschungserkenntnisse aneignen. Seine Stellung als Generalmajor der chinesischen Volksbefreiungsarmee (VBA) verheimlichte er vor der Universität, die von der wahren Identität des Professors erst 2018 erfuhr.

Die Wege, die ausländische Nachrichtendienste einschlagen, um an deutsches Know-how zu gelangen, sind vielfältig: die Entsendung von Forscherinnen und Forschern in staatlichem Auftrag, die Rekrutierung deutscher Wissenschaftlerinnen und Wissenschaftler, aber auch klassische Spionage sind dabei bewährte Methodiken. Dabei wird die eigentliche Herkunft der Forschenden wie im Falle von Professor Hu häufig verschleiert.

Neben Hochschulen und anderen Forschungsinstituten stehen auch technologieorientierte, forschende Unternehmen im Fokus ausländischer Nachrichtendienste. Von besonderem Interesse sind die Bereiche Luft- und Raumfahrttechnik, Biotechnologie, Medizintechnik, Industrierobotik, Informations- und Kommunikationstechnik, Automobil- und Maschinenbau sowie Energie- und Umwelttechnologie. Branchen also, in denen Wirtschaft und Wissenschaft eng miteinander verknüpft sind, ob in eigenbetrieblicher Forschung und Entwicklung (F&E) oder durch Kooperationen mit außerbetrieblichen Forschungseinrichtungen.

Gerade diese Forschungsfreiheit ist ein in Deutschland durch Artikel 5 des Grundgesetzes geschütztes hohes Gut, das für Offenheit, Vielfalt und Austausch steht. Was passiert, wenn diese Freiheit durch ausländische Akteurinnen und Akteure ausgenutzt wird, die eigene staatliche Interessen mit in Deutschland erworbenem Wissen verfolgen?

China und Russland, die Global Player in der Wissenschafts- und Wirtschaftsspionage

Bei der Ausspähung ausländischen Know-hows treten die Volksrepublik China und die Russische Föderation besonders hervor. Es ist staatlich gesteuerte Strategie beider Länder, die eigene Forschung und Produktion wichtiger Technologien nicht nur durch eigene Innovationskraft, sondern auch durch die Leistungen anderer voranzutreiben.

Chinas Ziele

Wirtschaftlich, wissenschaftlich und militärisch will China bis 2049 global führend sein und setzt Spionage gezielt ein, um der nationalen Forschung und Entwicklung einen Vorteil gegenüber der internationalen Konkurrenz zu verschaffen. Dazu kann das Land auf scheinbar unerschöpfliche menschliche und finanzielle Ressourcen zurückgreifen. Von der Regierung aufgesetzte Programme unterstützen die ambitionierten Ziele des Landes

zusätzlich. So zum Beispiel der „High-end Foreign Experts Recruitment Plan“ zur gezielten Anwerbung ausländischer Expertinnen und Experten oder die „Military-Civil Fusion“, die darauf setzt, durch Zuhilfenahme der Kreativität des privaten Sektors Chinas militärisches Potenzial zu erhöhen.

Strategische Wissenschaftsspionage für die militärische Nutzung

Die Förderung internationaler Forschungskooperationen ist ebenso Teil der chinesischen Strategie wie zunehmende Methode. Die im Mai 2022 veröffentlichte „China Science Investigation“, eine investigative Recherche eines Konsortiums von elf europäischen Medien, zeigt diesbezüglich eine besorgniserregende Entwicklung auf. 350 000 wissenschaftliche Studien europäischer Hochschulen aus den vergangenen zwei Jahrzehnten wurden auf Verbindungen zum chinesischen Militär untersucht. Dabei wurden die Tätigkeiten entsandter chinesischer Wissenschaftlerinnen und Wissenschaftler, die mit der VBA assoziiert werden, besonders beleuchtet. Das Ergebnis: Europaweit konnten circa 3 000 Projekte identifiziert werden, die mit chinesischen, dem Militär nahestehenden Instituten kooperierten. In Deutschland seien es 349 Arbeiten, entstanden an 48 Hochschulen.

Auf chinesischer Seite stachen in der Recherche sieben Universitäten heraus, die dem Militär in Forschung und Lehre besonders nahe- und seit Langem im Fokus westlicher Nachrichtendienste stehen, die sogenannten Seven Sons of National Defence. In den USA wurde bereits 2020 für Absolventinnen und Absolventen sowie Studierende dieser Einrichtungen ein Einreiseverbot erlassen.

Dual-Use-Güter
Ein besonderes Risiko

Die von China stark vorangetriebene Verflechtung von Wirtschaft, akademischen Institutionen und dem Militär hat ein erhöhtes Interesse an Ergebnissen der Grundlagenforschung und sogenannten Dual-Use-Gütern, die sowohl zivil als auch militärisch genutzt werden können, zur Folge. So sollen künftig gerade zivile Technologien in die Rüstungsentwicklungen und -forschungen einfließen. Eine ausreichende Sensibilität, um die Gefahren der Spionage und das hohe Risiko des Know-how-Verlusts richtig einschätzen zu können, fehlt jedoch an deutschen Hochschulen häufig genauso wie entsprechende Schutzmaßnahmen.

Ein aktuelles Beispiel zeigt, wie unbedarft teilweise bei wissenschaftlichen Kooperationen vorgegangen wird. So pflegte eine technische Universität in Deutschland von 2017 bis 2022 einen intensiven Forschungsaustausch im materialwissenschaftlichen Bereich zu Stoffen, die sich als Dual-Use-Güter auch für hochmoderne Waffensysteme verwenden lassen, mit einer chinesischen Universität, die zu den Seven Sons of National Defence zählt. Während die deutsche Seite primär wissenschaftliche Ambitionen hegte und eine Publikation anstrebte, war es ihr durchaus bewusst, dass sich die chinesische Seite auf die praktische Anwendung und gewinnbringende Absichten konzentrierte. Ungeachtet dessen wurde die Zusammenarbeit bis zum planmäßigen Abschluss fortgeführt.

So eindeutig der Sachverhalt auch erscheint, verstieß die Zusammenarbeit nicht gegen ein geltendes Gesetz. Das Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) überwacht zwar den Export von Dual-Use-Gütern, Ergebnisse von Forschungskooperationen fallen jedoch nicht unter diese Restriktionen. Es liegt oftmals bei den Instituten, Hochschulen und Unternehmen selbst, die Risiken oder Bedenken einer Kooperation mit externen Wissenschaftlerinnen und Wissenschaftlern gegenüber dem Willen zum schnellen Fortschritt abzuwägen. Zudem können die meisten Hochschulen auf Drittmittel nicht mehr verzichten, um als Forschungsbetrieb wettbewerbsfähig zu bleiben.

China Defence University Tracker:
Der vom Australian Strategic Policy Institute (ASPI) entwickelte China Defence University Tracker hilft Universitäten, Unternehmen und der Politik dabei, ihr Engagement mit chinesischen Forschungs- und Wissenschaftseinrichtungen einzuordnen.

Die Datenbank dokumentiert chinesische Forschungs- und Wissenschaftseinrichtungen und ihre Verbindungen zum Verteidigungs- und Sicherheitssektor. Je nach nachgewiesener Verstrickung (z. B. Involvierung in Spionage oder Cyberattacken, Listung in proliferationsrelevanten Endnutzerinnen- und Endnutzerlisten oder Verbindungen zu Menschenrechtsverletzungen) wird jeder einzelnen Einrichtung eine Kategorie zugewiesen, die das Risiko der Spionage einordnet (www.unitracker.aspi.org.au).

Russlands Ziele

Thomas Haldenwang, Präsident des Bundesamtes für Verfassungsschutz (BfV), konstatierte Mitte 2021 in einem Interview mit der WELT AM SONNTAG, dass die Aktivitäten der russischen Nachrichtendienste in Deutschland mittlerweile das Niveau des Kalten Krieges erlangt haben. Die Nachrichtendienste der Russischen Föderation sind ein fester Bestandteil der staatlichen Sicherheitsarchitektur und – wie die chinesischen Dienste – mit umfangreichen Befugnissen ausgestattet. Die Spionageaktivitäten erstrecken sich auf die Zielbereiche Politik, Wirtschaft, Wissenschaft, Technik und Militär.

Im Streben nach Hegemonie gehören staatlich gesteuerte Ausspähungen ausländischen Know-hows für China zum Standard.

Auch Russland priorisiert dabei bestimmte Bereiche für die nächsten 10–15 Jahre. Rückschlüsse auf das Aufklärungsinteresse seiner Nachrichtendienste lassen sich aus wirtschaftspolitischen Strategiedokumenten ableiten. So auch die am 1. Dezember 2016 von Präsident Wladimir Putin erlassene „Strategie für die wissenschaftliche und technologische

Entwicklung der Russischen Föderation“. Demnach stehen im Vordergrund des wirtschafts- und wissenschaftsbezogenen Ausforschungsinteresses der russischen Nachrichtendienste vornehmlich technologieorientierte und innovative deutsche Unternehmen aus den Bereichen Informations- und Kommunikationstechnik, Biotechnologie, Optoelektronik, Automobil- und Maschinenbau, Luft- und Raumfahrttechnik sowie Energie- und Umwelttechnologie.

Spionierende haben es dabei insbesondere auf kleine und mittlere Unternehmen, das Rückgrat der deutschen Wirtschaft, abgesehen, die im Gegensatz zu großen Konzernen oftmals nur über unzureichende personelle oder finanzielle Ressourcen verfügen, um ganzheitliche Sicherheitskonzepte umzusetzen. Aber auch die Wissenschaftslandschaft in Deutschland ist schon lange im Visier der russischen Nachrichtendienste.

Erst im April 2022 wurde ein russischer Staatsangehöriger wegen geheimdienstlicher Agententätigkeit vom Oberlandesgericht München verurteilt. Seit 2014 hatte er als wissenschaftlicher Mitarbeiter für einen naturwissenschaftlich-technischen Lehrstuhl im Bereich Materialwissenschaften der Universität Augsburg gearbeitet. Ein als Vizekonsul akkreditierter Mitarbeiter des russischen Generalkonsulats in München, der für den zivilen Auslandsgeheimdienst der Russischen Föderation (SWR) arbeitete, soll im Herbst 2019 zu dem Angeklagten Kontakt aufgenommen haben. Gegenüber dem Angeklagten gab der Vizekonsul bei einem ersten Treffen vor, für eine russische Bank zu arbeiten und Informationen für private Investments zu benötigen. Schließlich gab der Angeklagte Informationen zu Forschungsprojekten aus dem Bereich Luft- und Raumfahrttechnologie weiter, insbesondere von den verschiedenen Entwicklungsstufen des europäischen Trägerraketenprogramms Ariane. Dafür habe er insgesamt 2.500 Euro erhalten.

Verschärfte Sanktionen erfordern eine erhöhte Alarmbereitschaft gegenüber russischen Spionageaktivitäten.

Etwas länger zurückliegt das Beispiel eines russischen Physikers, der ebenfalls unter dem Verdacht stand, vertrauliche Forschungsinhalte an den SWR weitergegeben zu haben. Von 2009 bis 2011 forschte er jeweils für mehrere Monate als Gastwissenschaftler am Max-Planck-Institut für die Physik des Lichts im bayerischen Erlangen im Bereich Quantenoptik und Nanophotonik – Grundlagenforschung, die etwa bei der Entwicklung von Quantencomputern eine Rolle spielt.

Aktuelle Entwicklungen

Für Russland ist in den letzten Jahren die Notwendigkeit, sich Technologien auf illegalen Wegen zu beschaffen, gestiegen. Bereits 2014/15 hatte die Europäische Union aufgrund der Annexion der Krim durch Russland ein Waffenembargo sowie Handelsbeschränkungen für Dual-Use-Güter und Ausrüstung für den Energiesektor veranlasst. Eine Situation, die sich durch den Angriff auf die Ukraine und neue Sanktionspakete seitens der EU und anderer Staaten noch verschärft hat. So ist nun die Lieferung sämtlicher Güter und Technologien, die zur militärischen und technologischen Stärkung Russlands oder zur Entwicklung des Verteidigungs- und Sicherheitssektors beitragen können, verboten.

Um in strategisch wichtigen Bereichen handlungsfähig zu bleiben, wird Russland mit großer Sicherheit versuchen, diese Sanktionen zu umgehen oder zu unterlaufen – sei es durch gesteigerte Spionageaktivitäten im Wirtschafts-, Finanz- und Technologiesektor oder durch die Errichtung von Tarnfirmen zur Beschaffung von Gerätschaften, die Exportbeschränkungen unterliegen.

Doch nicht nur Spionageaktivitäten können unsere Wissenschaft und Forschung schädigen. Auch absichtlich gestreute Desinformationen können unter anderem zu Reputationsschäden führen und Zweifel bezüglich wissenschaftlicher Erkenntnisse schüren. Lesen Sie dazu auch unseren Artikel „Fledermäuse als Biowaffen – Russlands Desinformationskampagne gegen das Friedrich-Loeffler-Institut“ (S. 16).

Die Methodik ausländischer Nachrichtendienste

Eine gängige und wesentliche Vorgehensweise ist die Gewinnung wirtschaftlicher, wissenschaftlicher, militärischer und politischer Informationen durch öffentlich zugängliche Quellen (OSINT - Open Source Intelligence). Das Internet spielt hier eine entscheidende Rolle. Aber auch die Nutzung von Personen als Informationsquellen hat kaum an Bedeutung eingebüßt. Dabei kommen bei der Informationsgewinnung durch menschliche Quellen – sogenanntes HUMINT (Human Intelligence) – alle Personen infrage. Entscheidend ist der mögliche Zugang der Zielperson zu bestimmten Informationen.

Im wissenschaftlichen Umfeld werden dazu verschiedene Wege genutzt: Bei der klassischen Anbahnung akademischen Personals geschieht die direkte Kontaktaufnahme zumeist im entsprechenden Umfeld, auf Tagungen, bei gemeinsamen Forschungsprojekten oder Austauschprogrammen. Mitarbeiterinnen und Mitarbeiter ausländischer Nachrichtendienste nutzen dabei häufig legendierte akademische Titel und Positionen („Vize-Direktor des Forschungsinstitutes XY“; „Vertreterin eines Think Tanks“) und schlagen beispielsweise die Mitarbeit in einem Forschungsprojekt vor.

Als weitere Möglichkeit der Kontaktaufnahme wird ein wissenschaftlicher Artikel zu bestimmten Themen gegen Bezahlung in Auftrag gegeben. Um eine langfristige Informationsgewinnung sicherzustellen, wird unter Umständen auch eine freundschaftliche Beziehung zur Zielperson aufgebaut. Ebenso kann das private Umfeld (Familie, Freundeskreis, Hobbys etc.) Anknüpfungspunkt für ausländische Nachrichtendienste sein. Die Aufträge werden mit der Zeit gezielter und riskanter wie die konkrete Beschaffung vertraulicher Informationen zu Forschungsprojekten oder Gewährung von Zugang zu sensiblen Daten, während die dafür gezahlten Summen steigen.

Hohe Gehälter und reichhaltige Forschungsmittel sind meist treibende Kraft für Wissenschaftlerinnen und Wissenschaftler. So forschte der mittlerweile verurteilte US-amerikanische Chemiker Charles Lieber, ein weltweit führender Experte im Bereich der Nanotechnologie, neben seiner Anstellung an der Harvard University zwischen 2011 und 2017 im Rahmen des „Tausend-Talente-Programms“ für die Wuhan University of Technology und verdiente damit Millionen.

Die Aussicht einer attraktiven beruflichen Position, Reisen, die Teilnahme an Veranstaltungen

oder Auszeichnungen werden von ausländischen Nachrichtendiensten ebenfalls als Werkzeuge genutzt, um zu einer Mitarbeit zu verleiten. Was die Sache noch verhängnisvoller macht, wenn die Annahme solcher „Belohnungen“ dann zur Kompromittierung genutzt und die Zielperson zu einer Zusammenarbeit erpresst wird.

Darüber hinaus nutzen insbesondere autokratisch geführte Staaten die eigenen Landsleute gezielt zur Informationsgewinnung im Ausland, wie in vorangegangenen Beispielen erläutert durch die Entsendung beispielsweise von Gastwissenschaftlerinnen und Gastwissenschaftlern oder Studierenden im Rahmen von Forschungskooperationen, Austauschprogrammen oder Studienaufenthalten. Auch hier wirken Mechanismen wie finanzielle Anreize und attraktive Positionen, Vergünstigungen für Angehörige, ideologische oder patriotische Motive, gesetzliche Bestimmungen des Heimatlandes oder Erpressung.

Wie lässt sich also der auf Austausch beruhende Grundgedanke von der Freiheit der Forschung gegen Strategien schützen, die diese Freiheit einseitig für ihre Zwecke ausnutzen?

Hochschulen und Forschungseinrichtungen stehen den Bestrebungen fremder Staaten und deren Nachrichtendiensten nicht hilflos gegenüber.

Maßnahmen zum Schutz vor Spionagetätigkeiten

Für Sicherheitsverantwortliche:

- Klassifizieren Sie Instituts- und Forschungsdaten nach Vertraulichkeitsklassen und setzen Sie das „Need-to-know-Prinzip“ um.
- Prüfen Sie bei geplanten Kooperationen, ob die Institutionen dem Militär nahestehen. Diese sind als besonders kritisch zu bewerten.
- Führen Sie bei der Personalauswahl (auch bei Gastwissenschaftlerinnen und -wissenschaftlern, ausländischen Praktikantinnen und Praktikanten etc.) Hintergrundchecks durch. Schauen Sie insbesondere auf Verbindungen zu Militäreinrichtungen.
- Etablieren Sie eine konstruktive Fehlerkultur und Meldewege.
- Bereiten Sie Besuche ausländischer Delegationen zur Besichtigung von Forschungseinrichtungen oder Innovationszentren von Unternehmen mit Hintergrundchecks und dem Verlangen der Namen aller Teilnehmerinnen und Teilnehmer gut vor.
- Stellen Sie ein striktes Handy- oder Fotografierverbot sowie ein Nutzungsverbot von portablen Datenträgern in sensiblen Bereichen sicher.
- Schulen Sie die Wissenschaftlerinnen und Wissenschaftler und Studierenden auch im Hinblick auf mögliche Anwerbungsversuche.

Für Wissenschaftlerinnen und Wissenschaftler sowie Studierende:

- Seien Sie vorsichtig bei Gefälligkeiten oder beruflichen Angeboten mit unüblichen Konditionen. Die Kontaktaufnahme kann auch über Social-Media- bzw. Social-Business-Kanäle erfolgen.
- Lassen Sie sich die Identität der Ansprechpartnerin oder des Ansprechpartners ggf. bestätigen.
- Schützen Sie Ihre Daten durch sichere Passwörter.
- Lassen Sie Skepsis walten bei ungewöhnlichen fachlichen Anfragen.
- Nehmen Sie im Zweifelsfall Kontakt mit der sicherheitsverantwortlichen Stelle bzw. den Sicherheitsbehörden auf.
- Bei Reisen ins Ausland weisen wir auf den Artikel „Sicherheit auf Geschäftsreisen“ (S. 42) in diesem Heft hin.

Fledermäuse als Biowaffen

Russlands Desinformationskampagne gegen das Friedrich-Loeffler-Institut

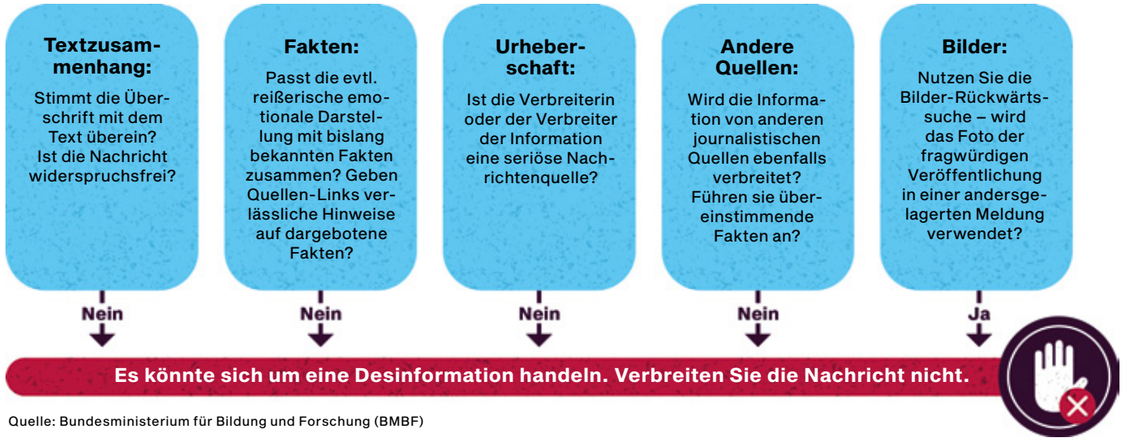
Redaktion: Wirtschaftsschutz

Es ist der 10. März 2022, als das russische Verteidigungsministerium auf einer Pressekonferenz erneut den Einmarsch in die Ukraine zu legitimieren versucht. Es geht um die angebliche Erforschung von Biowaffen in der Ukraine, die gegen Russland eingesetzt werden sollen. Eine als Desinformation entlarvte Erzählung Moskaus, die aber eine neue Qualität bekommt, als Forscherinnen und Forscher des Friedrich-Loeffler-Instituts (FLI), des Bundesforschungsinstituts für Tiergesundheit, namentlich als Unterstützerinnen und Unterstützer dieser Forschung benannt werden.

Fotos: gettyimages/Mike Powles; mediaphotos

Bereits seit 1910 widmet sich das FLI, mit Hauptsitz auf der Insel Riems im idyllischen Greifswalder Bodden, der Gesundheit und dem Wohlbefinden landwirtschaftlicher Nutztiere, aber auch dem Schutz des Menschen vor übertragbare Zoonosen – zwischen Tier und Mensch übertragbare Infektionen. Der Vorwurf der Russen: Gemeinsam mit ukrainischen Kolleginnen und Kollegen und weiteren westlichen Staaten arbeite das FLI daran, Fledermäuse, Vögel und Reptilien mit übertragbaren Krankheiten zu infizieren und sie anschließend über die russische Grenze ziehen zu lassen. Vermeintlich festgeschrieben wurde diese Zusammenarbeit in einem Vertrag, der neben der Desinformation ebenfalls veröffentlicht wird. Ein echtes Dokument zwar, doch regelte es lediglich die Übersendung von inaktivierten Proben, die im FLI auf mögliche Krankheitserreger, die von Flöhen, Zecken und Fliegen auf den Menschen übertragen werden könnten, hin untersucht wurden. Für die russische Propagandamaschine reichte die Arbeit des FLI mit tierischen Infektionserregern, die Zusammenarbeit mit dem ukrainischen Institut und die Komplexität des Themas jedoch aus, um der Erzählung genügend Glaubwürdigkeit zu geben. Das Ziel der Desinformationskampagne, eine möglichst große Reichweite zu generieren, wurde durch die schnelle Verbreitung der Desinformation durch russlandfreundliche Medien sowie Influencerinnen und Influencer gewährleistet.

Fakt oder Fake? 5 Tipps, wie Sie Desinformation erkennen können.



Quelle: Bundesministerium für Bildung und Forschung (BMBF)

Debunking – wie sich Organisationen wehren können

Das FLI entschloss sich gemeinsam mit dem ukrainischen Labor, den falschen Anschuldigungen mit einer Richtig- und Klarstellung sowie Erklärung der Sachlage anhand überprüfbarer Fakten entgegenzutreten – das sogenannte Debunking. In einem Artikel im Science-Magazin und in der regionalen Presse wurde die Kampagne benannt und mitsamt von Hintergrundinformationen richtiggestellt. Der Artikel wurde auch über die Social-Media-Kanäle des FLI verbreitet, um möglichst die gleiche Zielgruppe wie die russische Desinformation zu erreichen. Größerer Schaden konnte so abgewendet werden. Doch nicht immer ist Debunking sinnvoll. Gibt es Anzeichen dafür, dass die Desinformation im Sande verläuft, kann eine Debunking-Maßnahme die Reichweite der Desinformation noch erhöhen. Wenn sich aber bereits eine hohe Reichweite abzeichnet und ein reputativer oder wirtschaftlicher Schaden anbahnt, sollten Sie handeln.

Was Sie beim Debunking beachten sollten:

- Vermeiden Sie Verlinkungen auf die ursprüngliche Desinformation.
- Ist eine erneute Nennung der Desinformation notwendig, verpacken Sie diese im Mittelteil Ihrer Nachricht und stellen die Fakten an deren Anfang und Ende. Diese bleiben Leserinnen und Lesern besser im Gedächtnis.
- Bleiben Sie sachlich und führen Sie lediglich relevante Argumente an.
- Visualisierungen von Informationen in bspw. Schaubildern sind besonders einprägsam und erhöhen die Reichweite, insbesondere in den sozialen Medien.
- Handeln Sie zeitnah.

Das schwächste Glied

Lieferketten im Fokus von Cyberkriminellen

Zwei von drei Cyberangriffen sind Attacken auf eine Lieferkette. Dahinter können kriminelle Gruppierungen mit finanziellen Motiven stecken, aber auch Spionage oder Sabotage durch staatliche Stellen.

Redaktion: Wirtschaftsschutz

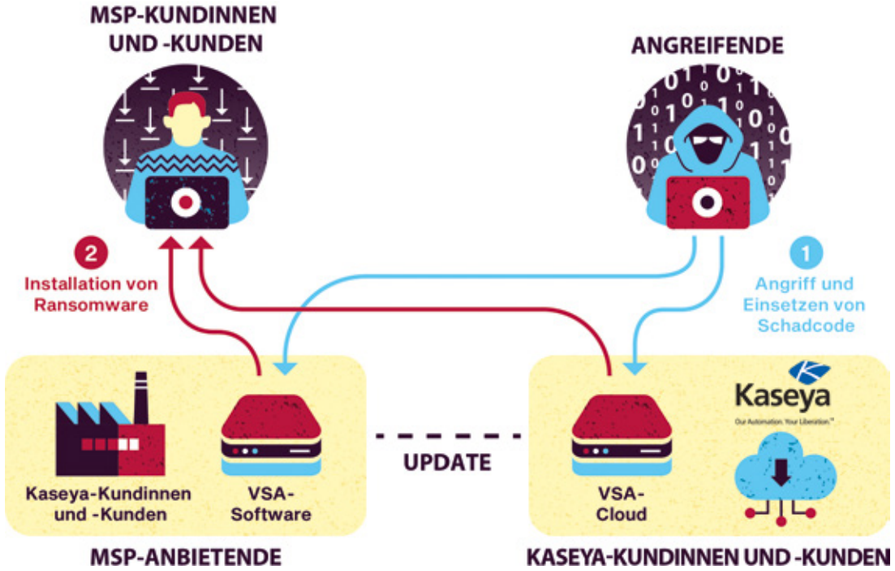
REvil ist zurück. Als im Frühjahr 2022 Meldungen über das Comeback der Cybercrimegruppe die Runde machten, dürften IT-Sicherheitsverantwortliche weltweit ins Schwitzen geraten sein. REvils Ransomware-Angriffskampagne im Sommer 2021, die unter anderem den weltgrößten Fleischproduzenten JBS in den USA und die Supermarktkette Coop in Schweden tagelang lahmlegte, gilt als eine der folgenreichsten der Geschichte, an der die Hackerinnen und Hacker Millionen verdienten.

> *Ransomware: Ransomware sind Schadprogramme, die den Zugriff auf Daten und Systeme verschlüsseln oder ganz sperren. Für deren Wiederherstellung verlangen Angreifende ein Lösegeld (Englisch „ransom"). Die Zahlung ist jedoch keinesfalls eine Garantie, dass die Opfer im Anschluss wieder auf Systeme und Daten zugreifen können.*

Der Angriff begann mit einem Hack des Software-Herstellers Kaseya, dessen IT-Management-Software VSA in Kassensystemen weltweit eingesetzt wird. Doch anstatt des neuesten Updates von Kaseya spielten sich Kundinnen und Kunden unwissentlich REvils Ransomware Sodinokibi auf, die ihre Systeme verschlüsselte. Für deren Wiederherstellung forderte REvil ein Rekordlösegeld von 70 Millionen Dollar.

Laut Kaseya-CEO Fred Voccola könnten von der Attacke weltweit bis zu 1 500 Unternehmen betroffen gewesen sein. Allerdings ist die Dunkelziffer wohl weitaus höher, weil Kaseyas Kundinnen und Kunden wiederum häufig selbst IT-Dienstleisterinnen und -Dienstleister für andere Unternehmen sind. Die Folge ist ein für Supply-Chain-Angriffe typischer, verheerender Dominoeffekt.

Foto: artpartner-images; Infografiken: Joana Schulze



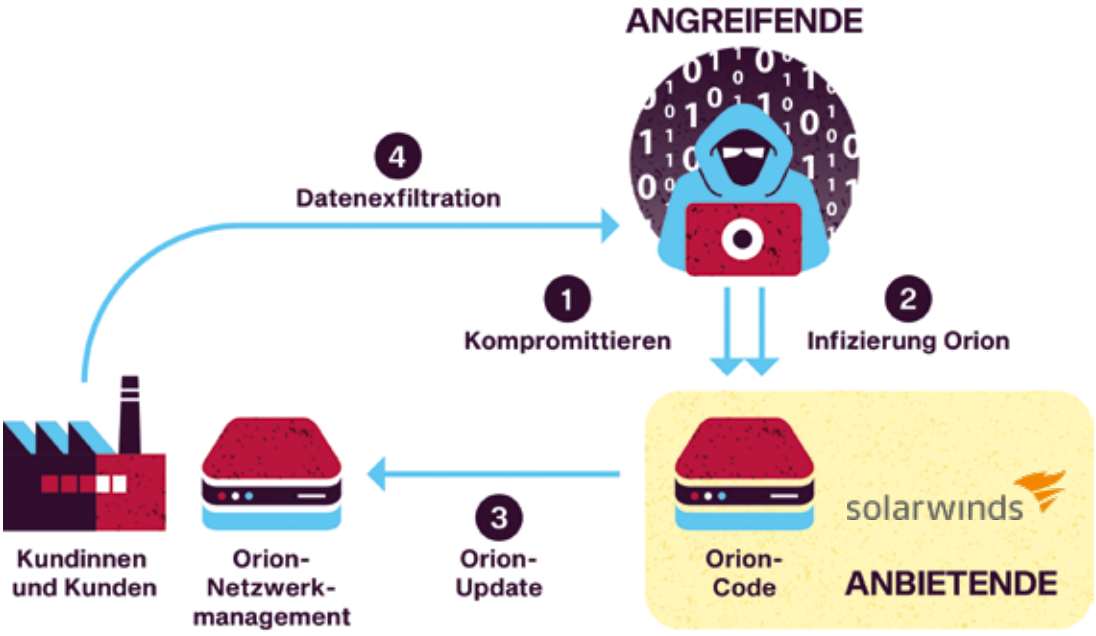
Grafische Darstellung des Lieferkettenangriffs auf Kaseya; die Angreifenden schleusten Code in VSA (Virtual Storage Appliance) Instanzen von MSP-Anbietenden (Managed Service Provider) ein (ob vor Ort wird noch geprüft). Über einige dieser MSPs wurden Schadprogramme und Ransomware bei deren Kundinnen und Kunden installiert. Quelle: European Union Agency for Cybersecurity (ENISA)

Angriffstechniken zur Kompromittierung einer Lieferkette

Malware-Infektion:	u. a. Einsatz von Spyware zum Diebstahl von Anmeldedaten von Beschäftigten
Social Engineering:	u. a. Phishing, gefälschte Bewerbungen, Typosquatting, Wifi-Imitation, Zielpersonen zu Handlungen verleiten
Brute-Force-Attacke:	u. a. Erraten eines SSH-Passworts oder Web-Logins
Ausnutzen von Software-Schwachstellen:	u. a. SQL-Injection oder Ausnutzen eines Puffer-Überlaufs in einer Anwendung
Ausnutzen von Schwachstellen im Prozess:	u. a. Vorteile aus einem Konfigurationsfehler ziehen
Modifizierung oder physische Attacke:	u. a. Modifizieren von Hardware oder physisches Eindringen
Open Soure Intelligence (OSINT):	u. a. Onlinesuche nach Anmeldedaten und API-Keys
Fälschung:	u. a. Fälschung von USB-Sticks mit maliziöser Software

Mögliche Angriffsvektoren für einen Supply-Chain-Angriff. Quelle: ENISA

Ein anderer brisanter Fall, der SolarWinds-Hack Ende 2020, verdeutlicht die Dimensionen, um die es geht. Über die SolarWinds-Plattform Orion war es Hackerinnen und Hackern gelungen, eine Hintertür namens Sunburst in die Systeme und Netzwerke der Nutzerinnen und Nutzer einzuschleusen. Das Fatale: Nicht nur konnte in kürzester Zeit eine Vielzahl von Systemen infiziert werden. Orion verfügt auch von Haus aus über umfangreiche Zugriffsrechte, sodass die Angreifenden schnell tief in die Opfersysteme vordringen und großen Schaden anrichten konnten. Weltweit zählt SolarWinds



Grafische Darstellung des Lieferkettenangriffs auf SolarWinds: Die Angreifenden kompromittierten das SolarWinds-Netzwerk und modifizierten die Orion-Software während des Build-Prozesses. Die Orion-Nutzerinnen und -Nutzer luden sich den Schadcode sodann direkt via Update herunter, sodass die Angreifenden Zugriff auf deren Daten erlangten. Quelle: ENISA

über 300 000 Kundinnen und Kunden. Darunter fast alle Fortune-500-Unternehmen der USA. Gut ein Zehntel davon nutzt Orion.

US-amerikanische Sicherheitsbehörden ordnen den SolarWinds-Hack dem russischen Auslandsnachrichtendienst SWR zu, genauer gesagt der ihm zugeschriebenen Cybergruppierung APT29.

> *Advanced Persistent Threat (APT): Unter APT versteht man einen komplexen, zielgerichteten und effektiven Angriff auf vor allem anspruchsvolle Ziele. APTs erfolgen nach langer Vorbereitung und Anpassung an das Opfer. Das Ziel ist, sich möglichst lange unentdeckt im Opfersystem zu bewegen, um möglichst viele Daten abzugreifen.*

Eine solche Steuerung durch ausländische staatliche Stellen lässt sich daraus ableiten, dass es den Angreifenden nicht nur um rein monetäre Motive geht, sondern dass sie weiterreichende Spionage- und Sabotageziele verfolgen. Die European Union Agency for Cybersecurity (ENISA) kommt in einer Auswertung von Supply-Chain-Angriffen zwischen Januar 2020 und Juli 2021 zu dem Schluss, dass in der Hälfte aller Fälle APTs dahintersteckten. Gleichzeitig nimmt die Zahl dieser Art von Angriffen weiter zu. Die Unternehmensberatung Accenture geht davon aus, dass inzwischen 61 % aller Cyberangriffe gegen Lieferketten gerichtet sind. Dabei liegt der Vorteil für Angreifende klar auf der Hand: Große Unternehmen verfügen über gut aufgestellte IT-Sicherheitsorganisationen. Kleineren Unternehmen und Betrieben hingegen fehlt es oft an notwendigen Kapazitäten, um Sicherheitsmaßnahmen laufend auf dem neuesten Stand zu halten. Einfallstore, die Angriffe auf das eigentliche Ziel erleichtern oder überhaupt erst ermöglichen, lassen sich bei ihnen deutlich einfacher finden.

IT-Sicherheitsmaßnahmen und -prozesse müssen daher sämtliche Stationen und Beteiligte entlang einer Lieferkette einbeziehen, im Analogen wie im Digitalen. Es reicht nicht aus, nur die eigenen Abläufe, Systeme und Daten gegen Störungen und Angriffe abzusichern. Umfragen wie das „Allianz Risk Barometer 2021“ oder der „Deloitte CFO Survey Frühjahr 2022“ deuten erfreulicherweise darauf hin, dass das Bewusstsein für Supply-Chain-Risiken in den Führungsetagen wächst. IT-Sicherheitsverantwortliche dürften das begrüßen.

> *Realweltliche Supply-Chain-Risiken: Als global vernetzte Exportnation ist Deutschland in besonderem Maße auf funktionierende Lieferketten angewiesen. Die Corona-Pandemie, die Blockade des Suez-Kanals durch das Containerschiff Ever Given oder der Krieg in der Ukraine haben allerdings gezeigt, wie verletzlich bestehende Strukturen sind. Eine kurzfristige Veränderung der weltpolitischen und wirtschaftlichen Lage im Sinne eines Abbaus von internationalen Produktions-, Liefer- und Handelshemmnissen ist nicht in Sicht. Die Herausforderungen scheinen im Gegenteil eher zuzunehmen.*

Bundesamt
für Verfassungsschutz (BfV)

PARTNER DES VERTRAUENS

Bundesamt für Verfassungsschutz (BfV)

Aufgaben, Verantwortungen, Kontrolle

Die Verfassung der Bundesrepublik Deutschland entwirft eine **wehrhafte Demokratie**. Dies umfasst alle rechtsstaatlichen Maßnahmen, mittels derer die Demokratie aktiv verteidigt wird.

Auch die Freiheit des Einzelnen, die selbst durch Freiheitsrechte und politische Teilhaberechte im Grundgesetz verankert ist, darf nicht zum Zweck instrumentalisiert werden, die **freiheitliche demokratische Grundordnung** abzuschaffen oder auszuhöhlen.

Der **Auftrag des Bundesamtes für Verfassungsschutz (BfV)** ist es, alle Anstrengungen, von außen und von innen, abzuwenden, die unser Land und die freiheitliche demokratische Grundordnung schädigen sollen.

It’s all about information

Das Bundesamt für Verfassungsschutz (BfV) ist einer der drei Nachrichtendienste des Bundes. Als Inlandsnachrichtendienst ist der Verfassungsschutz ein wichtiger Bestandteil der deutschen Sicherheitsarchitektur. Seine Aufgaben umfassen unter anderem die Abwehr von Spionage und den Schutz der absoluten und unabänderlichen Werteprinzipien, die unseren demokratischen Rechtsstaat ausmachen: die **freiheitliche demokratische Grundordnung**. Um die Sicherheit der Bundesrepublik Deutschland vor solchen Bestrebungen durch fremde Mächte, Terrorismus und politischen wie religiösen Extremismus zu schützen, sammelt und analysiert der Verfassungsschutz – in enger Zusammenarbeit mit den Landesbehörden für Verfassungsschutz – Informationen. Diese werden zu einem großen Teil aus öffentlich zugänglichen Quellen bezogen, aber auch – unter Wahrung der engen gesetzlichen Voraussetzungen – mit nachrichtendienstlichen Mitteln.

So sollen **Bestrebungen gegen die freiheitliche demokratische Grundordnung** frühzeitig erkannt und der Bundesregierung eine präzise Gefahrenanalyse ermöglicht werden.

Die **freiheitliche demokratische Grundordnung** beschreibt die unabänderlichen obersten Werteprinzipien — die Menschenwürde, das Demokratieprinzip und die Rechtstaatlichkeit — als Kernbestand der Demokratie. Sie bestimmen die Gesetzgebung des Bundes und der Länder.

Bestrebungen gegen die freiheitliche demokratische Grundordnung sind politisch bestimmte, ziel- und zweckgerichtete Verhaltensweisen in einem oder für einen Personenzusammenschluss, die darauf gerichtet sind, einen der Verfassungsgrundsätze zu beseitigen oder außer Geltung zu setzen.

Spionage- und Proliferationsabwehr

In und gegen Deutschland sind fremde Nachrichtendienste mit zum Teil geheimen Mitteln und Methoden aktiv. Die Aktivitäten dieser Nachrichtendienste und die Herausforderungen, die sich daraus für die Spionageabwehr ergeben, sind vielfältig. Das primäre Ziel ausländischer Staaten ist es, sensible Informationen zu erlangen, z. B. aus den Bereichen Politik, Militär sowie Wirtschaft und Wissenschaft. Aber ausländische Dienste unterwandern auch Parteien oder Personen wie Oppositionelle oder Exilantinnen und Exilanten, werden staatsterroristisch tätig und betreiben Einflussnahme und Desinformation. Auch machen Staaten vor Beschaffung und Diebstahl von Komponenten und Technologien für Massenvernichtungswaffen (Proliferation) nicht Halt.

Die Spionage fremder Staaten beeinträchtigt die nationale Souveränität Deutschlands. Daher gehört es seit der Gründung des BfV am 7. November 1950 zu den zentralen Aufgaben des Dienstes, Spionageaktivitäten aufzudecken und zu verhindern. Die geopolitischen Verschiebungen der letzten Jahre in Verbindung mit der fortschreitenden Digitalisierung führen darüber hinaus zu einem sich zunehmend verstärkenden Kampf um die Meinungshoheit mittels Einflussnahme und Desinformation. Diese dienen dazu, die Kernelemente der freiheitlichen demokratischen Grundordnung infrage zu stellen und Deutschland zu destabilisieren.

Spionage und Konkurrenzausspähung

Auch Wirtschaftsspionage fällt in das Aufgabengebiet des Verfassungsschutzes – diese wird von fremden Staaten unter Einsatz nachrichtendienstlicher Methoden betrieben. Dies steht im Gegensatz zur sogenannten Konkurrenz- oder Industriespionage, bei der Unternehmen durch andere Unternehmen ausgespäht werden. Jedoch tarnen fremde Staaten ihre Wirtschaftsspionage auch durch halbstaatliche oder private Unternehmen: die Grenzen zwischen Wirtschaft und Staat verlaufen hier fließend.

Wirtschafts- und Wissenschaftsschutz

Wirtschaft und Wissenschaft in Deutschland sind aufgrund ihrer herausragenden Stellung Ziel vielfältiger Bedrohungen. Neben Terrorismus und gewaltbereitem Extremismus stellen insbesondere die Spionage, Sabotage und Einflussnahme durch staatliche Akteurinnen und Akteure aus dem Ausland ernst zu nehmende Gefahren für deutsche Unternehmen und Forschungseinrichtungen dar. Der Schutz der deutschen Wirtschaft und Wissenschaft ist Teil des gesetzlichen Präventionsauftrags des Verfassungsschutzes. Im Rahmen seiner **Präventionsmaßnahmen** informiert das BfV über eigene Erkenntnisse und Analysen, welche die Wirtschaft und Wissenschaft dabei unterstützen, sich eigenständig und effektiv vor den Gefahren von Ausspähung, Sabotage aber auch vor Bedrohungen durch Extremismus und Terrorismus schützen zu können.

In der Präventionsarbeit des BfV geht es insbesondere darum,

1. Gefahren, z. B. durch Spionage, besser verständlich zu machen und über beteiligte Akteurinnen und Akteure und angewandte Methoden zu informieren,

2. realistische Bedrohungsszenarien für ein effektives Risikomanagement zur Verfügung zu stellen

3. sowie Rückmeldungen und Erfahrungswissen aus Wirtschaft und Wissenschaft in den analytischen Prozess des Verfassungsschutzes einzubeziehen.

Wesentliche Erkenntnisse, die das BfV im Rahmen seines gesetzlichen Auftrags zusammen mit den Landesbehörden für Verfassungsschutz gewonnen hat, werden im jährlichen Verfassungsschutzbericht auch der Öffentlichkeit zugängig gemacht.

Die Berichte sind online unter **www.verfassungsschutz.de** einsehbar.

Wirtschafts- und Wissenschaftsschutz – Ihr Single Point of Contact

Das BfV verfügt über umfangreiche Erkenntnisse zu möglichen Angreifenden, ihren Zielen und Methoden und unterstützt Wirtschaft und Wissenschaft mit zielgruppengerechten Sensibilisierungsangeboten. Der Bereich Prävention (Wirtschafts- und Wissenschaftsschutz) innerhalb des BfV ist dabei zentrale Anlaufstelle für Unternehmen und Forschungseinrichtungen.

3 FRAGEN AN ...

Dr. Dan Bastian Trapp, Leiter des Referats Prävention in Wirtschaft, Wissenschaft, Politik und Verwaltung

Wo lauern aktuell die größten Gefahren für Unternehmen und Forschungseinrichtungen?

Deutsche Unternehmen und die Sicherheitsbehörden rechnen mit einer weiter anwachsenden Bedrohung durch Cyberangriffe und Spionage. Laut aktuellen Schätzungen liegt der Schaden bei mittlerweile über 200 Milliarden Euro. Aktuelle Zahlen belegen: Eine große Gefahr geht dabei von Social Engineering aus, über 48 % der Unternehmen waren wissentlich davon betroffen.

Wie können sich Unternehmen und Forschungseinrichtungen schützen?

Angriffe – egal ob analog oder digital – lassen sich nicht verhindern. Das Ziel muss sein, es den Angreifenden nicht unnötig leicht zu machen und sicherzustellen, dass ich Vorfälle rechtzeitig detektieren kann. Dazu müssen sensible Informationen identifiziert werden und sämtliche Unternehmensprozesse unter Sicherheitsgesichtspunkten analysiert werden, um praktikable Lösungen zu finden.

Welche Rolle spielt dabei das Personal?

Eine absolut zentrale Rolle! Die eigenen Beschäftigten sollten sowohl bei der Analyse als auch bei der Maßnahmenentwicklung unbedingt mit einbezogen werden. Sie sollen die Maßnahmen ja später auch umsetzen. Auch eine sicherheitssensible Führungskultur und eine hohe Zufriedenheit bei Mitarbeiterinnen und Mitarbeitern sind entscheidende Punkte, z. B. beim Schutz vor Innentäterschaft.

Geheim- und Sabotageschutz

Eine bedeutsame, jedoch in der Öffentlichkeit weniger bekannte Aufgabe des BfV ist der Geheim- und Sabotageschutz. Bestimmte sensible staatliche Informationen müssen vor einer Kenntnisnahme durch nicht befugte Personen geschützt werden. Dabei kommen sowohl personelle als auch materielle (organisatorische, bauliche und technische) Maßnahmen zum Einsatz, wie z. B. Sicherheitsüberprüfungen oder die Klassifizierung von Verschlusssachen.

Die vom BfV durchgeführte Sicherheitsüberprüfung ist ein zentrales Instrument des Sabotageschutzes im Bereich der Kritischen Infrastrukturen (KRITIS). Zweck ist es, Einrichtungen, die für das Gemeinwesen unverzichtbar sind, wie die Energieversorgung oder Telekommunikation, vor potenziellen Innentäterinnen und Innentätern zu schützen. Die Überprüfung soll sicherstellen, dass an besonders sicherheitsrelevanten Stellen keine Personen beschäftigt sind, bei denen Sicherheitsrisiken vorliegen.

Klassifizierungen von Verschlusssachen

Die Kenntnisnahme durch Unbefugte kann:

→ **STRENG GEHEIM**
den Bestand oder lebenswichtige Interessen der Bundesrepublik Deutschland oder eines ihrer Länder gefährden.

→ **GEHEIM**
die Sicherheit der Bundesrepublik Deutschland oder eines ihrer Länder gefährden oder ihren Interessen schweren Schaden zufügen.

→ **VS-VERTRAULICH**
für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder schädlich sein.

→ **VS-NUR FÜR DEN DIENSTGEBRAUCH**
für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig sein.

Die Sicherheits-überprüfung

Ziel einer Sicherheitsüberprüfung ist es, festzustellen, ob Personen sorgsam mit Informationen umgehen und kein Sicherheitsrisiko darstellen. Voraussetzung für eine Sicherheitsüberprüfung ist immer die Zustimmung der zu überprüfenden Person.

Die Sicherheitsüberprüfung von Beschäftigten in Unternehmen oder Behörden richtet sich nach dem Sicherheitsüberprüfungsgesetz. Dieses sieht eine Überprüfung nur dann vor, wenn:

- das Unternehmen geheimschutzbetreut ist und im Rahmen eines staatlichen Auftrags mit Verschlusssachen arbeitet
- oder es sich um Schlüsselstellen in Unternehmen der KRITIS handelt.

Arten von Sicherheitsüberprüfungen

Einfache Sicherheitsüberprüfung
Die einfache Sicherheitsüberprüfung wird bei Personen durchgeführt, die Zugang zu „VS-VERTRAULICH“ eingestuften Verschlusssachen haben oder ihn sich verschaffen können oder Tätigkeiten in einer Nationalen Sicherheitsbehörde wahrnehmen sollen.

Erweiterte Sicherheitsüberprüfung
Die erweiterte Sicherheitsüberprüfung wird bei Personen durchgeführt, die Zugang zu „GEHEIM“ eingestuften oder einer hohen Anzahl von „VS-VERTRAULICH“ eingestuften Verschlusssachen haben oder ihn sich verschaffen können sowie bei Personen, die in einer lebens- und verteidigungswichtigen Einrichtung oder im Bundesverteidigungsministerium tätig werden sollen.

Erweiterte Sicherheitsüberprüfung mit Sicherheitsermittlungen
Diese Art der Sicherheitsüberprüfung wird bei Personen durchgeführt, die Zugang zu „STRENG GEHEIM“ eingestuften oder einer hohen Anzahl von „GEHEIM“ eingestuften Verschlusssachen haben oder ihn sich verschaffen können sowie bei Personen, die bei einem Nachrichtendienst des Bundes oder einer vergleichbaren Einrichtung Tätigkeiten wahrnehmen sollen.

Folgende Feststellungen können einem Einsatz in sicherheitsempfindlicher Tätigkeit entgegenstehen:

- Zweifel an der persönlichen Zuverlässigkeit (z. B. wegen begangener Straftaten oder Drogenmissbrauchs).
- Eine besondere Gefährdung der betroffenen Person, insbesondere die Besorgnis der Erpressbarkeit bei möglichen Anbahnungs- oder Werbungsversuchen durch ausländische Nachrichtendienste, kriminelle, extremistische oder terroristische Organisationen (Überschuldung ist bspw. ein geeigneter Ansatz, die betroffene Person gegen Bezahlung zu einem Geheimnisverrat zu bewegen).
- Zweifel am Bekenntnis zur freiheitlichen demokratischen Grundordnung (z. B. bei extremistischer Betätigung).

Für Unternehmen und Forschungseinrichtungen, die nicht unter einen Anwendungsfall des Sicherheitsüberprüfungsgesetzes fallen, ist für kritische Positionen die Durchführung von geeigneten **Pre-Employment-Screenings** anzuraten.

Oft helfen schon **Plausibilitätsprüfungen** des Lebenslaufes, Hinweise auf Unregelmäßigkeiten zu detektieren.

Verfassungsschutz – stark im Verbund

Die Bundesrepublik Deutschland ist ein föderaler Bundesstaat. Diesem Prinzip folgend, verfügt jedes der 16 Bundesländer über eine eigene Verfassung und auch über eine eigene Landesbehörde für Verfassungsschutz. Diese sind zuverlässige Partner im Bereich der inneren Sicherheit vor Ort. Gemeinsam mit dem BfV bilden sie den Verfassungsschutzverbund, in dem das BfV die Zentralstellenfunktion übernimmt.

Auch im Bereich des präventiven Wirtschaftsschutzes arbeiten die zuständigen Landesbehörden vernetzt und stehen im regelmäßigen Austausch. Auf diese Weise entsteht ein starkes Netzwerk bis zu den Unternehmen vor Ort. Unser Tipp: Nehmen Sie unabhängig von einem konkreten Verdachtsfall schon einmal Kontakt zum Wirtschaftsschutzbereich Ihrer Landesbehörden für Verfassungsschutz auf. Wenn die Kommunikationswege etabliert sind, kann der Kontakt im Notfall schneller hergestellt werden.

Eine Übersicht über die einzelnen Verfassungsschutzbehörden gibt es unter **www.wirtschaftsschutz.info**.

Jederzeit ansprechbar ist auch der Bereich Wirtschaftsschutz des BfV unter **wirtschaftsschutz@bfv.bund.de** oder **030 18792-3322**.

Kontrolle

An die Arbeit des BfV werden strenge rechtsstaatliche Maßstäbe gelegt. Neben der Verwaltungskontrolle sollen die parlamentarische, die gerichtliche und die öffentliche Kontrolle sicherstellen, dass der Verfassungsschutz ausschließlich im Rahmen seiner Befugnisse und Kompetenzen arbeitet. Das Schaubild zeigt die unterschiedlichen Kontrollmechanismen. Nähere Informationen finden Sie auch auf **www.verfassungsschutz.de**

Allgemeine Kontrolle

- Debatten im Bundestag
- Kleine und Große Anfragen
- Regelmäßige Berichte von Innen- und Haushaltsausschuss, ggf. Untersuchungsausschuss
- Petitionen

Besondere Kontrolle

- Parlamentarisches Kontrollgremium (PKGr)
- Regelmäßige Berichte, ggf. Untersuchungsausschuss
- Petitionen

G 10-Kontrolle G 10-Kommission

- Entscheidung über Maßnahmen zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses
- Vier Mitglieder vom PKGr bestellt

Bundesamt für Verfassungsschutz (BfV)

Verwaltungskontrolle

- Bundesministerium des Innern und für Heimat (BMI - Dienst- und Fachaufsicht)
- Bundesbeauftragter für den Datenschutz und die Informationsfreiheit

Öffentliche Kontrolle

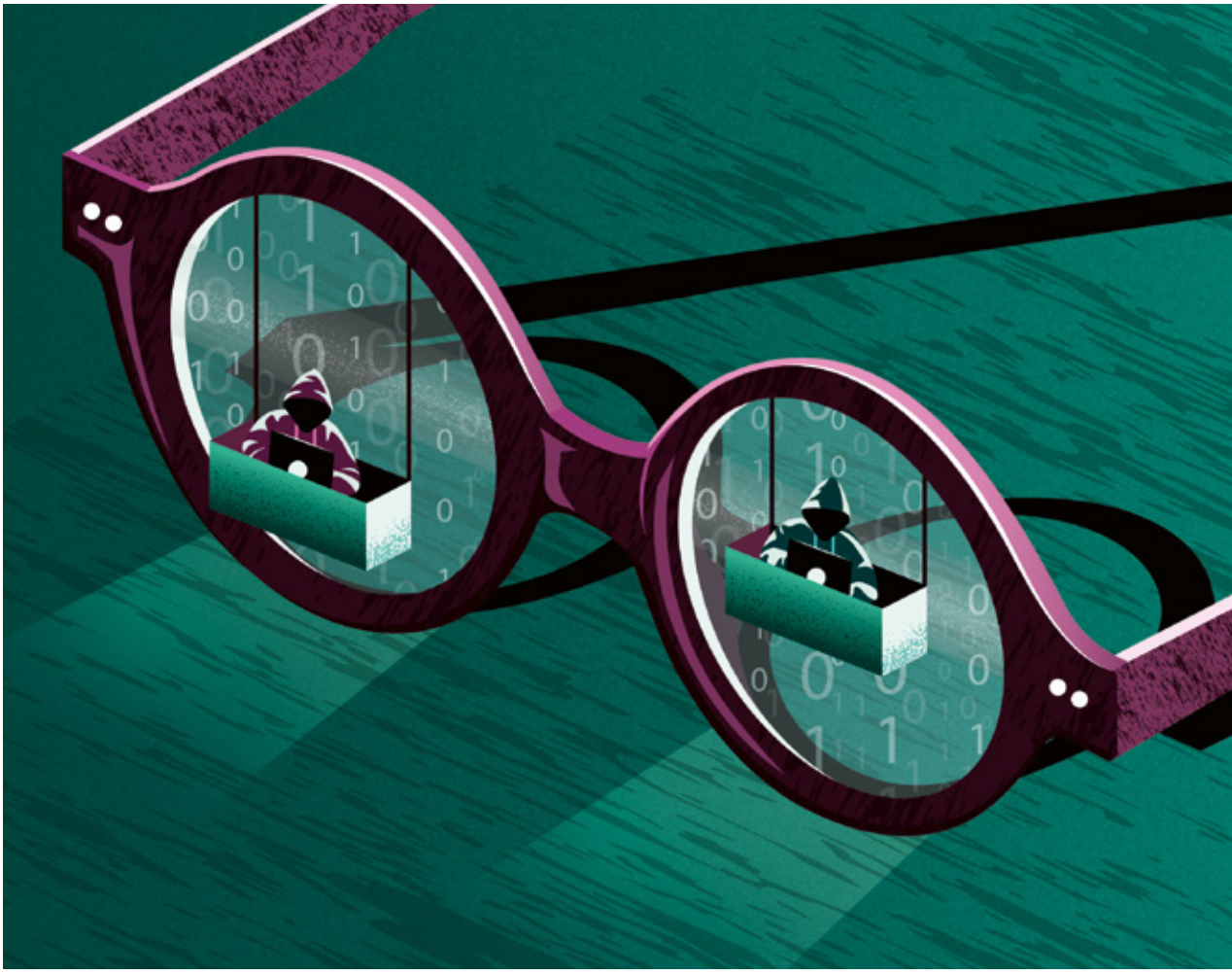
- Bürgerinnen und Bürger (Eingaben, Anfragen, Auskunftsrecht)
- Presse (Berichte, Anfragen)

Gerichtliche Kontrolle

- Klagen gegen Maßnahmen des Verfassungsschutzes

Bildcredits

S. 21 Bundesamt für Verfassungsschutz (BfV), S. 23 Unsplash/@theasophie, S. 24 Markus Winkler, S. 26 Bundesamt für Verfassungsschutz (BfV), S. 27 Brian A. Jackson, S. 28 izusek/istockphoto, S. 30 Clay Banks, S. 32 Bundesamt für Verfassungsschutz (BfV)



Professor Who?

Wie falsche Professorinnen und Professoren Forschende ausspionieren

Redaktion: Cyberabwehr **Illustration:** Joana Schulze

IT-Sicherheitsforschende ordnen Nordkorea mehrere Gruppen von Hackerinnen und Hackern zu, die seit Jahren weltweit groß angelegte Spionagekampagnen gegen Industriebetriebe fahren und gezielt Kryptobörsen angreifen. Im Schatten dieser spektakulären Fälle fanden die Aktivitäten der nordkoreanischen Gruppierung Kimsuky bisher wenig Beachtung. Dabei nehmen die Hackerinnen und Hacker insbesondere Forschende ins Visier und richten durch das Ausspähen von Informationen einen politischen Schaden an, der nur schwer zu beziffern ist.

Auf der ganzen Welt sammelt die APT Kimsuky – auch bekannt als Velvet Chollima oder Konni Group – Informationen, die dem nordkoreanischen Regime in seiner besonderen Lage als international isolierter Staat dienlich sind. Dazu gehören interne Strategiepapiere von Außenministerien genauso wie Dokumente mit Forschungs- sowie Expertinnen- und Expertenwissen, von denen das Land aufgrund der verhängten Sanktionen abgeschnitten ist. So stehen neben akademischen und diplomatischen Zielen auch Nichtregierungsorganisationen und Think Tanks auf der Angriffsliste der Hackerinnen und Hacker.

Die Anbahnung

Eine häufig bei Kimsuky-Kampagnen beobachtete Vorgehensweise ist das „Spear-Phishing" mit „gespooften" E-Mail-Adressen.

> *(Spear-)Phishing: Unter dem Begriff Phishing versteht man Versuche, mittels gefälschter Webseiten, E-Mails oder Kurznachrichten an persönliche Daten von Internetnutzerinnen und Internetnutzern, insbesondere Log-in-Informationen, zu gelangen. Sobald Angreifende es gezielt auf bestimmte Personen, Unternehmen oder Organisationen abgesehen haben, spricht man von Spear-Phishing.*

Beim E-Mail-Spoofing werden zunächst E-Mail-Adressen angelegt, deren Absenderadressen bekannten Behörden, Unternehmen oder Einzelpersonen ähneln. Die Hackerinnen und Hacker von Kimsuky wählten hier zum Beispiel reale Personen, die auf einem bestimmten Fachgebiet Bekanntheit genießen. Darunter befanden sich in der Vergangenheit südkoreanische Politikexpertinnen und Politikexperten wie Professor Moon Chung-in, ein Berater des ehemaligen südkoreanischen Präsidenten Moon Jae-in, sowie langjährig tätige russische Diplomatinnen und Diplomaten. Bei der anschließenden Kontaktaufnahme mit den Opfern wird vorgegeben, an einem fachlichen Austausch interessiert zu sein, oder die Einschätzung zu einem wissenschaftlichen Paper erbeten. Professorinnen und Professoren als Absendende gespoofter E-Mail-Adressen bieten sich bei diesem Vorgehen im besonderen Maße an, da ihre Arbeiten häufig publiziert und die vermeintliche Anfrage zum akademischen Austausch durchaus als Wertschätzung interpretiert werden kann.

Kompromittierung des Opfersystems

Nach erfolgreicher Kontaktaufnahme versendet Kimsuky oftmals ein Köderdokument. Auf den ersten Blick normale PDF- oder Word-Dokumente im zum vermeintlich Absendenden passenden Erscheinungsbild. Opfer aus Diplomatie und Politik erhalten so Dokumente im nachgeahmten offiziellen Layout eines Ministeriums; Forschende erhalten häufig Einladungen oder Agenden für Fachkonferenzen. Tatsächlich enthalten die Dokumente aber schädliche Funktionen oder laden diese über maliziöse „Makros" aus dem Internet nach – eine sogenannte „Remote Template Injection".

Die vor der Ausführung von Makros erscheinenden Schutzdialoge von Microsoft Office werden von den Opfern in der Regel weggeklickt, weil sie der Absenderin oder dem Absender der E-Mail vertrauen. Nach erfolgreicher Kompromittierung durch die Malware versuchen sich die Hackerinnen und Hacker möglichst lange im System des Opfers zu bewegen, um Informationen zu sammeln.

> *Makro: Ein Makro ist eine zusammengefasste Folge von Anweisungen oder Deklarationen, um diese mit nur einem einfachen Aufruf ausführen zu können. Im Fall von Office-Dokumenten dient ein Makro bspw. der automatisierten Durchführung wiederkehrender Arbeitsabläufe. Jedoch kann ein Makro auch zur Ausführung schadhafter Aktionen missbraucht werden.*

Credential-Phishing

Neben dem Einsatz von Malware greift Kimsuky auch auf „Credential-Phishing" zurück, eine Spielart des Phishings, die auf die Erbeutung von Zugangsdaten abzielt.

Der Ablauf des Angriffs ist bis zur Übersendung des Köderdokuments gleich. Doch statt eines Dokuments wird der Link zu einer von der Gruppierung erstellten Webseite übersendet, die das Erscheinungsbild einer echten Webseite wie etwa die Anmeldemaske einer Universität nachahmt. Folgt das Opfer dem Link, wird es aufgefordert, die persönlichen Log-in-Informationen einzugeben, die von den Hackerinnen und Hackern im Hintergrund ausgelesen und dokumentiert werden. So erhält Kimsuky nicht nur Zugang zu internen Informationen, sondern auch häufig zu E-Mail-Konten, die sie für weitere Angriffe nutzen.

Ausblick

Es ist davon auszugehen, dass Kimsuky im Sinne seines Auftraggebers weiter auf die Jagd nach Informationen geht. Die Gruppe ist seit mehreren Jahren aktiv und bekannt für ihre Kreativität und Methodenvielfalt. Dabei haben die Hackerinnen und Hacker immer wieder großes Interesse an einem breiten Opferspektrum bewiesen, was bevorstehende Angriffe kaum branchenspezifisch voraussagen lässt.

Lars Findorff (rechts) im Gespräch mit Dr. Dan Bastian Trapp (BfV)

Chancen und Risiken

Interview mit Lars Findorff von der TRUMPF-Gruppe

Q.ANT, das Tochterunternehmen des Hochtechnologieunternehmens TRUMPF, ist eines der führenden deutschen Unternehmen und Hidden Champion bei industriellen Produkten, die auf Quantentechnologie basieren. Erst im Mai 2022 hat das Start-up aus Stuttgart ein Photonik-Chip-Verfahren vorgestellt, durch das sich die heute etablierten elektronischen Großrechner schon in wenigen Jahren um Prozessoren erweitern lassen, die mit modernster Quantentechnologie arbeiten. Im Gespräch mit Lars Findorff, Leiter der Unternehmenssicherheit bei der TRUMPF-Gruppe, sprach das SPOC-Magazin über Sicherheitskultur im Wandel und den wachsenden Herausforderungen insbesondere für KMUs.

Herr Findorff, wann können wir mit dem ersten Quantencomputer rechnen?

Die Auszeichnung der Quantenphysiker Alain Aspect, John F. Clauser und Anton Zeilinger in diesem Jahr mit dem Physik-Nobelpreis macht das Thema gerade sehr präsent und es entsteht das Gefühl, dass es in wenigen Monaten oder Jahren so weit wäre. Das ist jedoch nicht zu erwarten. Die Entwicklung einer solch komplexen Technologie braucht sehr viel Zeit. Im Bereich der Quantensensorik hingegen, auf den sich Q.ANT konzentriert, wird es in den nächsten Jahren neue Produkte und Anwendungsbereiche geben. Wir haben bereits funktionsfähige Produkte am Markt. Deutlich früher als ein universeller Quantencomputer wird wohl ein Quantenrechner für spezielle Anwendungen verfügbar sein, der als Begleitcomputer in Hochleistungsrechenzentren eine Rolle spielen kann.

Was macht Ihren Ansatz so besonders?

Der von Q.ANT entwickelte Quantenchip funktioniert auf Basis photonischer Quantentechnologie, also auf Basis von Licht. Der größte Vorteil dieser Technologie ist, dass ein solcher Chip fast ohne zusätzliche Kühlung betrieben werden kann.

Und in welchen Bereichen sehen Sie am ehesten Einsatzmöglichkeiten für diese Technik?

Wenn der Quantenchip fertig ist, wird er am ehesten in den Bereichen Industrie, Wirtschaft und Forschung eine Rolle spielen. Wir haben bereits einen quantenbasierten Industriesensor marktfähig und arbeiten derzeit an weiteren Anwendungsfällen.

Mit dem Fortschritt der Quantentechnologie erhöht sich auch das Risiko für Cyberangriffe. Es droht die Gefahr, dass bestimmte Sicherheitsmaßnahmen mit dem Aufkommen von Quantencomputern über Nacht obsolet werden. Können Sie da Entwarnung geben?

Entwarnung kann ich nicht geben, jedoch beruhigen. Wie erwähnt, ist die Entwicklung der Quantentechnologie ein Prozess, der lange dauern wird und in dem wir auch die Gelegenheit bekommen werden, unsere Schutzmaßnahmen anzupassen. Nichtsdestotrotz müssen wir das Thema heute schon mitdenken.

Zum jetzigen Zeitpunkt finde ich es viel problematischer, dass immer noch viele Unternehmen, insbesondere KMUs, ihre Systeme nicht einmal vor den derzeitigen Bedrohungen bestmöglich schützen. Insofern würde ich immer den Fokus auf die Bedrohungen, die aktuell da sind, legen, gepaart mit einem guten Blick in die Zukunft und dem Anspruch, das Schutzkonzept immer auf einem aktuellen Stand zu halten.

» **Unternehmen müssen Schutzmaßnahmen stets aktuell halten und fortentwickeln.** «

Springen wir dennoch kurz in die Zukunft. Wie werden sich aus Ihrer Sicht die Sicherheitsanforderungen von Unternehmen mit dem Aufkommen von Quantencomputertechnologie verändern?

Die Quantentechnologie wird uns bei den Sicherheitsanforderungen vor enorme Herausforderung stellen; unter anderem wird ein Teil unserer derzeitigen Verschlüsselungsverfahren untauglich werden. Sie wird aber auch neue Möglichkeiten eröffnen, wie zum Beispiel die Entwicklung neuer Verschlüsselungsverfahren. Auch jetzt stehen schon quantensichere Verschlüsselungsverfahren zur Verfügung, die zumindest der ersten Generation von Quantencomputern standhalten dürften.

Es gibt also Chancen und Risiken. Unternehmen müssen die Zeit nutzen, Schutzmaßnahmen aktuell zu halten und fortzuentwickeln.

Wie muss eine Sicherheitsarchitektur heutzutage mit der immensen Bedrohung beispielsweise durch Ransomware gedacht werden. Was sind die drei wichtigsten Aspekte?

Ein Aspekt ist die konsequente Zusammenarbeit der verschiedenen Sicherheitsabteilungen. Der Austausch dieser Abteilungen muss perfekt funktionieren. Nur so werden wir in der Lage sein, mit

Foto: Unternehmen TRUMPF

den enormen Sicherheitsherausforderungen der Zukunft durch die immer komplexer werdenden Angriffe umzugehen und darauf adäquat und frühzeitig reagieren zu können.

Ein anderer wichtiger Aspekt ist das Thema Awareness. Ein geringes Sicherheitsbewusstsein von Mitarbeiterinnen und Mitarbeitern ist ein Thema, das niemals ausgeschlossen werden kann. Insofern gilt es, langfristig neue und kreative Ideen zu entwickeln, um bei Mitarbeiterinnen und Mitarbeitern immer wieder einen Impuls zu setzen und Aufmerksamkeit zu erzeugen.

Und letztendlich dreht sich beim Thema Sicherheitsarchitektur alles um Risikomanagement. Die vorhandenen Maßnahmen – und dazu gehören aus meiner Sicht nicht nur jene, die uns vor Cyberangriffen schützen sollen, sondern alle, die dem Schutz und der Sicherheit des Unternehmens dienen – müssen zur Unternehmensstrategie passen. Es sollte ein ganzheitlicher, flexibler Ansatz sein, der nicht nur reaktiv, sondern auch präventiv wirksam ist.

Es klingt bei Ihnen schon durch, Unternehmenssicherheit wird zunehmend komplexer. Komplexität behindert jedoch häufig das Umsetzen von Sicherheitsmaßnahmen auch durch die Beschäftigten. Wie nehmen Sie Mitarbeiterinnen und Mitarbeiter bei so etwas mit?

Wir erleben gerade im Zuge der Digitalisierung, dass Mitarbeiterinnen und Mitarbeiter auch private Endgeräte mit ins Unternehmen bringen und mit diesen auch im Unternehmensnetzwerk unterwegs sind; oder sich im Rahmen des mobilen Arbeitens von irgendwo auf der Welt ins Unternehmensnetz einloggen wollen. Sofern das unkontrolliert passiert, ist das eine erhebliche Gefahr für Unternehmen. Die Mitarbeiterinnen und Mitarbeiter jedoch wollen nicht mehr darauf verzichten. Die Fortentwicklung dieser Technologien schafft damit Tatsachen, auf die wir als Unternehmen reagieren müssen. Und das kann meiner Meinung nach nicht ausschließlich durch Verbote passieren. Im Gegenteil, das muss in einem sicheren Rahmen zulässig und damit in den Schutzmaßnahmen abgebildet sein. Insofern kommt dabei neben den ganzen technischen Sicherungsmaßnahmen dem Thema Awareness wieder eine besondere Bedeutung zu.

Unternehmen der TRUMPF-Gruppe sind auch in verschiedenen Netzwerken eingebunden. National ist da zum Beispiel die TRUMPF Hüttinger als Mitglied des Branchenverbandes Silicon Saxony zu nennen. Wie wird sich dort auch zu Themen wie Know-how-Schutz oder Cybersecurity ausgetauscht? Und wie stellen Sie den effektiven Austausch zwischen den einzelnen Bereichen auch innerhalb des TRUMPF-Netzwerks sicher?

Das Thema Austausch und Netzwerken halte ich für alternativlos. Insbesondere die letzten beiden Jahre während der Pandemie haben gezeigt, wie wichtig ein gutes Netzwerk ist. Dabei sind die kleineren Zusammenschlüsse oft von guter Qualität. Aus einer Bosch-Initiative heraus gibt es hier zum Beispiel den Stuttgarter Sicherheitskreis, eine Zusammenkunft von Unternehmen, die alle im Großraum Stuttgart ihren Sitz haben. Mit denen tauschen wir uns in sehr kleinem Kreis vertrauensvoll aus.

Im großen Kreis und auf Behördenseite ist insbesondere der Austausch mit dem BKA zum Beispiel im Rahmen der Global-Player-Initiative und mit dem BfV, beziehungsweise dem LfV Baden-Württemberg (BW) zu nennen. Aber auch der „Sicherheitstag“ des BMI / BDI ist eine wichtige Netzwerkveranstaltung. Auch die Arbeiten in den Gremien, wie zum Beispiel des ASW-BW, dort sitze ich im Vorstand, oder die Arbeit des ASW Bundes halte ich für wichtig und uneingeschränkt unterstützenswert.

Gute Sicherheit kostet; zumindest die wirksame Sicherheit. Zusätzlich macht sich gerade im Bereich Cybersecurity ein gehöriger Fachkräftemangel bemerkbar. Macht es Sinn, dass sich KMUs gegenseitig beim Thema Know-how-Schutz unterstützen?

Ich glaube, das Thema Kooperation kommt mit ganz großen Schritten auf uns zu. Sie haben es angesprochen: Fachkräftemangel. Dieses Thema haben wir sehenden Auges in Kauf genommen. Denn vor zwanzig Jahren hätten wir bereits damit planen können, dass die Babyboomer-Generation jetzt bereit ist, in Rente und Pension zu gehen. Wir haben derzeit schon die Lage, dass wir insbesondere hoch qualifizierte Fachkräfte im Sicherheitsbereich kaum noch bekommen. Das wird in den nächsten Jahren nicht besser werden. Verknüpft mit der Aussicht, dass die allgemeine Sicherheitssituation komplexer werden wird, droht hier ein enormes Problem. Wir werden also in eine Mangelverwaltung gehen. Das wird ausnahmslos alle Unternehmen betreffen. Ich sehe hier großes

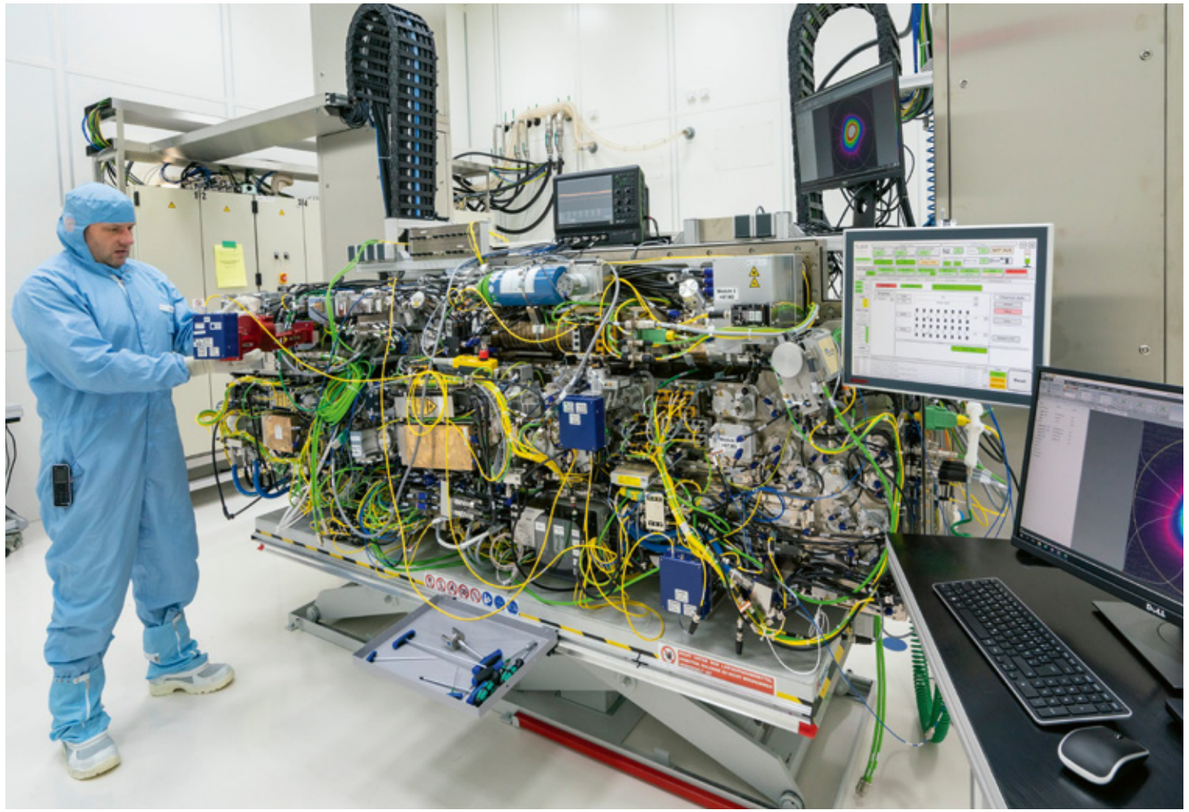
Potenzial, dass sich KMUs gegenseitig unterstützen. Es gibt bereits erste Ansätze, bei denen sich Unternehmen zusammentun und in Projekten gemeinsam arbeiten. Das ist aber noch nicht die Regel. Bis jetzt versuchen sich vermutlich die meisten vor allen Dingen allein vor Know-how-Abfluss zu schützen.

Welche Unterstützung erwarten Sie von der Politik oder den Sicherheitsbehörden?

Ich bin sehr froh über die Unterstützung und den Austausch, den die Landesbehörden für Verfassungsschutz, das BfV und auch das BMI / BDI möglich machen. Auch beim Thema Wirtschaftsschutz gibt es bereits viele Angebote. Ich glaube aber, dass es notwendig ist, das Thema Wirtschaftsschutz wichtiger zu nehmen und die Verantwortung dafür zentral zu organisieren.

Große Unternehmen und gut aufgestellte KMUs haben jetzt schon die Möglichkeit, Informationen

Foto: Unternehmen TRUMPF



zu erhalten und sich auszutauschen. Ich glaube, es gibt aber eine ganze Menge kleiner KMUs, die bisher wenig Möglichkeit zum Austausch oder diese Themen gar nicht auf dem Schirm haben, sodass wir dort die Anstrengungen enorm erhöhen müssen. Und auch in der Start-up-Szene müssen wir von Anfang an für ein Sicherheitsbewusstsein sorgen und die Unternehmen mit in das Thema Wirtschaftsschutz einbinden. Es gibt viele Start-ups, die nur eine einzige Idee haben, mit der sie unterwegs sind. Und wenn die weg ist, ist ihr Business weg.

Auch die akademische Forschung lebt von der Kooperation, dem freien Austausch von Ideen. In bestimmten Bereichen sehen wir Entwicklungen, dass Länder wie beispielsweise China, diese Forschungsfreiheit einseitig ausnutzen, um möglichst schnell an Wissen zu kommen. Wie gehen Sie in internationalen Forschungskooperationen mit diesem Spannungsfeld um?

Bei TRUMPF sehen wir natürlich, dass uns das jetzt zumindest teilweise das Leben schwerer macht. Auf der anderen Seite sind Unternehmen wie TRUMPF auf den Austausch angewiesen, auf globale Handelsstrukturen und suchen diese auch aktiv. Das ist ein ganz sensibles Thema und wir verwenden viel Energie darauf, jetzt und auch zukünftig darüber nachzudenken, mit wem wir wie eng kooperieren und gemeinsam forschen wollen.

Gerade in Bezug auf Sicherheit haben Unternehmen und Forschungseinrichtungen häufig eine unterschiedliche Kultur. Welche Wege beschreiten Sie in der Kooperation mit Forschungseinrichtungen?

Dass Forschungseinrichtungen das Thema Sicherheit nicht als Hauptfokus haben, finde ich verständlich. Es ist an uns, dort in den nächsten Jahren für ein Umdenken zu sorgen und das Thema Sicherheit mit auf die Agenda zu bringen, bevor Kooperationen eingegangen werden. Meiner

Fotos: Unternehmen TRUMPF

Meinung nach geht es nur mit einem Mindeststandard von Sicherheitsmaßnahmen in Bezug auf Know-how-Schutz. Wir müssen uns genau überlegen, was wir an Informationen weggeben und wann der richtige Zeitpunkt ist, die Kooperation wieder einzuschränken, um Know-how-Abfluss zu verhindern.

Ein weiterer schwieriger Bereich ist der Umgang mit Stellenbewerbungen. Jetzt, mit dem Angriffskrieg Russlands auf die Ukraine steht vor allem die Frage im Raum, wie Unternehmen oder Forschungseinrichtungen mit russischen Bewerberinnen und Bewerbern umgehen. Welchen Rat würden Sie geben?

Ich empfehle, einen Pre-Employment-Check als Prozess aufzusetzen. Dazu bedarf es vorher einer Kategorisierung von Positionen im Unternehmen und die Festlegung, was im Vorfeld einer Einstellung abgeprüft werden soll. Das ist dann abhängig von der jeweiligen Position, die bekleidet werden soll, welche Zugriffe im Unternehmen und auf welche Daten damit einhergehen.

Was glauben Sie, welche maßgeblichen Veränderungen in der Sicherheitsbranche stehen uns innerhalb der nächsten fünf Jahre bevor?

Aus meiner Sicht ist das einzige Stabile die Gewissheit, dass es nicht einfacher wird. Das, was wir gerade an Veränderung im Sicherheitsbereich erleben, wird sich fortsetzen. Das bedeutet, dass wir uns ständig mit neuen Bedrohungslagen und -szenarien auseinandersetzen werden müssen.

Man braucht keine Kristallkugel, um festzustellen, dass Spannungen zwischen einzelnen Ländern auch weiterhin zur Tagesordnung gehören werden. Und vielleicht werden wir intensive Spannungen oder gar Kriegszustände erleben – was ich nicht hoffe.

Das Thema Physical Security wird wieder stärker in den Fokus rücken. Jahrelang lag der Fokus auf Gefahren, die durch Cyberattacken entstehen können. Jetzt, nach den Anschlägen auf die Gaspipelines oder auch auf die Deutsche Bahn merken wir, dass die Risiken für Kritische Infrastruktur nicht ausschließlich aus dem digitalen Raum hervorgehen. Die Angriffe auf Unternehmen werden weiterhin zunehmen und komplexer werden. Deswegen werden wir unsere Schutzkonzepte weiterentwickeln müssen. Das sollte sich zukünftig auch in der Gesamtheit der Gefahrenbetrachtung wiederfinden.

Wo sehen Sie die größte Herausforderung?

Ganz klar im Schutz Kritischer Infrastruktur.

Herr Findorff, vielen Dank für das Gespräch.

Auf fremdem Boden und rauer See

SICHERHEIT AUF GESCHÄFTSREISEN

Redaktion: Wirtschaftsschutz **Illustration:** Sonja Marterner

Schnell und zielstrebig durchsuchen die fünf Personen das Hotelzimmer. Nehmen alle möglichen Verstecke präzise in Augenschein, fotografieren vorgefundene Dokumente. Begleitet nur von einer Reinigungskraft hinterlassen sie das Zimmer ohne Spuren, wie vom Zimmerservice aufbereitet. Lediglich ein USB-Stick und ein für die landestypische Steckdose passendes Smartphone-Ladegerät werden als Aufmerksamkeit des Hauses platziert. Es geht schnell, eine Standardvorgehensweise beim chinesischen Inlandsnachrichtendienst angewendet bei ausgewählten Geschäftsreisenden, Journalistinnen und Journalisten, Gastforschenden und sogar Diplomatinnen und Diplomaten. Die hinterlassenen „Willkommensgeschenke“ sind Spionage-Tools, in der Lage angeschlossene Geräte unbemerkt zu durchsuchen und Informationen zu erbeuten.

Insbesondere China und Russland besitzen enorme Ressourcen, um innerhalb ihres Staatsgebiets flächendeckend nachrichtendienstlich zu agieren. Und während in Deutschland geheimdienstliche Agententätigkeit strafbar ist, stehen China und Russland im eigenen Land rechtlich und physisch weitreichende Aufklärungsmöglichkeiten zur Verfügung. Das gilt auch für nachrichtendienstliche Aktivitäten in befreundeten oder abhängigen Staaten. Bislang jedoch fand fremdstaatlicher Zugriff auf in China und Russland agierende deutsche Unternehmen oder Geschäftsreisende in einem überschaubaren Umfang statt. Mögliche politische Konsequenzen und ein Interesse an diplomatischer Gesichtswahrung waren in vielen Fällen wohl begrenzender Faktor für zu offensichtliche Ausspähaktivitäten. Doch es entwickelt sich zunehmend ein Klima, in dem politische Rücksichtnahme und diplomatische Korrektheit weniger wichtig sind. Gleichermaßen erhöht die zunehmende Distanz den Bedarf an Informationen; und China und Russland haben gerade in wirtschaftlicher Hinsicht ambitionierte Ziele. Betriebsgeheimnisse deutscher Technologieunternehmen im Bereich der IT, Telekommunikation, Militärtechnik, Fahrzeugtechnik, Automatisierung, Robotik, Luftfahrt, Energieversorgung, maritimer Ausrüstung, Biopharma und Landwirtschaft sind somit von großem Interesse – auch für viele andere autoritäre Staaten.

Methoden nachrichtendienstlicher Informationsgewinnung

Zur Informationsgewinnung wenden Nachrichtendienste hauptsächlich die folgenden drei Methoden an:

> ***Human Intelligence (HUMINT)*** *ist die Gewinnung von Informationen mittels menschlicher Quellen. Dabei werden Zielpersonen u. a. danach ausgewählt, welchen Zugang sie zu Informationen haben. Nachrichtendienste wenden zahlreiche Methoden an, sie zu einer Mitarbeit zu bewegen. Gewonnene Erkenntnisse werden z. B. als Kompromat – also als kompromittierende Information über eine Person – als Druckmittel zur Zusammenarbeit eingesetzt.*
>
> ***Open Source Intelligence (OSINT)*** *bezeichnet die Informationsgewinnung aus offenen Quellen, wie z. B. Internetseiten, Social-Media-Kanälen oder Blogs. Das Anlegen und Nutzen fiktiver Social-Media-Profile kann zur legendierten Kommunikation eingesetzt werden.*
>
> ***Signals Intelligence (SIGINT)*** *sind Informationen, die durch das Abfangen von Telekommunikationssignalen oder anderen elektronischen Übertragungsweisen gewonnen und genutzt werden.*

Technische Aufklärung gehört aufgrund ihrer effizienten und ressourcenschonenden Einsetzbarkeit zum wahrscheinlichsten Angriffsszenario während Geschäftsreisen.

Angriffsvektoren

In China müssen Geschäftsreisende grundsätzlich davon ausgehen, ausspioniert zu werden, insbesondere durch technische Mittel. Der Zugriff kann, wie eingangs geschildert, über zur Verfügung gestellte Ladekabel oder USB-Sticks erfolgen, auch können Hotelzimmer abgehört und kameraüberwacht werden. Bei der Einreise in die Xinjiang-Region installieren chinesische Grenzpolizistinnen und Grenzpolizisten seit einiger Zeit gar eine Spionage-App auf Smartphones. Im vorgeschobenen Zuge der Überwachung der uigurischen Minderheit prüft die App namens BXAQ oder Fengcai (gesprochen Fung-tsai) Kontakte, Nachrichten, Dateien und Bilder auf relevante Inhalte. Ganz allgemein bergen Einreisekontrollen in autoritäre Staaten ein besonderes Risiko. Insbesondere am Flughafen haben ausländische Nachrichtendienste viele Anknüpfungspunkte, in dessen Fokus, wie in Xinjiang, Smartphones der Reisenden sind. Denn für die gibt es kaum Schutzmöglichkeiten. Selbst Kryptierungen können die Auswertung der Inhalte oft nicht verhindern, vielmehr ermutigen sie Sicherheitskräfte genauer hinzusehen. In einigen Ländern bestehen zudem klare gesetzliche Restriktionen für die Verschlüsselung von Daten.

> *SICHERHEITSHINWEIS: Wir empfehlen für die Einreise den Verschluss Ihres Smartphones in einem SafeBag. Der Siegelverschluss dieser Plastikbeutel lässt sich ohne Beschädigung nicht öffnen und verrät Ihnen, wenn sich jemand an Ihrem Gerät zu schaffen gemacht hat.*

Neben der technischen Aufklärung haben Nachrichtendienste zudem etliche Methoden entwickelt, Informationen durch Befragungen und Observierungen zu gewinnen; mittels subtiler unbemerkter Ausspähungen bis hin zu offensiven und direkten Konfrontationen und angedrohten Diskreditierungen. Dabei hat sich die Quantität und Qualität der Methoden in den vergangenen Jahren gleichsam mit der voranschreitenden Digitalisierung weiterentwickelt. Social-Media und allgemein die digitale Infrastruktur ermöglichen den Nachrichtendiensten einen tiefen und oftmals leichten Zugriff auf Informationen. So ist unter anderem das „Honey Trapping“, die von einem Nachrichtendienst gezielt gesteuerte Kontaktaufnahme im Rahmen von Onlinedating nach wie vor ein probates Instrument der Informationsgewinnung, insbesondere zur Nutzung als Kompromat.

Empfehlungen für Ihre Reisesicherheit

Die Entwicklung eines Schutzkonzepts für Auslandsreisen ist eine dezidierte Empfehlung des Bundesamtes für Verfassungsschutz (BfV). Bereits die Sensibilisierung und Schulung von Mitarbeiterinnen und Mitarbeitern kann die Sicherheit auf Geschäftsreisen erhöhen.

Unsere Sicherheitscheckliste:

vorab

- Informieren Sie sich über die aktuelle **Sicherheitslage im Zielland**. Auf der Webseite des Auswärtigen Amtes sowie in dessen Reise-App finden Sie für alle Länder aktuelle Reise- und Sicherheitshinweise.

Tipps zur Reisesicherheit bietet die Reise-App des Auswärtigen Amtes.

auswaertiges-amt.de/de/app-sicher-reisen/350382

- Füllen Sie **Visaanträge und Formulare** wahrheitsgemäß aus, ohne sicherheitsbedenkliche Informationen preiszugeben.
- Holen Sie bei Kolleginnen und Kollegen **Erfahrungen zur lokalen Sicherheitslage** ein. Und fragen Sie Schulungsangebote zum Themenkomplex des Travel Risk Managements in Ihrem Unternehmen an.
- Stellen Sie **Kontakte** zu diplomatischen Vertretungen **vor Ort**, zur medizinischen Versorgung und zu Ihrer Unternehmenssicherheit zusammen.
- Planen und **buchen Sie Reiserouten im Voraus**. Achten Sie auf einen guten Versicherungsschutz. Verkehrsunfälle könnten provoziert und entstehende Kosten als Druckmittel eingesetzt werden.
- Laden Sie ausschließlich **für den Aufenthalt benötigte Daten** auf Laptop und Smartphone. Vermeiden Sie Zugriffe auf das Firmennetzwerk und hinterlegen sich nicht die entsprechenden Zugangsdaten. Bei Reisen nach bspw. China, Russland und Israel dürfen keine Verschlüsselungen der Geräte erfolgen.
- Nehmen Sie nur mit, was für die Reise unmittelbar benötigt wird. Führen Sie **keine Dokumente von Geheimhaltungswert** mit. Wir empfehlen ausschließlich den Gebrauch von Kopien.

vor Ort

- Wie bereits geschildert, ist **bei der Einreise besondere Vorsicht** und Wachsamkeit geboten.
- Das Hotelzimmer und auch ein dortiger Safe sind kein sicherer Ort für Ihr Gepäck. **Tragen Sie Ihre Dokumente und Geräte stets bei sich**. Nutzen Sie keine zur Verfügung gestellten Ladekabel oder USB-Sticks.
- **Verhalten Sie sich unauffällig** und bleiben Sie potenziell gefährlichen Situationen fern. Seien Sie vorsichtig, was Sie in der Öffentlichkeit, in Hotelzimmern oder im Gespräch mit einer Kollegin oder einem Kollegen kommunizieren. Gespräche mit Ihnen fremden Personen sollten auf oberflächlicher Ebene bleiben.

danach

- **Besprechen Sie** alle auf der Reise beobachteten **Auffälligkeiten** mit den zuständigen Kolleginnen und Kollegen.
- Lassen Sie **auf der Reise verwendete technische Geräte** in heimischer Umgebung eingehend **prüfen**, bevor Sie diese wieder verwenden. Ändern Sie alle Zugangsdaten für berufliche und private Konten – von einem Gerät aus, dass Sie auf der Geschäftsreise nicht mitgeführt haben.
- Sollte es zu Anbahnungsversuchen ausländischer Nachrichtendienste oder sonstigen Auffälligkeiten gekommen sein, empfehlen wir die Kontaktaufnahme mit dem Bundesamt für Verfassungsschutz (BfV).

Sie finden alle Hinweise auch auf unserem Informationsblatt zur Sicherheit auf Geschäftsreisen zum Download unter:

Spezifische Hinweise zur Sicherheit auf Geschäftsreisen nach China finden Sie hier:

Darüber, welche Länder konkret ein hohes Risiko für die Sicherheit von Geschäftsreisenden bergen, gibt die vom Bundesministerium des Innern und für Heimat (BMI) festgelegte Staatenliste im Sinne von § 32 des Sicherheitsüberprüfungsgesetzes Auskunft. Zu finden ist die Liste auf der Webseite des BMI unter **www.bmi.bund.de** unter dem Stichwort "Staatenliste".

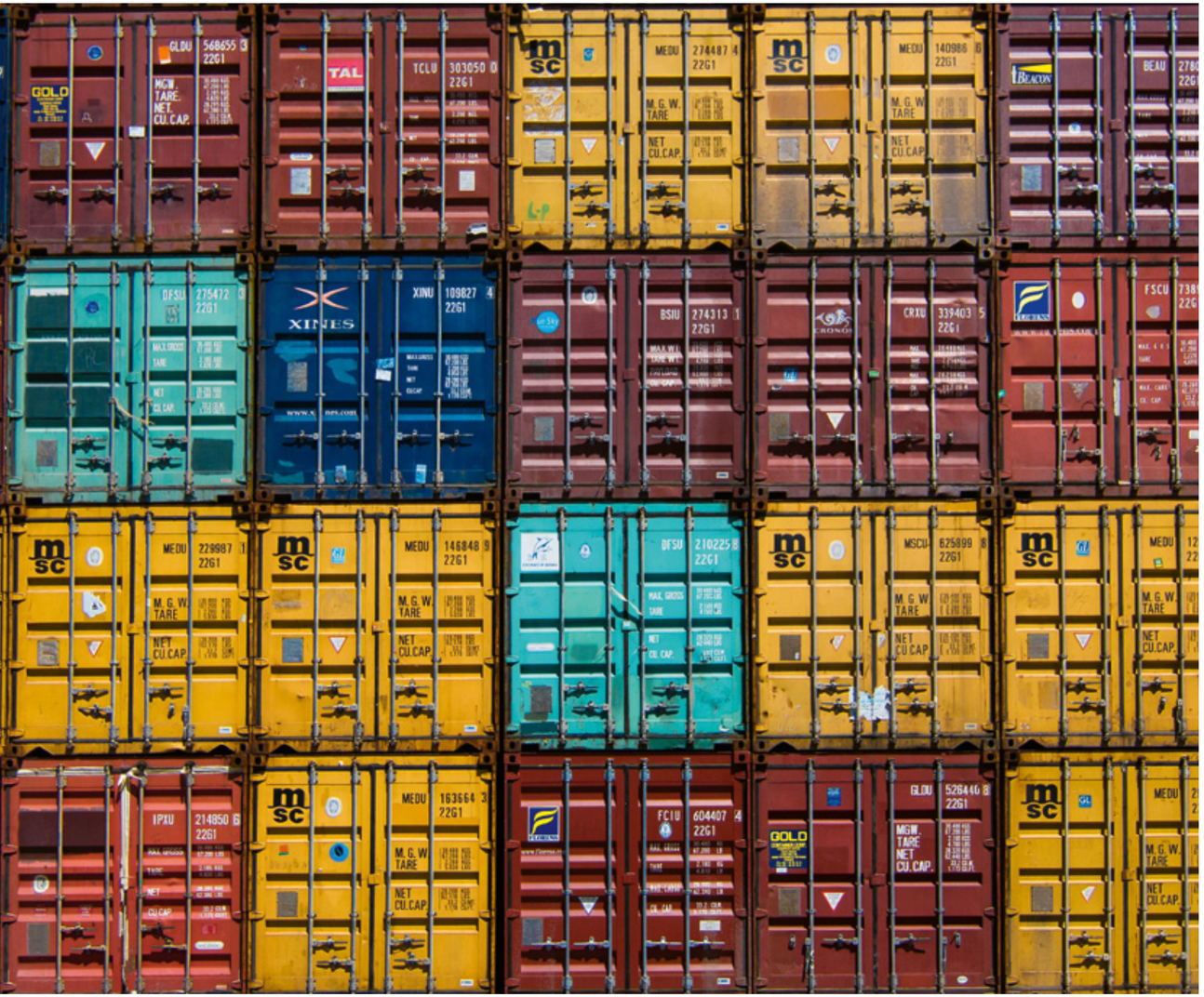


Foto: Guillaume Bolduc; Abbildung Lexikon der gesamten Technik (1904) von Otto Lueger

Die MACHT der NORMEN

Redaktion: Wirtschaftsschutz

Es ist der 15. Mai 1966, als die MS Fairland im Bremer Hafen anlegt und mit ihr die ersten Seecontainer Deutschland erreichen. Bereits zehn Jahre zuvor setzt der Speditionsunternehmer Malcolm McLean seine Idee um, Waren in großen Containern zu transportieren, um sie nicht mehr mühsam einzeln verladen zu müssen. Damit die Container universell auf Schiffen, Güterbahnen oder Lkw einsetzbar waren, einigt man sich 1968 auf einheitliche Standardmaße. Mittlerweile werden 95 % des weltweiten Warenhandels mithilfe von genormten Containern abgewickelt.

Normen und Standards sind das Rückgrat unseres modernen Welthandels. Doch seit Peking dieses Regelwerk als geopolitisches Werkzeug erkannt hat und zunehmend zur Durchsetzung politischer und wirtschaftlicher Interessen nutzt, rumort es in der Welt der Normen. So geht China mit dem Forschungsprojekt „Chinese Standards 2035“ unter anderem der Frage nach, wie politische Ziele durch das Normungssystem unterstützt werden können. Ein zentraler Baustein der daraus resultierenden Normungsstrategie ist die internationale Etablierung eigener Standards über Normierungs- und Standardisierungsgremien. Um dies zu erreichen, nutzt China unter anderem seine Mitgliedschaften in den internationalen Standardisierungsorganisationen ISO und IEC – mit viel Expertinnen- und Experten-Know-how, strategischen Prioritäten und finanziellen Mitteln. Ein weiterer integraler Bestandteil der Normungsstrategie ist die „Belt and Road Initiative“ (BRI), besser bekannt als „neue Seidenstraße“. Ein globales Investitionspartnerschaftsprogramm, bei dem es nicht nur um den weltweiten Bau von Häfen, Straßen oder Eisenbahnlinien, sondern auch um den Ausbau von Glasfaserkabeln oder Smart Cities geht. Regelmäßig verpflichtet China die Beteiligten dabei zur Nutzung chinesischer Normen und schafft so langfristige Abhängigkeiten von chinesischen Firmen und Standards, zum Beispiel bei Instandhaltungs- oder Ausbauprojekten. Eine solche Verbreitung nationaler Technologiestandards, so die Befürchtung vieler Fachleute, kann zu einer Zersplitterung der Normenwelt und in der Folge zu einem Rückgang der Nachfrage nach deutschen und europäischen Waren und Technologien führen.

Historischer Exkurs

Bereits drei Monate nach ihrer Gründung, im März 1918 veröffentlichte der „Normenausschuss der Deutschen Industrie“ – heute DIN – die DIN 1, die erste deutsche Industrienorm. Sie regelte die Beschaffenheit von sogenannten Kegelstiften, die als Verbindungselement insbesondere im Standardmaschinengewehr 08/15 zum Einsatz kamen. Durch die Norm konnten schließlich Kegelstifte verschiedener herstellender Unternehmen im Standardgewehr der deutschen Armee im Ersten Weltkrieg verbaut werden.

Was sind Normen eigentlich? Ein Exkurs

Erarbeitet werden Normen in einer Vielzahl internationaler, europäischer und nationaler Normungsgremien in denen Fachleute aus vielen Ländern

zusammenwirken und unter Einbeziehung der Öffentlichkeit gemeinsam Regelungsentwürfe erarbeiten. Diese werden am Ende des Normungsverfahrens als Norm etabliert. Dabei ist Deutschland seit vielen Jahren einer der Hauptakteure im internationalen Normungs- und Standardisierungswesen und in bestimmten Bereichen Spitzenreiter. Doch gerade hier hat China stark aufgeholt und konnte sich in der letzten Dekade bei der Besetzung von Spitzenpositionen in internationalen Normierungsgremien um 106 % steigern und versucht so seine Interessen in ausgesuchten Technologie- und Themenfeldern strategisch einzubringen. Dabei sei an dieser Stelle noch auf einen bedeutsamen Unterschied in der Art, wie Normung in Europa sowie bei den bisherigen, zumeist westlichen Hauptakteurinnen und Hauptakteuren und in China betrieben wird, hingewiesen: Das Normungswesen in Europa und den USA ist größtenteils privatwirtschaftlich organisiert und finanziert. China verfolgt einen strengen Top-Down-Ansatz mit dem Staat als treibende Kraft von Normung und Standardisierung.

Die neue Normungsstrategie der EU-Kommission ist nun ein erster Schritt, um den chinesischen Machtbestrebungen im Bereich der Normen zu begegnen und die globale Wettbewerbsfähigkeit der EU zu stärken. Das Thema Normung wird und muss aber auch in den betroffenen Wirtschaftskreisen stärker in den Blick genommen werden.

Im Gespräch mit dem SPOC-Magazin erläutert der Pressesprecher des Deutschen Instituts für Normung (DIN), Julian Pinnig, warum.

Bei der Setzung von Normen und Standards geht es nicht nur um Marktmacht, sondern auch um Werte. Welche Unterschiede gibt es zwischen europäischen und chinesischen Werten bei der Ausgestaltung von Normen für neue digitale Technologien?

Ein Beispiel von unterschiedlichen Werten, von dem auch die Normung berührt wird, ist der Umgang mit Daten. In Europa haben wir ein hohes Maß an Datenschutz. China dagegen setzt auf einen zentralen Zugang zu Daten, um dem Staat alle Möglichkeiten zu geben, Daten für eigene Ziele zu verwenden. Diese unterschiedlichen Herangehensweisen schlagen sich auch in der Ausgestaltung von Standards nieder. Bei der Normung im Bereich von KI wird es zum Beispiel wichtig sein, Anforderungen unter anderem an Fairness, Sicherheit, Datenschutz, Verlässlichkeit, Autonomie, Kontrolle, Verständlichkeit und Transparenz zu definieren, die europäischen Werten entsprechen. Denken Sie zum Beispiel an den Einsatz von KI-Systemen in Bewerbungsverfahren.

» **Wir brauchen mehr Expertinnen und Experten in den relevanten Normungsgremien.** «

Welche Bemühungen seitens China sehen Sie, im Bereich der Telekommunikation Standards zu setzen?

Grundsätzlich ist China sehr bemüht, im Bereich der Telekommunikation Standards zu setzen. Bei der ITU (Internationale Fernmeldeunion) besetzt China die Schlüsselposition des Generalsekretärs. Auch hat China leitende Positionen in sämtlichen ITU-T Study Groups, welche für die Erarbeitung von ITU-Standards verantwortlich sind.

Sehen Sie eine Gefahr, dass europäische Datenschutzstandards durch chinesische Normierungsbemühungen zukünftig aufgeweicht werden?

In der EU gilt die Datenschutz-Grundverordnung, das heißt der Datenschutz in den EU-Mitgliedsstaaten ist gesetzlich geregelt. Standards sind grundsätzlich Empfehlungen, die Anwenderinnen und Anwendern eine Stütze bieten und durch die Definition von technischen Anforderungen die Einhaltung der gesetzlichen Vorgaben erleichtern. China ist Mitglied in den internationalen Standardisierungsorganisationen ISO und IEC, nicht aber auf europäischer Ebene bei CEN und CENELEC und hat damit keinen direkten Einfluss auf europäische Datenschutzstandards. Es besteht jedoch die Gefahr, dass internationale Standards nicht mit den europäischen Werten vereinbar sind. Diese Standards sind aber lediglich Empfehlungen und müssen europäisch und national nicht übernommen werden. Wichtig ist es, mit den besten Expertinnen und Experten in den relevanten Normungsgremien vertreten zu sein, denn letztendlich geht es in der Normung um technische Expertise. In einigen Ausschüssen kommen derzeit jedoch fünf Chinesinnen und Chinesen auf eine europäische Expertin oder einen Experten. Gleichzeitig macht sich in Europa gerade bei den Zukunftsthemen der Fachkräftemangel bemerkbar.

DIN arbeitet in bilateralen Gremien auch mit chinesischen Behörden zusammen. Wie würden Sie die Zusammenarbeit beschreiben?

Wir empfinden die Gespräche als vertrauensvoll und auf Augenhöhe. Schwerpunktthemen sind derzeit die Bereiche Elektromobilität und Industrie 4.0, die Themenfelder Cybersicherheit, zivile Luftfahrt, Energieeffizienz und autonomes Fahren. Dabei hat die Zusammenarbeit von Deutschland und China in der Normung eine lange Tradition. Bereits im Jahr 1979 wurde das erste Abkommen zwischen den Normungsinstituten beider Länder unterzeichnet.

China setzt Normung und Standardisierung zunehmend als Instrument einer aktiven Handelspolitik ein. Erfahren die weitreichenden Auswirkungen der chinesischen Bemühungen ausreichend Aufmerksamkeit in der westlichen Staatengemeinschaft?

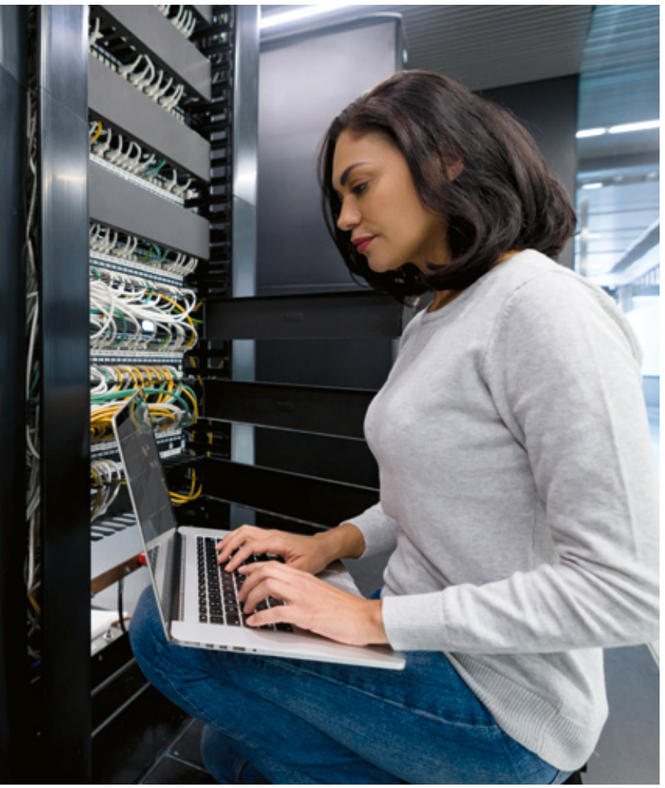
Nein, das Thema erfährt bisher keine ausreichende Aufmerksamkeit in der westlichen Staatengemeinschaft. Bei uns ist die Normung wirtschaftsgetrieben, das betrifft auch die Themen, die in der Normung von Deutschland und Europa aus gesetzt

DIN-Pressesprecher Julian Pinnig

Foto: DIN

werden. Wenn aber eine wirtschaftsgetriebene Normung einer staatsgetriebenen Normung, wie sie China verfolgt, gegenübersteht, dann entstehen Interessenskonflikte. Etwa in Bereichen, die von strategischer Bedeutung sind, wie Rohstoffe oder Umgang mit Daten. Hier müssen auch politisch Agierende im Sinne der strategischen Autonomie und digitalen Souveränität die Normung auf dem Schirm haben und ganz konkret Expertinnen und Experten der öffentlichen Hand in die Normung senden.

Was können deutsche Verantwortliche in Behörden und Unternehmen tun, um dem chinesischen koordinierten Vorgehen zu begegnen?



Politik, Wirtschaft und Normung müssen jetzt gemeinsam Schlüsselthemen definieren und priorisieren, die für die zukünftige Wettbewerbsfähigkeit von Deutschland und Europa entscheidend sind. Zugleich müssen Expertinnen und Experten aus Unternehmen, Behörden, Forschungseinrichtungen und zivilgesellschaftlichen Organisationen diese Themen in die internationalen Normierungsgremien bringen. Nur so können wir unsere traditionell starke Stellung in der internationalen Normung aufrechterhalten, die in den vergangenen Jahrzehnten eine der Grundlagen für wirtschaftlichen Erfolg war. Die neue Standardisierungsstrategie der Europäischen Kommission weist da in die richtige Richtung.

Welcher Normbereich nimmt aus ihrer Sicht eine herausragende Stellung ein und warum?

Mit Blick auf China müssen wir unser Engagement insbesondere in der Normung und Standardisierung von digitalen Technologien, also zum Beispiel von KI, Quantentechnologie, Blockchain, aber auch bei der Normung im Bereich Rohstoffe intensivieren. Unsere größte gemeinsame Herausforderung ist sicherlich der Klimawandel. Um eine grüne Transformation zu ermöglichen, braucht es daher jetzt neue technische Regeln sowie eine Überprüfung und Anpassung bestehender Standards. Denn beim Aufbau einer grünen und nachhaltigen Wirtschaft schaffen Normen und Standards Vertrauen in klimafreundliche Technologien, helfen bei der Erschließung neuer Märkte und erhöhen für Unternehmen und Staat die Investitionssicherheit.

Herr Pinnig, vielen Dank für das Gespräch.

Foto: Hispanolistic

Wirtschaft & Wissenschaft.
Zukunftssicher.
Verfassungsschutzverbund des Bundes und der Länder

EINE GEMEINSAME AUFGABE

Das System Verfassungsschutz der Bundesrepublik Deutschland ist weltweit einzigartig. In enger Zusammenarbeit kooperieren Bund und Länder in allen Angelegenheiten des Verfassungsschutzes und bilden einen schlagkräftigen Verbund. Insbesondere im Bereich des präventiven Wirtschafts- und Wissenschaftsschutzes profitieren Unternehmen und Organisationen von der Bündelung der Fachkompetenz der Landesbehörden vor Ort und der national sowie international eingebundenen Expertise des BfV.

Der beständige Austausch mit Wirtschaft und Wissenschaft knüpft ein flächendeckendes dynamisches Netzwerk, das in kooperativer Zusammenarbeit einen wesentlichen Beitrag zu einem resilienten Wirtschafts- und Wissenschaftsstandort Deutschland leistet.

ÜBERSICHT DER LÄNDER ANSPRECHBARKEITEN

Mehr Informationen unter
www.verfassungsschutz.de