N° 1 | 2021/2022

SPOC

Wirtschaft und Wissenschaft schützen

Social Engineering

Einblicke in moderne Wirtschaftsspionage

Der Verfassungsschutz
Aufgaben, Verantwortungen, Kontrolle

Chinas neue Wege der Spionage
Vor welchen Herausforderungen westliche Sicherheitsbehörden und Unternehmen jetzt stehen

Bundesamt für Verfassungsschutz

Liebe Leserinnen, Liebe Leser,

die Pandemie hat wie ein Brennglas auf viele relevante Themen unseres Landes gewirkt. Insbesondere die Wirtschaft musste sich rasch auf Entwicklungen und neue Verfahrensweisen einstellen. Für das Bundesamt für Verfassungsschutz (BfV) waren die Themen Wirtschaftsspionage und Sabotage von besonderer Dringlichkeit. Denn für einen resilienten Wirtschafts- und Wissenschaftsstandort Deutschland müssen wir vor allem Sicherheitskonzepte und -strukturen fortwährend anpassen.

Mit dem neuen SPOC-Magazin des BfV geben wir Ihnen Einblick in unsere Spionageabwehr und beleuchten ausgewählte Aspekte: So haben wir während der Pandemie eine erhebliche Anzahl von Social Engineering-Kampagnen beobachtet. Ob als Spear-Phishing-Angriff oder Deepfake, niemand ist vor geschickter Täuschung sicher. Darüber hinaus fragen wir nach konkreten Bedrohungen für Unternehmen durch moderne Spionage und Sabotage und mit welchen Maßnahmen sich Unternehmen schützen können.

Bei Ihrer persönlichen Gefahreneinschätzung möchten wir Sie mit dem SPOC-Magazin unterstützen. Als Single Point of Contact (SPOC) ist das Team vom Wirtschaftsschutz des BfV bei konkreten Sicherheitsanfragen und Verdachtsfällen Ihr vertraulicher Ansprechpartner.
Ich wünsche Ihnen eine spannende Lektüre.

Thomas Haldenwang
Präsident Bundesamt für Verfassungsschutz

Single Point of Contact –
SPOC

Dieses Heft wird vom Bereich Prävention in Wirtschaft, Wissenschaft, Politik und Verwaltung des Bundesamts für Verfassungsschutz 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
+49 (0)30 18 792 3322

Impressum:

Herausgeber
Bundesamt für Verfassungsschutz

Redaktionsleitung
Dr. Dan Bastian Trapp und Philip Kornberger

Art Direktion und Gestaltung
Sonnenstaub, Berlin | sonnenstaub.com

Mitwirkende
Katrein Baumeister | agentur-sheila.com
Sean Dunn | agentur-sheila.com

Korrektorat
Katrein Baumeister | agentur-sheila.com

Herstellung
Spreedruck

MIX
Papier aus verantwortungsvollen Quellen
FSC® C125128
www.fsc.org

Klimaneutral
Druckprodukt
ClimatePartner.com/11669-2110-1003

Inhalt

04

Radar
Wichtiges auf einen Blick

06

Die Gefahr von Social Engineering
Steht die soziale Manipulation erst am Anfang ihrer (technischen) Möglichkeiten?

12

Sicher ins digitale Zeitalter
Interview mit Dirk Fleischer, CSO & CISO der Dürr AG sowie Autor des Buches „Wirtschaftsspionage“

15

Der Verfassungs-schutz
Partner des Vertrauens

27

Albtraum statt Traumjob
Die Social Engineering-Methoden der Hackergruppe Lazarus

30

Chinas neue Wege der Spionage
Vor welchen Herausforderungen westliche Sicherheitsbehörden und Unternehmen jetzt stehen

35

Deepfake
Auf dem Weg zum Social Engineering 2.0?

Bitkom-Untersuchung:

Zunehmende Attacken auf Unternehmen

Die vom Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (Bitkom) veröffentlichte Studie „Wirtschaftsschutz 2021“ zeigt einen deutlichen Anstieg digitaler wie analoger Angriffe auf deutsche Unternehmen im vergangenen Jahr. Insbesondere Social Engineering-Attacken wurden vermehrt registriert. So gaben 27% der befragten Unternehmen an, am Telefon angesprochen worden zu sein, 10% der Ansprachen fanden im privaten Umfeld statt.

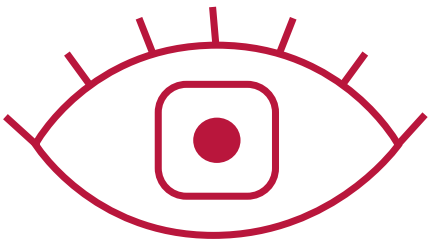
Rund 1.000 Geschäftsführerinnen und Geschäftsführer sowie Sicherheitsverantwortliche quer durch alle Branchen wurden für die Studie befragt. 88% gaben an, im Zeitraum der letzten 12 Monate von Diebstahl, Industriespionage oder Sabotage vermutlich betroffen gewesen zu sein. Im Vorjahreszeitraum waren es lediglich 75%. Insgesamt verursachen Datendiebstahl, Industriespionage und Sabotage jährlich einen Schaden von über 223,5 Milliarden Euro.

www.bitkom.org

Innentäter

Wie die aktuelle Bitkom-Umfrage (2021) zeigt, stecken hinter 61% der Fälle von Datendiebstahl, Industriespionage oder Sabotage aktuelle oder ehemalige Beschäftigte. Unternehmen können dem Phänomen „Innentäter“ begegnen, indem sie in ihren Sicherheitskonzepten entsprechende präventive Maßnahmen verankern.

Die aktuelle Broschüre „Informationsabfluss aus Unternehmen – Innentäterschaft als unterschätztes Massenphänomen“ vermittelt anhand verschiedener Beispiele und Checklisten praxisorientierte Umsetzungshilfen für Prävention, Detektion und Reaktion. Die Broschüre können Sie auf der Internetseite **www.wirtschaftsschutz.info** kostenfrei herunterladen.



Von Katzen, Bären und Pandas

Eine Gruppierung, die Cyberangriffe verübt, kann mitunter zahlreiche verschiedene Namen tragen. So führen beispielsweise unterschiedliche IT-Sicherheitsunternehmen ein und dieselbe Gruppierung unter einem ganz anderen Namen (z. B. Karma Panda, Tonto Team, Cactus Pete). Typisch ist jedoch am Ende des Gruppennamens eine tierische Metapher: So werden Pandas der VR China zugeordnet, Bären der Russischen Föderation und Kätzchen dem Iran.

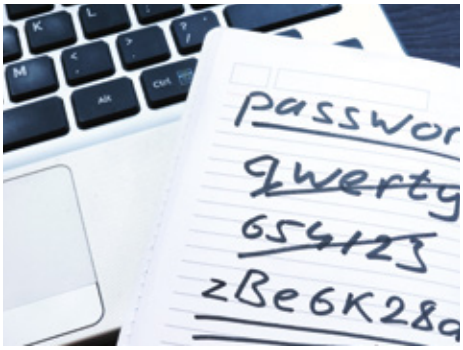
Übrigens hat die Cyberabwehr hierzu ein Cyberkartenspiel entwickelt, welches wir bei verschiedenen Gelegenheiten herausgeben.

Foto: istockphoto.com/portfolio/da-kuk; Illustration: Sonnenstaub

IT-NOTFALL-KARTE

Was tun, wenn's brennt? Im Ernstfall können die Alarmpläne „Verhalten im Brandfall", die oft in öffentlichen Gebäuden aushängen, Leben retten. Kurz und übersichtlich finden sich dort die wichtigsten Verhaltensweisen in chronologischer Reihenfolge abgebildet. Auch bei IT-Störungen, wie zum Beispiel bei einem Hackerangriff, ist schnelles und besonnenes Handeln unerlässlich. Um dies zu unterstützen, hat der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. eine IT-Notfallkarte herausgegeben. Wie die Alarmpläne sollte die IT-Notfallkarte zum Sicherheitsstandard in Unternehmen gehören.

Deutsche nutzen nach wie vor unsichere Passwörter



Das Hasso-Plattner-Institut (HPI) veröffentlicht jedes Jahr die häufigsten Passwörter der Deutschen. Ein Blick auf die Top Twenty 2019 zeigt, dass sich immer noch zu viele Internetnutzerinnen und Internetnutzer auf simple Zahlenreihen wie „123456", Tastenkombinationen wie „qwertz" oder Wörter wie „password" verlassen, die keinen wirksamen Schutz vor Cyberangreifern bieten.

Das HPI greift dabei auf 67 Millionen Zugangsdaten zurück, die auf E-Mail-Adressen mit .de-Domain registriert sind und 2019 im Netz geleakt wurden. Ob man selbst Opfer eines Datendiebstahls geworden ist, lässt sich mit dem „Identity Leak Checker" des HPI unter **https://sec.hpi.de/ilc** prüfen.

Tipps zum Erstellen sicherer Passwörter bieten u. a. das Bundesamt für Sicherheit in der Informationstechnik (BSI) oder die Verbraucherzentralen:

www.bsi-fuer-buerger.de
www.verbraucherzentrale.de

25% der deutschen Unternehmen, v. a. Kleinunternehmen, erlitten durch Cyberangriffe nahezu existenzbedrohende Schäden

55% der in der Bitkom-Studie befragten Führungskräfte wurden Opfer von Social Engineering

89% der Befragten der Bitkom-Studie von 2020 sehen mehr Cyberattacken als im Vorjahr

9 von 10 Unternehmen sind durch Cyberangriffe betroffen

Im Vergleich zum Vorjahr steigen Erpressungsvorfälle, mit einem Ausfall von Informations- und Produktionssystemen sowie der Störung von Betriebsabläufen, um

358%

Quellen: bsi.de, bitkom.org

Die Gefahr von SOCIAL ENGINEERING

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

Den Besten wie Alethe Denis reichen zwanzig Minuten. Während sie vom Publikum mit tosendem Applaus gefeiert wird, dürfte ihr Gegenüber wohl am liebsten im Erdboden versinken wollen.[1] In simulierten Angriffen werden beim Wettbewerb Social Engineering Capture the Flag (SECTF) auf der jährlich in Las Vegas stattfindenden Hackerkonferenz DEFCON, die Gefahren, die von Social Engineering für Unternehmen ausgehen, eindrücklich aufgezeigt.

Alethe Denis, die Siegerin von 2019, brachte während des Wettbewerbs einen Angestellten ihres Zielunternehmens nicht nur dazu am Telefon detaillierte Angaben über seine IT-Ausstattung und installierte Software zu machen, sondern sie konnte ihr Opfer sogar dazu bewegen, auf seinem Rechner zwei Internetadressen aufzurufen, die sie ihm diktierte. Um das Vertrauen ihrer Zielperson zu gewinnen, musste sie sich lediglich als Kollegin aus der IT ausgeben, die sich um einen angeblich anstehenden Rechneraustausch kümmert.

Das Zielunternehmen wurde Denis vom Veranstalter des Wettbewerbs bereits drei Wochen vor dem Angriff auf der Live-Bühne der DEFCON zugewiesen. In diesen hatte sie Zeit, einen Bericht über das Zielunternehmen anzufertigen, in dem sie bestimmte „Flags" abarbeitet – spezifische Informationen über das Ziel, die vorab in einem Katalog festgelegt wurden und die sich ein tatsächlicher Social Engineering-Angreifer zunutze machen könnte: Persönliche Angaben zu Angestellten, Adressdaten, Namen von Ehepartnerinnen und Ehepartnern, Kindern oder Hobbys bis hin zu Details zu Hard- und Software, die im Unternehmen genutzt wird.

Dabei ist in dieser ersten Phase des Wettkampfs der direkte Kontakt per E-Mail oder Telefon ausdrücklich untersagt. Lediglich öffentlich zugängliche Quellen wie die Unternehmenswebseite, Medienberichte, Suchmaschinen wie Google, soziale Netzwerke wie LinkedIn oder Xing dürfen für die Erstellung des Berichts hinzugezogen werden.

> *Open Source Intelligence (OSINT): OSINT ist ein Begriff aus dem nachrichtendienstlichen Sprachgebrauch. Er bezeichnet die Informationsgewinnung aus frei für jedermann verfügbaren Quellen. Dabei kann es sich um analoge oder digitale Medien, Webseiten und soziale Netzwerke oder auch schlicht um ganz alltägliche Gesprächssituationen handeln.*

Der zweite Teil des Rankings wird beim Live-Auftritt vor Publikum im Rahmen der Konferenz ermittelt. In einer schalldichten Kabine sitzend, haben die Teilnehmerinnen und Teilnehmer zwanzig Minuten Zeit, am Telefon mit einer oder einem Angestellten des Zielunternehmens erneut zuvor erhaltene Flags abzuarbeiten und schließlich an vertrauliche Informationen zu kommen.

Der Schaden, den Denis bei einem realen Angriff hätte anrichten können, wäre immens gewesen. Mit hinter den genannten Internetadressen versteckter Malware hätte sie nicht nur Zugriff auf den infizierten Rechner, sondern darüber auch auf das gesamte Firmennetzwerk erhalten können. Der simulierte Angriff zeigt auf drastische Weise, dass selbst noch so ausgefeilte technische Schutzmaßnahmen umgangen werden können, wenn Angreifer gezielt den Menschen und sein Verhalten ins Visier nehmen. Mittels gezielter Ausnutzung menschlicher Eigenschaften wie Hilfsbereitschaft, Vertrauen, Angst, Respekt vor Autorität oder schlichtweg Neugier, werden beim Social Engineering Personen in ihrem Verhalten manipuliert. Ein Opfer, das auf die Täuschung hereinfällt, handelt im Glauben, das Richtige zu tun. Tatsächlich spielt es jedoch dem Motiv des Täters in die Hände.[2]

Social Engineering an sich ist nichts Neues. Seit Menschengedenken dient soziale Manipulation als Grundlage für unterschiedlichste Betrugsmaschen. Ein klassisches Beispiel ist der „Enkeltrick", bei dem

[1] https://www.spiegel.de/netzwelt/web/social-engineering-die-besten-tricks-der-menschen-hacker-a- 1281453.html
[2] https://www.bsi-fuer- buerger.de/BSIFB/DE/DigitaleGesellschaft/IT_Sicherheit_am_Arbeitsplatz/SoEng/Social_Engineering_node.html

sich Trickbetrüger – meist telefonisch – gegenüber älteren Personen als nahe Verwandte ausgeben, um unter Vorspiegelung falscher Tatsachen an Bargeld oder Wertgegenstände zu gelangen. Im Zeitalter der digitalen Kommunikation ergeben sich zudem neue, äußerst effektive Möglichkeiten für Social Engineering und die zunehmende Vernetzung sorgt dafür, dass die Zahl potentieller Opfer rasant steigt. Studien belegen, wie groß das Problem für die Wirtschaft bereits ist. So hat der Digitalverband Bitkom zuletzt ermittelt, dass in den Jahren 2020 bis 2021 etwa 41 Prozent aller Unternehmen von digitalem Social Engineering betroffen waren. Am höchsten war dabei der Anteil von telefonischen Angriffen. Dieser lag bei ungefähr 27 Prozent.[3]

Die bekannteste Form des digitalen Social Engineering ist das „Phishing". Dabei handelt es sich um E-Mails, die von einem auf den ersten Blick vertrauenswürdigen Absender stammen und auf eine vom Angreifer (nach)gebaute Webseite verlinken. Der E-Mail-Text erläutert, dass auf besagter Webseite dringend Daten aktualisiert werden müssen oder wichtige Informationen bereitstehen und verleitet so Empfängerinnen und Empfänger zum Klick auf den Link. Infolgedessen infiziert sich das Opfer dann mit Malware oder aber wird zur Eingabe persönlicher Daten animiert, die der Angreifer wiederum „abfischen" und für seine eigenen Zwecke missbrauchen kann.

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

Neben den klassischen Phishing-E-Mails via Massenversand an einen beliebigen Empfängerkreis lässt sich zunehmend eine gezieltere Variante dieser Methode beobachten, das „Spear-Phishing". Beim Spear-Phishing werden die E-Mails mit vorab recherchierten Inhalten, nicht selten Insiderwissen, auf ausgewählte Personengruppen oder einzelne Mitarbeiterinnen und Mitarbeiter maßgeschneidert. Eine Methode, welche die Erfolgschancen des Angreifers signifikant erhöht.

Ähnlich ist die Herangehensweise bei der Angriffsstrategie „Watering-Holes". Bei dieser suchen Angreifer gezielt nach Webseiten, die regelmäßig von Mitarbeiterinnen und Mitarbeitern des eigentlichen Zielunternehmens frequentiert werden: wie die Webseite von der Pizzeria oder Reinigung um die Ecke oder dem Kurierdienst, mit dem das Unternehmen regelmäßig zusammenarbeitet. Webseiten, die in der Regel weniger geschützt sind als die des Zielunternehmens und sich besser für die Einschleusung von Malware eignen. Bestellen Beschäftigte nun online über die infizierte Webseite der Pizzeria, holen sie sich auch den Schadcode frei Haus dazu.

> *Watering-Holes: Bei Watering-Holes handelt es sich um legitime Webseiten, die mit Schadsoftware infiziert wurden. Die Infizierung ist meist durch unbekannte Sicherheitslücken, sogenannte Zero-Day-Exploits, möglich. Watering-Holes können als Attacke gegen Unternehmen oder Institutionen verwendet werden, indem gezielt häufig genutzte Webseiten der betreffenden Opfer infiziert werden. Der Begriff stammt aus der Tierwelt der afrikanischen Savanne, wo sich zu bestimmten Zeiten diverse Arten, die ansonsten Fressfeinde sind, zum Trinken am selben Wasserloch einfinden.*

Da der Kosten-Nutzen-Aufwand vergleichsweise höher ist, sind die Hintermänner beim Spear-Phishing oder bei Watering-Holes in der Regel nicht unter den Hackern zu finden, die willkürlich Daten abgreifen.

[3] https://www.bitkom.org/sites/default/files/2021-08/bitkom-slides-wirtschaftsschutz-cybercrime-05-08-2021.pdf

Stattdessen handelt es sich hier um Social Engineering-Profis. Dazu zählen auch staatliche Akteure, allen voran ausländische Nachrichtendienste. Insbesondere die Dienste aus China, Russland und dem Iran tun sich hier mit entsprechenden APT-Kampagnen hervor.

> *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.*

Sie interessieren sich nicht nur für die deutsche Politik und deren Akteure, sondern auch für die hiesige Wirtschaft und Wissenschaft. Das Ziel: strategische Informationen sowie Unternehmens- und Forschungs-Know-how abzuschöpfen, um damit dem eigenen Land einen illegitimen Vorteil im internationalen Wettbewerb zu verschaffen. Die Angriffskampagnen betreiben dafür einen erheblichen Aufwand und setzen auf eine breite Palette an Methoden, darunter auch ständig neue Ansätze von Social Engineering.

Wie systematisch Nachrichtendienste potentielle Angriffsziele bereits im Vorfeld mittels Social Engineering ausforschen, illustriert eine Kampagne, über die der Verfassungsschutz erstmalig 2017 und erneut 2019 die Öffentlichkeit informierte. So waren chinesische Nachrichtendienste dabei beobachtet worden, wie sie über LinkedIn und andere soziale Netzwerke versuchten, für sie interessante Kontakte anzubahnen. Die Nachrichtendienstler traten dabei getarnt als Angestellte von Think Tanks, Wissenschaftlerinnen oder Wissenschaftler oder Angehörige chinesischer Behörden auf. Manchmal gaben sie sich auch als Headhunterinnen und Headhunter oder Führungskräfte von Consulting-Firmen aus.

Die zunehmende Vernetzung und Kommunikation über digitale Kanäle sorgen dafür, dass die Zahl der Opfer rasant steigt.

Beispiele für die Nutzung von Social Engineering durch APT:

• Seit 2015 tritt die mutmaßlich staatlich gesteuerte iranische Cyberangriffsgruppierung Mabna Institute weltweit mit umfangreichen Spear-Phishing-Kampagnen in Erscheinung. Diese richten sich in erster Linie gegen akademische Einrichtungen. Das Ziel der Kampagnen scheint der Zugang zu wissenschaftlichen Publikationen sowie Anmeldedaten für Lernplattformen von Universitäten zu sein. Die Spear-Phishing-Mails sind sehr professionell gestaltet und animieren die Empfängerinnen und Empfänger einen Link anzuklicken, über den angeblich der Zugang zu der jeweiligen Lernplattform entsperrt wird. Der Link führt jedoch auf eine hochwertige Kopie der legitimen Anmeldeseite der Lernplattform. Erst nach Eingabe der Zugangsdaten erfolgt eine Weiterleitung auf die tatsächliche Seite der jeweiligen Institution. Die so erbeuteten Informationen werden entweder auf akademischen Portalen im Iran zum Verkauf angeboten oder für den Download von Inhalten auf den Plattformen genutzt.[4]

• Aus wahrscheinlich Südasien stammt eine umfassende Spear-Phishing-Kampagne, die im Sommer 2020 von legitim erscheinenden E-Mail-Adressen versendet wurde. Ein staatlich gesteuerter Cyberakteur gab sich als ausrichtende Organisation für Tagungen aus, die sich mit sicherheitspolitischen Themen benachbarter Staaten beschäftigen. Die gefälschten E-Mails kündigten inhaltlich eine kurzfristige Programmänderung einer zeitnah anstehenden Tagung an. Der Cyberakteur wollte hierdurch einen besonders hohen Reaktionsdruck bei den empfangsberechtigten Personen auslösen, da der E-Mail-Versand nur wenige Stunden vor dem Veranstaltungsbeginn erfolgte. Das vorgeblich aktualisierte Tagungsprogramm war nur durch Öffnen des der E-Mail beigefügten maliziösen Word-Dokuments zu sehen. Im Fokus des Angriffs standen die beruflichen E-Mail-Adressen der an der Tagung teilnehmenden Personen sowie von Personen aus deren beruflichen Umfeld. Im Oktober 2016 wurde bekannt, dass die Kampagne Charming Kitten (auch bekannt als Newscaster oder Ajax Hacking Team), deren Ursprung im Iran vermutet wird, gezielt Unternehmen aus der Energiebranche ins Visier nahm. Hierzu empfand die Gruppierung Domains von echten Jobportalen für den Öl- und Gassektor nach. Parallel wurden (Word-)Dokumente mit Links zu angeblichen Stellenangeboten produziert, die mit Malware versehen wurden.

• Seit Ende 2016 richtet die mutmaßlich chinesische Kampagne APT 10 (auch bekannt als Menu Pass Team oder Stone Panda) ihr Augenmerk verstärkt auf Unternehmen in Europa. Ausgangspunkt der Angriffe sind in der Regel Spear-Phishing-E-Mails, die thematisch auf die jeweiligen Empfängerinnen und Empfänger zugeschnitten sind und maliziöse (Word-)Dokumente enthalten.

• Vermutlich zwischen August 2017 und Juni 2018 gab es eine besonders hochwertige Spear-Phishing-Angriffswelle u. a. gegen deutsche Medienunternehmen. Die versandten E-Mails enthielten im Anhang ein maliziöses (Word-)Dokument. Beim Öffnen des Dokuments erschien der Hinweis, die Ausführung sogenannter Makros zu erlauben. Dabei handelt es sich um Abfolgen von Befehlen und Anweisungen, die zusammengefasst werden, um damit eine Automatisierung häufig ausgeführter Aufgaben zu ermöglichen. Wurde die Ausführung erlaubt, führte das zur Installation von Schadcode, welcher dem Angreifer letztlich bestimmte administrative Befehlsrechte einräumte. Die Kampagne wird der staatlich gesteuerten APT-Gruppierung Sandworm (auch bekannt als Quedagh oder Black Energy) zugerechnet.

[4] https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/2018/nachrichtendienstlich-gesteuerte-cyberangriffe.html

Unter dem Vorwand sich für die Arbeit der jeweiligen Zielperson zu interessieren, erkundigten sie sich nach Möglichkeiten eines fachlichen Austauschs und verwiesen auf „wichtige Kunden“, die an westlicher Expertise interessiert seien. Im nächsten Schritt wurden Betroffene um Übermittlung eines Lebenslaufs und einer – vergüteten – Probearbeit gebeten. Fiel diese zur Zufriedenheit aus, folgte eine Einladung nach China, um sich dort mit dem „wichtigen Kunden“ zu treffen. Die Kosten des Aufenthaltes wurden übernommen. Tatsächlich trat der wichtige Kunde jedoch niemals in Erscheinung und wurde auch nie namentlich benannt. Im weiteren Verlauf wurden Betroffene regelmäßig aufgefordert, wiederum gegen entsprechende Vergütung, Berichte zu verfassen oder interne, sensible Informationen aus ihrem jeweiligen Arbeitsbereich weiterzugeben.

Obwohl Social Media-Plattformen wie LinkedIn immer wieder aktiv gegen auffällige Fake-Profile vorgehen, beobachtet der Verfassungsschutz auch weiterhin entsprechende Anbahnungsversuche.

Was können Sicherheitsverantwortliche in Wirtschaft und Wissenschaft tun, um dem zu begegnen?

Je stärker die Vernetzung von Unternehmen oder Forschungseinrichtungen mit Zulieferern oder Dienstleistungsunternehmen, desto größer ist auch die Gefahr, Opfer von Social Engineering zu werden. So nutzen Angreifer immer wieder die vermeintlich schlecht gesicherten Unternehmen innerhalb einer Lieferkette, um sich Zugang zum eigentlichen Zielunternehmen zu verschaffen.

Eine typische Social Engineering-Attacke lässt sich in vier Phasen unterteilen: Planung, Aufklärung und Informationsbeschaffung sowie Entwicklung eines Szenarios und Durchführung. Für das Aufsetzen geeigneter Sicherheitsstrategien hilft es, sich an diesen Phasen zu orientieren.

In einem ersten Schritt sollten mittels einer Risikoanalyse mögliche Angriffsziele, das heißt sensible Unternehmensdaten und -informationen, sowie eventuelle Angriffspfade identifiziert werden. Dabei muss auch die Möglichkeit eines gewollten oder versehentlichen Informationsabflusses durch eigene Beschäftigte berücksichtigt werden. Aufbauend auf dieser Analyse können nun entsprechende Schutzmaßnahmen abgeleitet werden. Die Grundlage effektiver Schutzmaßnahmen bildet dabei ein Klassifizierungssystem, in dem die identifizierten Schutzgüter bestimmten Schutzstufen zugeordnet werden.

Ziel der zweiten Phase eines Social Engineering-Angriffs ist es, möglichst viele Informationen über das Angriffsziel zu erlangen: Organisationsaufbau, relevante Personen, Kontaktdaten, verwendete Hard- und Software, Geschäftsbeziehungen etc. Diese Informationsbeschaffung erfolgt über Onlinerecherchen, durch technische Verfahren oder auch durch direkte Aufklärung vor Ort oder persönliche Kontaktaufnahme. Mit verschiedenen Maßnahmen kann Angreifern die Informationssuche erschwert werden:

- Mit Berechtigungskonzepten zur Informationssicherheit
- Bereinigung der Webseite von sensiblen Informationen
- Richtlinien für den Umgang mit Organisationsdaten auf Social Media-Plattformen
- Der Verwendung sicherer Passwörter
- Stets aktualisierter Software
- Regelmäßigen Schulungen aller Beschäftigten, insbesondere Personen an sicherheitssensiblen Stellen

Insbesondere die stetige Sensibilisierung der Beschäftigten für Social Engineering-Methoden und das Einstudieren von Handlungsroutinen über Rollenspiele und praktisches Ausprobieren ist ein wichtiger Baustein in einer effektiven Sicherheitsarchitektur. Gut geschultes Personal wird dann auch im Falle eines tatsächlichen Angriffs diesen schneller erkennen, kann besser reagieren und so das Unternehmen vor größerem Schaden bewahren.

SICHER
ins digitale Zeitalter

Interview mit Dirk Fleischer von der Dürr Group

Mit rund 16.500 Beschäftigten ist die von Paul Dürr 1896 gegründete Dürr Group eines der Schwergewichte des deutschen Mittelstands. Bereits seit Jahren treibt die Organisation die Digitalisierung voran und unterstützt unter anderem das von der Dürr AG mitgegründete IoT-Netzwerk Adamos, um die digitale Transformation im deutschen Maschinen- und Anlagenbau voranzutreiben.
Mit Dirk Fleischer, Corporate Security Officer und Corporate Information Security Officer bei Dürr sowie Autor des Buches „Wirtschaftsspionage“, sprach das SPOC-Magazin darüber, wie Dürr der Umstieg in das digitale Zeitalter in Bezug auf Sicherheit gelingt, über generelle Herausforderungen für mittelständische Unternehmen im Bereich Sicherheit und wie die Gefahren von Social Engineering in der Praxis einzuordnen sind.

Herr Fleischer, bei Dürr bauen Sie seit eineinhalb Jahren eine Sicherheitsarchitektur auf. Wie haben Sie die Beschäftigten für das Thema Sicherheit motivieren können?

Wir haben von Beginn an deutlich gemacht, dass Sicherheit nicht Selbstzweck, sondern zukunftssicherndes Element ist, dass ein gelebter Wirtschaftsschutz unternehmerische Aktivitäten ermöglicht und nicht blockiert. Beispielsweise bekommen jene Unternehmen ein besseres Rating bei Nachhaltigkeitsindizes, welche ein schlüssiges Sicherheitskonzept haben. Wir versuchen also immer mit zu identifizieren, wo es Handlungsoptionen für das Unternehmen gibt, die durch ein ausgewogenes und gutes Sicherheitsdenken begünstigt werden und positionieren uns so als wirtschaftlicher Faktor im Unternehmen.

Was sind aus Ihrer Sicht die wesentlichen Sicherheitsgefahren für deutsche Unternehmen?

Know-how-Abfluss durch Industriespionage, Cyberkriminalität im engeren Sinne – insbesondere im Hinblick auf die Fortführung von Geschäftsprozessen; das Phänomen Ransomware macht uns, glaube ich, in allen Unternehmen große Sorgen. Das dritte Thema sind „Allgemeine Kriminalitätsformen", wie Wirtschaftsstraftaten, Eigentumsdelikte ebenso wie Cyberkriminalität im weiteren Sinne. Die Digitalisierung sämtlicher Bereiche katalysiert vor allem Cybergefahren.

Als weltweit agierendes Unternehmen sind Sie auf globale Vernetzung angewiesen. Wie schaffen Sie es, mit Ihrer Sicherheitsarchitektur die Balance zwischen Sicherheit und Offenheit zu halten?

Das Thema Sicherheit darf keine Wirtschaftsprozesse hemmen. Deswegen setzen wir bei Dürr sehr stark auf Awareness, Sensibilisierung und Enabling, denken also immer auch inhaltskritisch darüber nach, ob es eine verhältnismäßige Maßnahme ist, die wir treffen.

Wie sieht das konkret aus?

Wir arbeiten in unseren Konzepten stark mit „Muss-, Soll- und Kann-Vorschriften". „Muss-Vorschriften" müssen von allen berücksichtigt werden. „Soll-Vorschriften" sind abgewogene Empfehlungen. Mit „Kann-Vorschriften" geben wir Hilfestellung, wie man beim Thema Sicherheit einen Schritt weiter gehen kann. So schaffen wir einen globalen Standard, der für jeden nachvollziehbar ist. Handhabbarkeit steht bei unserer Arbeit an oberster Stelle.

Laut der aktuellen Bitkom-Studie sind rund 55% der befragten Unternehmen von Social Engineering betroffen. Haben Sie selbst bereits Erfahrungen mit diesem Thema gemacht?

Erst kürzlich haben wir eine größere Social Engineering-Kampagne erlebt, auf die wir schnell mit einer Sensibilisierungskampagne nach innen reagieren mussten. Im konkreten Fall haben in erheblichem Umfang Personen angerufen, die sich nach den Funktionsträgerinnen und Funktionsträgern in einer bestimmten Abteilung erkundigt haben. Es war recht eindeutig, dass ein Teilbereich, der insbesondere beim Know-how-Schutz eine zentrale Rolle spielt, gezielt ausgeforscht wurde. Das half uns bei der Einordnung ungemein. Dabei ist es unwahrscheinlich wichtig, die Person, die durch Social Engineering angesprochen wird, nicht zum „Mittäter" zu machen. Wer so eine Reaktion befürchten muss, wird seine Bereitschaft, sich an die Unternehmenssicherheit zu wenden, reduzieren.

» **Wir müssen den Mitarbeiterinnen und Mitarbeitern den Rücken stärken.** «

Können Sie uns ein paar Tipps geben, zum Schutz vor Social Engineering?

Wenn Sie angerufen werden, lassen Sie sich die Nummer der anrufenden Person geben und rufen Sie zurück. Wichtig ist dann, das Gespräch selbst zu führen und sich nicht führen zu lassen. Dafür müssen wir wiederum den Firmenangehörigen das Rüstzeug an die Hand geben, um selbstbewusst reagieren zu können, auch wenn auf der anderen Seite Druck aufgebaut wird, beispielsweise wenn sich der Angreifer auf höher gestellte Personen beruft. Der Klassiker ist und bleibt: am Telefon nicht mit jedem über alles sprechen.

Trotz der verstärkten Aufklärung und Prävention in diesem Bereich – wie schätzen Sie die Entwicklung dieses Phänomens ein?

Foto: Dürr AG

Mit zunehmender Technologisierung und Digitalisierung – Stichwort Deepfakes – wird die Gefahr, die von Social Engineering ausgeht, nicht nur deutlich wachsen, sondern sich auch neue Formen des Social Engineering entwickeln. Durch die Schaffung virtueller Umgebungen potenziert sich beispielsweise die Gefahr virtueller Scheinwelten.

Welche Unternehmenssicht zum Thema Sicherheit müsste im politischen Raum präsenter sein?

Dass ein guter und aktiv gelebter Wirtschaftsschutz ein wesentlicher Standortfaktor ist. Einer, der das Überleben der Wirtschaft genauso sichert wie günstige Kredite.

Welche Unterstützung wünschen Sie sich dabei von deutschen Sicherheitsbehörden?

Ich wünsche mir einen pragmatisch-fördernden und kooperativen Wirtschaftsschutz. Die amerikanische Regierung hat zum Beispiel eine Ransomware-Taskforce eingerichtet und Ransomware-Angriffe auf die Stufe terroristischer Attacken gestellt. Hierdurch werden Ermittlungsmöglichkeiten verbessert und gleichzeitig bekommen Unternehmen ganz konkrete Hinweise und Ansprechstellen. Das ist für mich priorisierend und zugleich maßnahmenfokussiert, pragmatisch.

Welche drei Ratschläge geben Sie anderen Unternehmen zum Thema Sicherheit?

Pragamatismus, Risikobasiertheit und Kooperation.
Das Thema Sicherheit sollte immer passend zum Unternehmen behandelt werden. Sich über für das Unternehmen relevante Sicherheitsthemen Gedanken zu machen, ist der erste Schritt.
Mit Risikobasiertheit meine ich, dass Sicherheit immer auch ein Teil des Risk-Managements ist. Die Reduzierung von wirtschaftlichen Risiken findet in Unternehmen seit Jahren statt. Auch Sicherheitsrisiken müssen dabei berücksichtigt werden. Es macht keinen Sinn über Supply Chain Security nachzudenken, wenn das Unternehmen keine Lieferketten ins Ausland hat.
Zuletzt sollte eine Sicherheitsabteilung immer als Teil des Unternehmens aufgebaut und verstanden werden und nicht als ausgelagerte Organisationseinheit innerhalb eines Unternehmens. Das Furchtbarste ist, als Unternehmenssicherheit wie ein Fremdkörper platziert zu sein, der nur über Governance und Regeln arbeitet. Das funktioniert heutzutage eigentlich nirgendwo mehr.

Herr Fleischer, vielen Dank für das Gespräch!

Foto: Dürr AG

Bundesamt
für Verfassungsschutz

PARTNER DES VERTRAUENS

Bundesamt für Verfassungsschutz

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 Bundesamts für Verfassungsschutz** 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 ist einer der drei Nachrichtendienste des Bundes. Als Inlandsnachrichtendienst ist der Verfassungsschutz ein wichtiger Bestandteil der deutschen Sicherheitsarchitektur. Als Frühwarnsystem hat er zuvorderst die Aufgabe, die absoluten und unabänderlichen Werteprinzipien zu schützen, die unseren demokratischen Rechtsstaat ausmachen: **die freiheitliche demokratische Grundordnung**. Um die Sicherheit der Bundesrepublik Deutschland vor Bestrebungen gegen diese Werteprinzipien durch Terrorismus und politischen wie religiösen Extremismus zu schützen, sammelt und analysiert der Verfassungsschutz – in enger Zusammenarbeit mit den Landesämtern 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.

Spionage & Konkurrenzausspähung

Wirtschaftsspionage wird von fremden Staaten unter Einsatz nachrichtendienstlicher Methoden betrieben.

Konkurrenz- oder Industriespionage bezeichnet die Ausspähung von Unternehmen durch andere Unternehmen. Oft tarnen fremde Staaten jedoch ihre Wirtschaftsspionage 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 und Sabotage durch staatliche 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 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 die beteiligten Akteure und über die angewandten 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 – Single Point of Contact

Das BfV verfügt über umfangreiche Erkenntnisse zu möglichen Angreifern, ihren Zielen und Methoden und unterstützt Wirtschaft und Wissenschaft mit zielgruppengerechten Sensibilisierungsangeboten. Der Bereich Prävention (Wirtschafts- und Wissenschaftsschutz) innerhalb des BfV ist dabei zentraler Ansprechpartner 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 45% 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 Mitarbeiterzufriedenheit 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 Infrastruktur (KRITIS). Zweck ist es, Einrichtungen, die für das Gemeinwesen unverzichtbar sind, wie die Sicherheit der Energieversorgung oder Telekommunikation, vor potentiellen 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 Kritischen Infrastruktur 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 Sicherheitsprüfung 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.

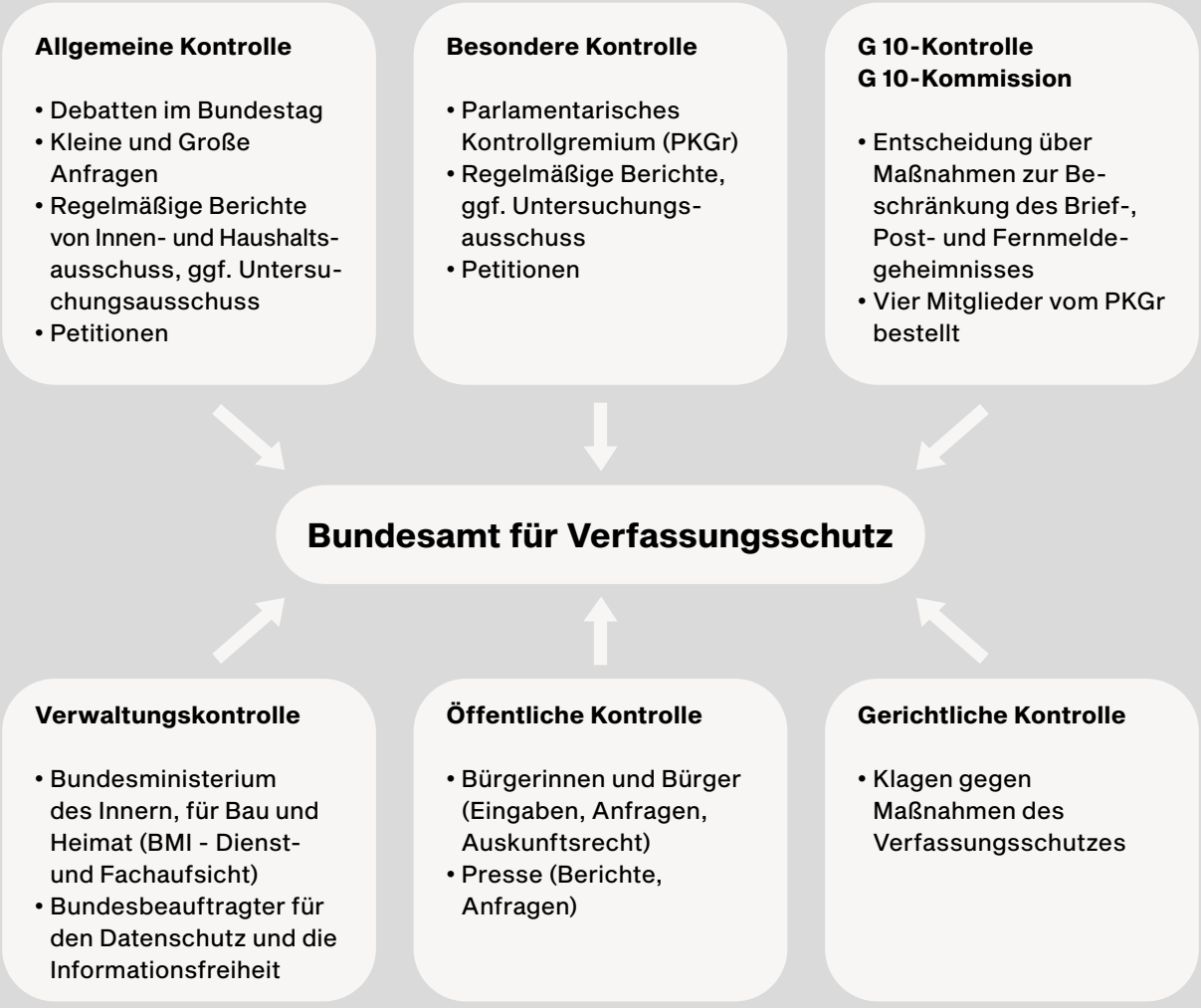
Auch im Bereich des präventiven Wirtschaftsschutzes arbeiten die zuständigen Landesbehörden vernetzt und stehen im regelmäßigen Austausch. Auf diese Weise entsteht ein starkes Netzwerk bis zu den Unternehmen vor Ort. Unser Tipp: Nehmen Sie unabhängig von einem konkreten Verdachtsfall schon einmal Kontakt zum Wirtschaftsschutzbereich ihres Landesamtes 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 **+49 (0)30 18 792 33 22**.

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**



Bildcredits

S. 15 Bundesamt für Verfassungsschutz, S. 17 Unsplash/@theasophie, S. 18 Markus Winkler, S. 20 Bundesamt für Verfassungsschutz, S. 21 Brian A. Jackson, S. 22 izusek/istockphoto, S. 24 Clay Banks, S. 26 Bundesamt für Verfassungsschutz

ALBTRAUM statt Traumjob

Case Study am Beispiel der APT-Gruppierung Lazarus

Redaktion: Cyberabwehr **Illustration:** Sonja Marterner

Schon lange treibt die Hackergruppe Lazarus ihr Unwesen. In einer groß angelegten Spionagekampagne gegen die Rüstungsindustrie, die nun schon seit Herbst 2019 andauert, erbeutet Lazarus geschützte Informationen und akquiriert im Einzelfall sogar finanzielle Mittel. Auch deutsche Konzerne stehen dabei im Fokus der Hacker. Gesteuert wird die Gruppierung vermutlich durch nordkoreanische Nachrichtendienste.

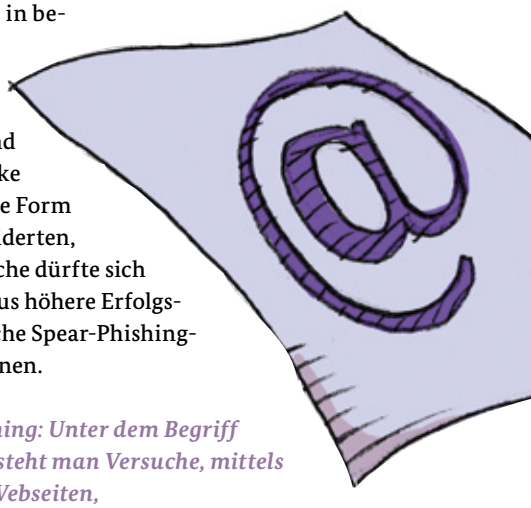
In der Frühphase ihrer Aktivitäten fiel Lazarus insbesondere durch Vergeltungsaktionen auf, zum Beispiel mit dem „Sony Pictures Hack“ in 2014 als Reaktion auf den Nordkorea-kritischen Film „The Interview“ sowie durch finanziell motivierte Angriffe auf Banken und Kryptowährungsbörsen. Doch zunehmend zeichnet sich bei der APT-Gruppierung (u.a. auch bekannt als Labyrinth Chollima, Andariel oder APT38) eine wachsende Professionalisierung ab, die eine entsprechend umfangreiche personelle und finanzielle Ausstattung vermuten lässt. 2015 bezifferte Reuters den Schaden auf bis zu 100 Millionen Dollar.[1]

> *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.*

So widmete sich Lazarus in jüngerer Vergangenheit vermehrt der „klassischen“ Cyberspionage zu Themen von strategischer und wirtschaftlicher Bedeutung für das nordkoreanische Regime. Im Verlauf der Covid-19-Pandemie hat sich der Fokus der Hacker zudem erweitert und Lazarus nimmt nun auch Organisationen der Pharma- und Gesundheitsbranche ins Visier, insbesondere Unternehmen und Forschungseinrichtungen, die einen Bezug oder Informationen zu Corona-Impfstoffen haben.
In ihrem Vorgehen setzt Lazarus auf ausgefeilte Social Engineering-Methoden, die im Folgenden skizziert werden.

Die Anbahnung

Zur Annäherung an ihre Opfer legen die Angreifer zunächst Fake-Profile in Karrierenetzwerken an, in denen sie sich als Headhunterinnen und Headhunter oder Beschäftigte der Personalabteilung namhafter Unternehmen ausgeben. Selbst die Profile realer Personen wurden zu diesem Zweck von Lazarus gefälscht.
Um den Profilen Legitimität zu verleihen, vernetzen sich die Angreifer zusätzlich mit Angestellten des vermeintlichen Arbeitgebers. Über die Fake-Profile schreiben sie schließlich Zielpersonen in den Unternehmen an, schicken diesen gefälschte Jobangebote und erlangen so ihr Vertrauen. Um die Kommunikation auf Messenger-Dienste umzulenken, verlangen die Angreifer schließlich nach weiteren Kontaktdaten. Letztendlich erfolgte die Ansprache in besagter Kampagne mitunter über mehrere Social Media- und Karrierenetzwerke gleichzeitig. Diese Form der maßgeschneiderten, direkten Ansprache dürfte sich durch eine weitaus höhere Erfolgsquote als klassische Spear-Phishing-E-Mails auszeichnen.

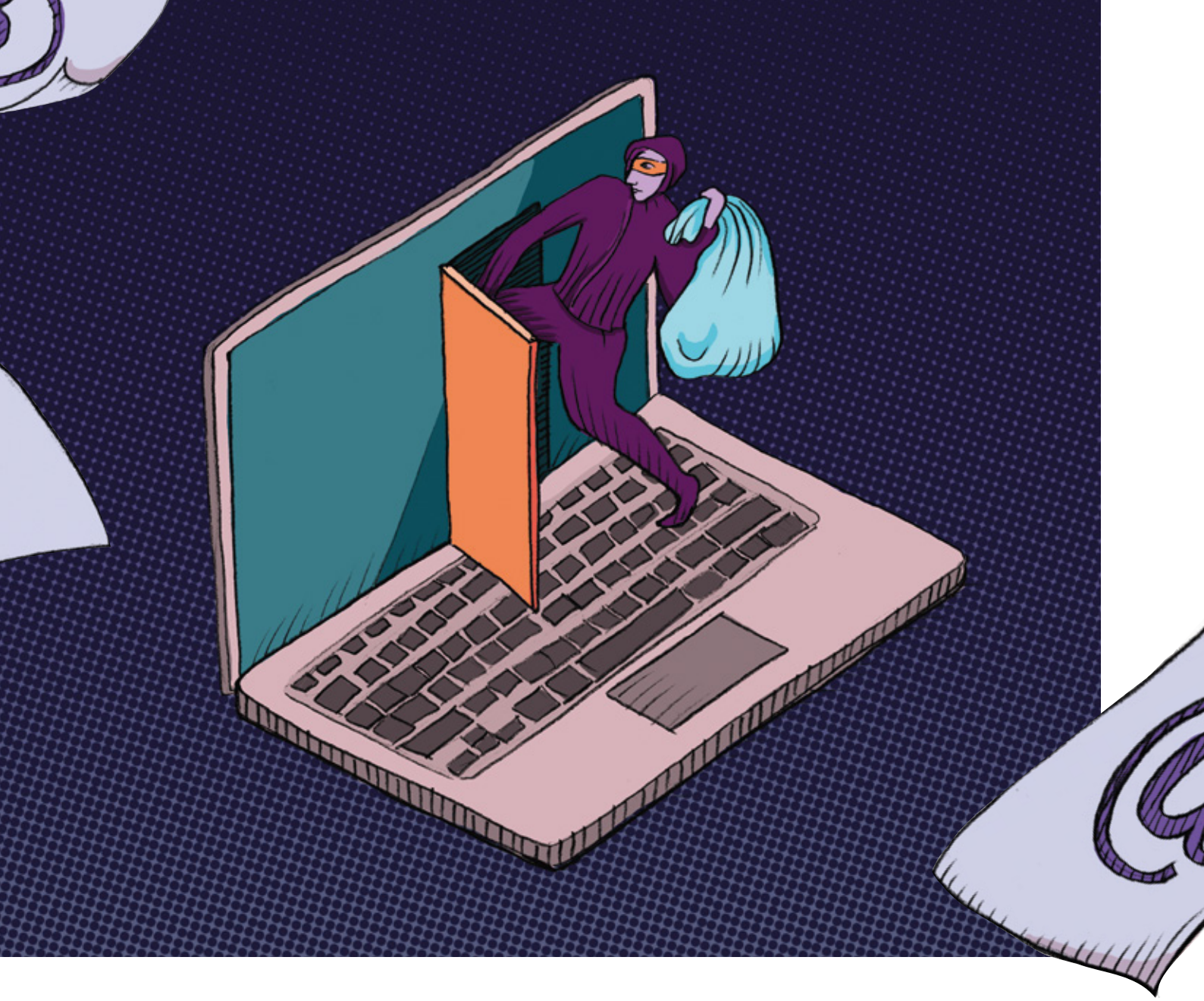


> *(Spear-)Phishing: Unter dem Begriff Phishing versteht man Versuche, mittels gefälschter Webseiten, E-Mails oder Kurznachrichten an persönliche Daten von Internetnutzerinnen und Internetnutzern, insbesondere Login-Informationen, zu gelangen. Sobald der Angreifer es gezielt auf bestimmte Personen, Unternehmen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

Das Übersenden des Köderdokuments

Nach erfolgreicher Anbahnung wird den angesprochenen Angestellten ein Dokument – im Corporate Design des vorgeblichen Arbeitgebers – mit vermeintlichen Details zum Jobangebot gesendet. Dabei handelt es sich um PDFs mit beigefügtem maliziösem PDF-Reader oder um Word-Dokumente mit versteckter Schadfunktion.
Eine Reaktion auf das Stellenangebot einfordernd, werden die Opfer von den Angreifern zum Öffnen der schadhaften Anhänge gedrängt. Eine Fehlermeldung erklärt, dass das Dokument nicht ordnungsgemäß geöffnet werden kann und die angesprochenen Personen werden verleitet, das Dokument auf unterschiedliche Rechner oder Mobilgeräte zu übertragen und die Ausführung von Makros zu erlauben. Mitunter enthalten die genutzten Microsoft Office-Köderdokumente selbst gar keine schadhaften Inhalte, verweisen jedoch auf eine externe Ressource. Über diese wird Microsoft Office veranlasst, eine Dokumentenvorlage-Datei mit maliziösem Makro aus dem Internet nachzuladen und auszuführen: eine sogenannte

[1] https://www.manager-magazin.de/digitales/it/sony-filmstudio-hackerschaden-ist-von-versicherung-gedeckt-a-1012169.html



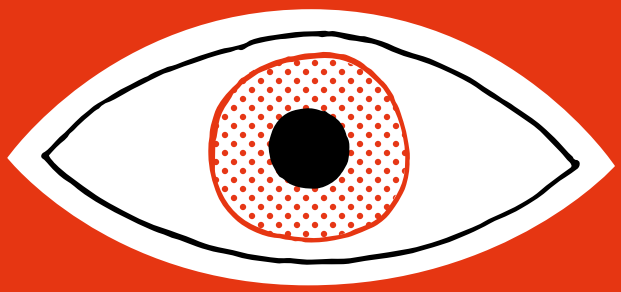
„Remote Template Injection“. Nachdem die externe Ressource geladen ist, erscheint ein Schutzdialog von Microsoft Office, der vor dem Ausführen von Makros warnt. Da das Köderdokument einen legitim erscheinenden Inhalt aufweist, wird die Ausführung der Makros von den jeweils betroffenen Personen in der Regel erlaubt.

Die Infektion

Haben die Angreifer so Zugriff auf das System erlangt, kundschaften sie zunächst das weitere Unternehmensnetzwerk aus und suchen nach Sicherheitslücken, beispielsweise aufgrund unterbliebener Updates. Nach erfolgreichem Kompromittieren des Netzwerks werden ausgewählte Dokumente oder Dateien in Archiven, beispielsweise im .zip und .cab-Format, zusammengezogen und verschlüsselt innerhalb des Netzwerks zu sorgfältig ausgewählten Ausleitungsknoten übermittelt. Die Cyberspione haben ihr Ziel erreicht.

Ausblick

Die zusammengefasste Kampagne macht die stete Weiterentwicklung der Methoden der APT-Gruppierung Lazarus deutlich. Charakteristisch sind der erhebliche Aufwand und zeitliche Vorlauf, mittels derer das eigentliche Kompromittieren durch professionelles Social Engineering vorbereitet wird. Es verdichtet sich die Vermutung einer professionellen und schlagkräftigen Cyberspionage-Gruppierung mit weltweitem Operationsradius. Es ist davon auszugehen, dass in Zukunft auch Unternehmen und Einrichtungen mit zeitgemäßer IT-Sicherheitsarchitektur Ziele derlei Spionageaktivitäten mittels immer aufwändigerem Social Engineering werden.



Chinas neue Wege der Spionage

Redaktion: Spionageabwehr **Illustration:** Sonja Marterner

Es war eine beeindruckende Zahl, die FBI-Direktor Christopher Wray anlässlich des zweiten Geburtstages der Chinainitiative des Attorney General im November 2020 verlautbaren ließ.[1] Seinen Angaben zufolge eröffnet das FBI alle zehn Stunden einen neuen Spionagefall mit Bezügen zu China.[2] Korrespondierenden Angaben des US-Justizministeriums im Februar 2021 zufolge bestehen zudem in etwa 80% aller Wirtschaftsspionagefälle Anhaltspunkte, die einen Nutzen für den chinesischen Staat nahelegen sowie in etwa 60% der Fälle des Diebstahls von Geschäftsgeheimnissen irgendwie geartete Verbindungen zu China.[3]

Auch wenn diese Daten und deren Veröffentlichung sicherlich hinterfragt werden beziehungsweise in Teilen politisch motiviert sein könnten, so zeigen sie eindrucksvoll, wie weit Chinas Bereitschaft geht, die eigenen Interessen zu verfolgen. Das Land lebt den „Chinesischen Traum",[4] in den nächsten Jahren zur weltweit führenden Industrie- und Technologiemacht zu werden, auch mit illegitimen Methoden. Nicht umsonst werden chinesische Ausspähbemühungen in den USA inzwischen von höchsten Stellen offen als Bedrohung für die wirtschaftliche und in der Folge die nationale Sicherheit eingestuft.[5] Welche Maßnahmen die US-Regierung in diesem Zusammenhang ergreift, zeigt eindrucksvoll auch die im Juli 2020 angeordnete Schließung des chinesischen Konsulats in Houston. Der ehemalige US-Außenminister Pompeo bezeichnete dieses als „Drehkreuz der Spionage und des Diebstahls geistigen Eigentums".[6]

Bereits seit Jahren betreibt die Volksrepublik China ein umfassendes und einzigartiges System des Technologietransfers mit dem Ziel, die zivile und militärische Entwicklung des Landes voranzutreiben und international seine Machtposition auszubauen und zu stärken. Dabei verfolgt die politische Führung eine ganzheitliche und gesamtgesellschaftliche Strategie („whole-of-society-approach") und findet passgenaue Wege zur Erreichung der eigenen Ziele.
Die wirtschaftlichen und wissenschaftlichen Ambitionen Chinas, niedergelegt unter anderem in dem Masterplan „Made in China 2025" oder den Fünf-Jahres-Plänen, verlangen unter anderem von den Nachrichtendiensten, aber zunehmend auch von sogenannten „non-traditional-actors", sensible Informationen aus den Bereichen Wirtschaft, Wissenschaft und Technik zu beschaffen.

[1] Die Chinainitiative wurde im November 2018 ins Leben gerufen und identifiziert Ziele für das US-Justizministerium, wie beispielsweise eine Priorisierung im Hinblick auf die Ermittlung und Verfolgung von Fällen des Diebstahls von Geschäftsgeheimnissen und Wirtschaftsspionage oder den Umgang mit chinesischen Direktinvestitionen.
[2] https://www.justice.gov/opa/pr/china-initiative-year-review-2019-20
[3] https://www.justice.gov/nsd/information-about-department-justice-s-china-initiative-and-compilation-china-related
[4] https://www.dw.com/de/xi-jinping-und-der-chinesische-traum/a-43545156
[5] https://www.fbi.gov/news/speeches/responding-effectively-to-the-chinese-economic-espionage-threat
[6] https://www.zeit.de/politik/ausland/2020-07/houston-china-usa-konsulat-raeumung-vergeltung-spionagevorwuerfe

‘Made in China 2025’ zielt darauf ab, bis zum Jahr 2025 aus China die stärkste Wirtschaftsmacht der Welt zu machen.

non-traditional-actors: Der Begriff bezeichnet Staatsangehörige eines Landes, die anlassbezogen oder dauerhaft Spionage in einem anderen Land betreiben, dies jedoch ohne eine formelle Zugehörigkeit zu einem Nachrichtendienst. Zur Rektrutierung von non-traditionals wird bevorzugt auf Personen aus der Wissenschaft, auf Studierende oder auf Arbeitskräfte im Ausland zurückgegriffen.

Intensives Interesse besteht beispielsweise an der wissenschaftlichen Forschung auf den Gebieten der Mikroelektronik, der Biotechnologie, der Umwelttechnologie und der erneuerbaren Energien. Im Grunde genommen ist aber kein Wirtschaftszweig mehr vor Chinas Spionen sicher. Zudem bemüht sich das Land immer intensiver um Zugänge zu Forschungs- und Wissenschaftseinrichtungen.

Made in China 2025 (MIC25): Die im Mai 2015 vom chinesischen Staatsrat verabschiedete Strategie MIC25 zielt darauf ab, bis zum Jahr 2025 aus China – mit allen Mitteln einer staatlich gelenkten Wirtschaft – die stärkste Wirtschaftsmacht der Welt zu machen. Der Schwerpunkt dabei liegt auf zehn Zukunftsbranchen, in denen China die globale Markt- und Technologieführerschaft anstrebt: Meerestechnik und Schifffahrt, Schienenverkehrstechnik und Eisenbahn, neue Energien und alternative Antriebe, neue Werkstoffe, Landwirtschaft, Medizintechnik, elektrische Ausrüstung, Industrierobotik und Roboterbau, neue Informationstechnologien, Luft- und Raumfahrttechnik.

Die Herausforderung besteht insbesondere auch darin, die Vielseitigkeit der Mittel und Wege nach-

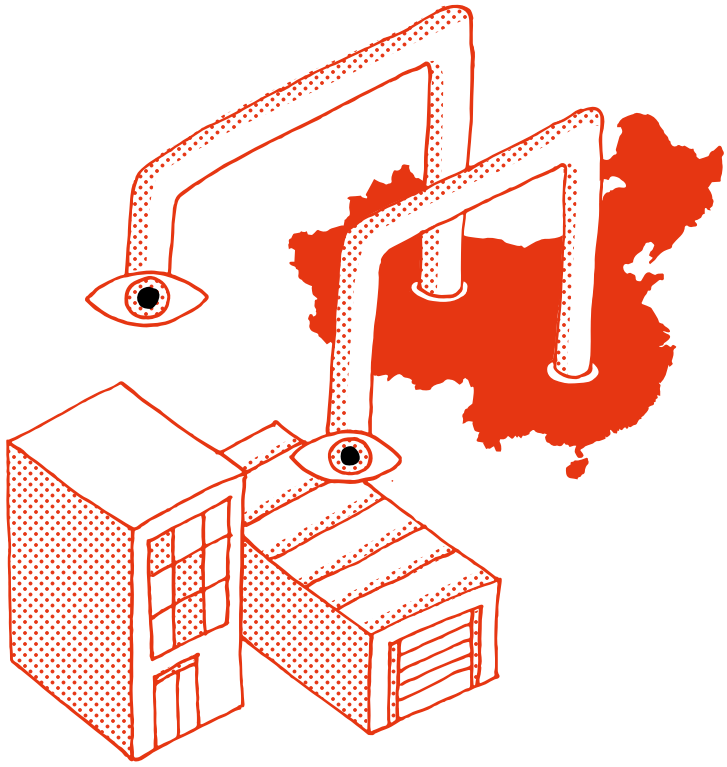
vollziehen und diesen mit geeigneten Gegenmaßnahmen begegnen zu können. Diese reichen von legalen bis illegalen, von legitimen bis illegitimen Mitteln. Hinzu kommt, dass es nahezu unmöglich ist, staatliche Wirtschaftsspionage und privatwirtschaftliche Konkurrenzausspähung voneinander zu trennen. Zwar spielen die chinesischen Nachrichtendienste auch weiter eine zentrale Rolle. Sie werden aber parallel immer häufiger auch durch andere Akteure, seien es Unternehmensvertreterinnen und -vertreter im Ausland oder kriminelle Hacker-Gruppierungen in der Heimat, in ihren Ausforschungs- und Beschaffungsbemühungen unterstützt. Neben deutlich erweiterten Angriffsmöglichkeiten bietet das aus chinesischer Sicht zusätzlich den Vorteil, dass aufgedeckte Spionageversuche einfacher dementierbar sind.

Auch in der Wissenschaft ist dieser Trend zur „Non-Professionalisierung" von Spionage feststellbar. So werden etwa chinesische wissenschaftliche Arbeitskräfte, die zu Besuch an Universitäten oder Forschungseinrichtungen im Ausland sind, ganz gezielt mit Ausforschungs- und Beschaffungsaufträgen betraut. Parallel sorgen Programme wie der „Tausend-Talente-Plan" dafür, dass auch Wissenschaftlerinnen und Wissenschaftler aus anderen Ländern ihre Expertise in den Dienst Chinas stellen und so dem Land zum Aufstieg im globalen Mächtekonzert verhelfen.

Tausend-Talente-Plan (TTP): Mit ihrem TTP setzte die chinesische Regierung ab 2008 gezielt Anreize für chinesisch-stämmige Wissenschaftlerinnen und Wissenschaftler im Ausland, ihre Forschungsarbeit nach China zu verlegen (und damit ihre Ergebnisse effektiv in den Dienst des Staates zu stellen). Gefragte Fachleute erhielten nicht nur umfangreiche Forschungsmittel und Ehrungen, sondern auch Gehälter, die teils das Drei- oder Vierfache des marktüblichen Niveaus erreichten. Nachdem international immer mehr Vorwürfe laut wurden, wonach das Programm lediglich dem illegitimen Know-how-Abfluss diente, stellte China die öffentliche Werbung für das Programm 2018 ein. Ungeachtet dessen läuft es aber bis heute fort, genauso wie zahlreiche ähnliche Programme.[7]

Besonders deutlich wird das chinesische Bestreben, alle Mittel und Wege der Wissensbeschaffung zum Zwecke des Machtzuwachses zu verbessern, im Konzept der „zivil-militärischen Fusion", das 2015 erstmalig formuliert und 2017 mit Gründung der „Zentralkommission für integrierte militärische und zivile Entwicklung" auch offiziell zur nationalen Strategie wurde.[8] Wie Staats- und Parteichef Xi Jinping seither in steter Regelmäßigkeit öffentlich ausgeführt hat, sei der Chinesische Traum nur zu erreichen, wenn parallel auch die entsprechende „harte", also militärische, Komponente zur Absicherung chinesischer Interessen gestärkt werde. Dafür wiederum benötige das Land die modernsten Technologien, egal woher diese stammen.[9]

Im Hinblick auf den Modus Operandi sind sowohl klassische Spionageaktivitäten als auch hybride Vorgehensweisen zu beobachten. Das konkrete Vorgehen orientiert sich dabei am jeweiligen Bedarf und Aufklärungsobjekt und lässt sich flexibel anpassen. Hoch frequentiert zur Etablierung wichtiger Kontakte sind Social Media-Plattformen, insbesondere Karrierenetzwerke wie LinkedIn oder Xing, aber auch (Fach)Konferenzen und Tagungen, Wirtschaftsdelegationen und Studentenaustauschprogramme. Das weitere gezielte Vorgehen reicht dann wiederum



[7] https://www.nytimes.com/2020/02/06/us/chinas-lavish-funds-lured-us-scientists-what-did-it-get-in-return.html
[8] https://www.wsj.com/articles/china-taps-its-private-sector-to-boost-its-military-raising-alarms-11569403806
[9] https://2017-2021.state.gov/chinas-military-civil-fusion-strategy-poses-a-risk-to-national-security/index.html

vom Hackerangriff über die Nutzung von Scheinfirmen bis zum physischen Entwenden von Daten.

China macht sich dabei ganz gezielt die Offenheit der westlichen Gesellschaften zunutze. Während etwa in den USA oder in Europa die zivilgesellschaftliche Sphäre (Unternehmen, Forschungseinrichtungen, Universitäten usw.) und die staatliche Sphäre (Regierung, Behörden, Militär usw.) zumeist deutlich voneinander zu trennen sind, ist in China das genaue Gegenteil der Fall.

Dort sind die Grenzen zwischen den Institutionen des Parteienstaates und den übrigen gesellschaftlichen Sektoren unscharf gezogen. Die Aktivitäten des Einzelnen haben sich den – zentral durch die Kommunistische Partei (KPCh) definierten – Zielen des Kollektivs unterzuordnen. Die Wege der Steuerung sind dabei vielfältig. Bei Firmen in staatlichem Besitz sind sie vielleicht noch augenfällig. Anders sieht es bei Unternehmen aus, die sich komplett in privater Hand befinden. Aber auch hier trägt die KPCh mit Instrumenten wie dem „Nationalen Geheimdienstgesetz“ oder dem Zwang, unternehmenseigene Parteizellen einzurichten, dafür Sorge, dass ihre Interessen Berücksichtigung finden.

> ***Nationales Geheimdienstgesetz (NGG): Im Juli 2017 verabschiedete der chinesische Volkskongress das neue NGG. Dadurch haben die Sicherheitsbehörden nun zahlreiche förmlich kodifizierte Sonderrechte, um nahezu ohne Einschränkungen im In- und Ausland nachrichtendienstlich tätig zu sein. Das NGG sieht u. a. auch vor, Einzelpersonen, Firmen, staatliche Strukturen und sonstige Organisationen im In- und Ausland zur Mitarbeit zu verpflichten.[10]***

Bereits im September 2020 hatte darüber hinaus das Generalbüro des Zentralkomitees der KPCh erstmals „Ansichten“ zur Privatwirtschaft veröffentlicht. Diese wurden am 16. September 2020 auf der „Nationalen Konferenz der Einheitsfront in der Privatwirtschaft“ präsentiert. Laut dieser Ansichten müsse die Partei dafür ihre Führungsrolle in der Privatwirtschaft auch durch die Einheitsfrontarbeit verstärken und Privatunternehmen zu stärkerem Engagement bei der Umsetzung der Parteipolitik erziehen und anleiten. Nach außen sollten sie den Austausch mit Weltklasse-Unternehmen betreiben, die nationalen Interessen Chinas verteidigen und beim Aufbau eines positiven Chinabilds mitwirken.[11] Hier wird erneut deutlich, dass die KPCh ihren Einfluss kontinuierlich auf allen Ebenen ausbaut, um die von ihr formulierten Ziele zu verwirklichen.

Das Risiko des Technologietransfers, auch im militärischen Bereich, steigt. Während große Konzerne im Hinblick auf diese Gefahren in der Regel sensibilisiert sind, sind sich insbesondere kleine und mittlere Unternehmen (KMU) sowie Start-ups auch heute noch schlicht nicht der Gefahren bewusst. Gleiches gilt oftmals für Universitäten und sonstige Forschungseinrichtungen.

Die mit der Abwehr von Spionage betrauten Stellen in den westlichen Ländern, aber auch die Gesellschaften insgesamt, täten daher gut daran, sich auf diese neue Dimension chinesischer Ausspähungsbemühungen einzustellen und entsprechende Gegenstrategien zu entwickeln. Denn wenn es richtig ist, dass Chinas Spione, wie es FBI-Direktor Wray formuliert, aus der langfristigen Perspektive eine Kunstform gemacht haben und einen allumfassenden Ansatz verfolgen, wird die Herausforderung in absehbarer Zeit weiter wachsen.

---

www.justice.gov
www.fbi.gov
www.bsi-fuer-buerger.de
www.verfassungsschutz.de
www.state.gov
www.aspi.org.au

[10] https://www.verfassungsschutz.de/embed/vsbericht-2018.pdf
[11] https://www.csis.org/analysis/chinese-communist-party-targets-private -sector

DEEPFAKE

Auf dem Weg zu Social Engineering 2.0?

Redaktion: Wirtschaftsschutz BfV **Illustration:** Sonnenstaub

Mark Zuckerberg verkauft Dialyse-Behandlungen an der Ecke Laramie & Fairfax in Cheyenne (USA), Richard Nixon hält eine Rede über die gescheiterte Mondlandung 1969 und Tom Cruise führt auf TikTok Taschenspielertricks auf.

Was 2017 als Witz-Trend im Internet startete, hat bis heute erschreckend realistische Ausmaße angenommen. Denn alle drei Videos sind Fälschungen, sogenannte Deepfake-Videos.

> ***Das Wort Deepfake ist eine Wortneuschöpfung, die sich aus den englischen Begriffen Deep Learning und Fake zusammensetzt. Ein Deepfake bezeichnet eine durch Künstliche Intelligenz manipulierte Video- oder Tondatei, geschaffen als Kunst- und Anschauungsobjekt oder aber als Mittel zur Diskreditierung, Manipulation und Propaganda.[1]***

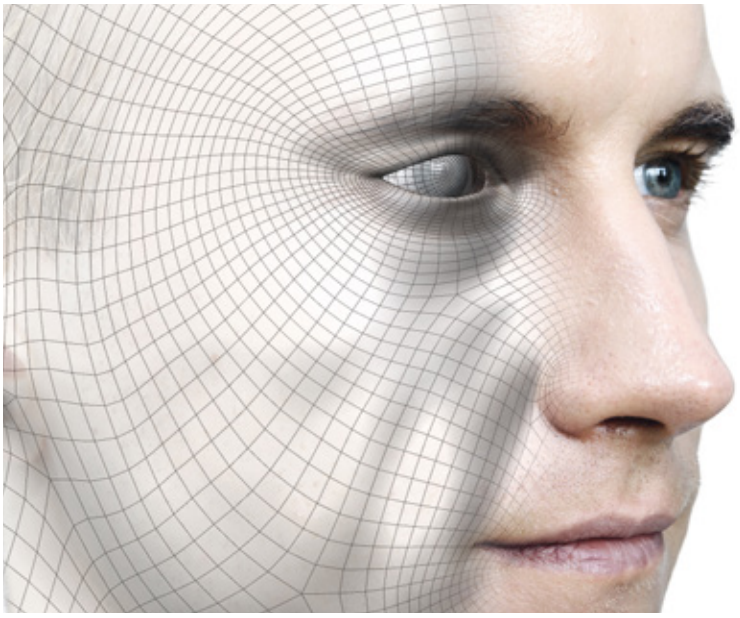
Deepfakes wurden durch die rasanten Entwicklungen auf dem Gebiet der Künstlichen Intelligenz (KI) und deren Teilbereich Maschinelles Lernen möglich. KI ist eine Schlüsseltechnologie, deren Stärke in der Analyse großer Datenmengen in sehr kurzer Zeit liegt. Zudem ist KI ein globaler Megatrend. Ein Trend, der nahezu all unsere Lebensbereiche betrifft und das Potenzial birgt, unser Leben grundlegend zu ändern.

Schon jetzt findet KI vielfältige Anwendungen: In Krankenhäusern ersetzt sie langwierige und kostspielige Analysen und ermöglicht eine schnellere Diagnostik. Wer heute bei großen Versandhändlern einkauft oder bei seiner Bank Kontakt mit dem Support aufnimmt, kennt bereits „Chatbots". Das Fraunhofer-Institut forscht an KI-gestützter Emotionserkennung in Fahrzeugen. Auf dem Gebiet der digitalen Assistenten und deren vielfältigen Einsatzmöglichkeiten gab es in den letzten Jahren bereits große Fortschritte.

Was passiert jedoch, wenn eine Technologie wie KI von ausländischen Nachrichtendiensten, von Gruppen oder Einzelpersonen missbraucht wird? Was bedeutet dies für die Themen Cybersicherheit oder Wirtschaftsspionage? Und wo besteht die Verbindung zwischen Social Engineering und Deepfakes?

Der erste bekannt gewordene Social Engineering-Betrugsfall, der mutmaßlich mittels einer KI durchgeführt wurde, ereignete sich im August 2019. Opfer wurde der CEO eines britischen Energieunternehmens. Dieser erhielt insgesamt drei Anrufe des Vorstandsvorsitzenden der deutschen Muttergesellschaft, bei denen letztendlich 243.000 Dollar auf ein fremdes Konto überwiesen wurden. Was dem britischen CEO nicht auffiel: Die Stimme des vermeintlichen Gesprächspartners wurde durch eine KI-Software imitiert.

Mit zunehmender Entwicklung der KI wird es Angreifern immer leichter fallen, Personen in Ton- und Videoaufnahmen nahezu perfekt nachzuahmen. Doch schon längst geht es nicht mehr nur um manipulierte und anschließend veröffentlichte Ton- und Videoaufnahmen, sondern auch um Live-Manipulation während eines Videocalls. Für Nachrichtendienste, Wirtschaftsspione, Hacker oder Social Engineers eröffnen sich so mittels Deepfake vollkommen neue Möglichkeiten der Manipulation und Datenabschöpfung. Das Perfide



Das Heimtückische an Deepfakes ist, dass Angreifer nicht erst Vertrauen aufbauen müssen.

Foto: Jiraroj Praditcharoenkul

[1] https://www.duden.de/presse/anglizismus-des-jahres-2019 und https://wirtschaftslexikon.gabler.de/definition/deepfake-120960

daran, im Vergleich zu bestehenden Social Engineering-Maßnahmen muss zum Opfer nicht zuerst Vertrauen aufgebaut werden, da die imitierte Person mutmaßlich bereits einen Vertrauensstatus beim Opfer hat.

Was bereits mit einem geringen bis mittleren technischen Sachverstand möglich ist, zeigt unter anderem die Software DeepFaceLab. Mit dieser Anwendung lassen sich innerhalb kurzer Zeit Deepfakes erstellen, die dem flüchtigen Blick auf dem Handy durchaus standhalten können.

Wie entstehen Deepfakes?

Früher war selbst für einfache Bildmanipulationen professionelle Software und Ausrüstung notwendig. Die Einstiegshürden in die Deepfake-Technologie sind im Gegensatz dazu extrem niedrig. Ein Deepfake besteht gerade einmal aus drei Komponenten:

- Der Originalszene so ähnlich wie möglich, auch in Ausleuchtung und Hintergrundgestaltung, nachgeahmte Szenen.
- Einem größtmöglichen Bestand an Videomaterial der Person, die imitiert werden soll. Angesichts Social Media stellt dies auch bei Privatpersonen mittlerweile kein größeres Problem mehr dar. Bereits mit ein bis zwei Minuten Videomaterial lässt sich ein halbwegs akzeptabler Clip erstellen[2].
- Computer mit entsprechender Rechenleistung und Software. Eine professionelle Software ist mitunter sogar kostenlos im Internet erhältlich, zusammen mit einigen nützlichen Tutorials.

Doch selbst kommerzielle Software, die über den AppStore erhältlich ist, kann nicht nur Lustiges produzieren. Mit nur wenigen Klicks auf dem Smartphone können auch Amateure ihren Vorgesetzten „Baby Girl“ singen lassen oder den Schwarm ein traumhaftes Liebeslied.

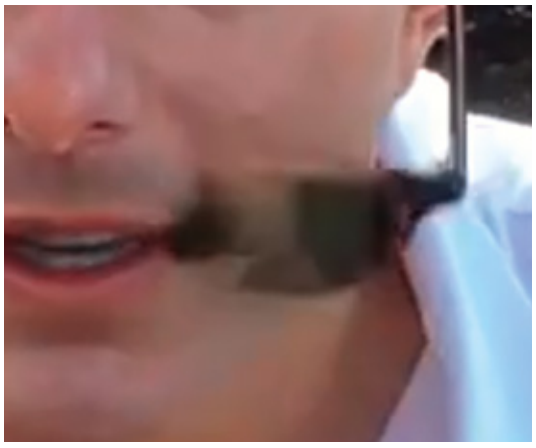
Wie sind Deepfakes zu erkennen?

- **AUF DIE UMGEBUNG ACHTEN!**
  Je höher die Auflösung bzw. die Bildgröße, desto leichter lassen sich Ungereimtheiten im Bild erkennen. Videos sollten daher nicht auf dem Handy, sondern auf einem größeren Monitor geschaut werden. Gute Farbeinstellungen zeigen ebenfalls Unstimmigkeiten, z. B. im Hautbild.

- **MIMIKEN ERKENNEN!**
  Natürliche Reaktionen, wie z. B. Blinzeln, Stirnrunzeln oder die berühmte „Zornesader“ können von einer KI ebenfalls noch nicht gut dargestellt werden. Ein genauer Blick auf die Augen und Stirn kann einen Fake schnell entarnen.

- **QUELLEN CHECKEN!**
  Letztlich hilft natürlich auch immer eine Quellenprüfung oder bei Unsicherheit die Bitte um Rückruf, um zumindest die Gelegenheit zu bekommen, den Videoanruf oder das Video zu verifizieren.

Wer in Live-Videos gegenüber seiner Kontaktperson misstrauisch ist, kann auch darum bitten, dass diese sich kurz an Nase oder Wange tippt. Die KI ist bis dato selbst in ihrer besten Form nicht in der Lage, diese Animation darzustellen. Das Bild würde sichtlich verzerrt werden. Hier empfehlen wir einen Blick auf die Arbeit des TikTok-Channels deeptomcruise, wo die Fakes so professionell erstellt sind, dass nur an einigen wenigen Stellen zum Beispiel ein fehlender Brillenbügel sichtbar wird[3].



Quelle: deeptomcruise bei TikTok

Auch wenn die gerade genannten Hilfestellungen zeigen, dass den Fähigkeiten der Künstlichen Intelligenz noch mit natürlicher Intelligenz entgegengetreten werden kann, so zeigt die Entwicklung der letzten vier Jahre auch die schöpferischen Fortschritte auf dem Gebiet der KI. Mit Blick auf die spektakulären und mit viel Aufwand betriebenen Hackerangriffe der letzten Jahre ist mit großer

[2] https://www.youtube.com/watch?v=EFR1XYZXhdU
[3] https://edition.cnn.com/videos/business/2021/03/02/tom-cruise-tiktok-deepfake-orig.cnn-business

Wahrscheinlichkeit davon auszugehen, dass gut ausgestattete Nachrichtendienste oder andere staatliche Akteure Deepfake als neue Angriffswaffe nutzen werden. Zwar gibt es bei Deepfake-Videos noch deutliche Lücken in der Darstellung, jedoch wäre vor gerade einmal fünf Jahren auch ein „wiederbelebter" Richard Nixon, der über die gescheiterte Mondlandung spricht, noch unmöglich gewesen.

Das Zeitalter von Social Engineering 2.0 und dessen großer Einfluss auf moderne Wirtschaftsspionage hat gerade erst begonnen und Sicherheitsverantwortliche in Wirtschaft und Forschung müssen den von Deepfake ausgehenden Gefahren entgegentreten. Erste Ansätze zielen darauf ab, die „angreifende" KI mit einer eigenen zu bekämpfen: so sollen KI-basierte Programme zukünftig eingehende Videos oder Streams auf bestimmte, eindeutige Auffälligkeiten prüfen.

3 FRAGEN AN ...

Prof. Dr. Martin Steinebach, Abteilungsleiter Media Security und IT-Forensics beim Fraunhofer SIT

Bei der aktuellen technologischen Entwicklung – wie lange wird es dauern, bis Deepfakes nicht mehr von authentischen Videos unterschieden werden können?

Wenn es nur um das rein Visuelle geht, also ob man bei einem Standbild ein Gesicht noch als eingefügt erkennen kann, ist damit zu rechnen, dass wir das mit dem bloßem Auge nicht mehr lange können. Das sind wahrscheinlich nur noch wenige Jahre, wenn überhaupt. Dabei muss man aber natürlich auch geeignetes Ausgangsmaterial vorliegen haben. Schwerer wird es, wenn man Verhalten, Mimik und Bewegungen miteinbeziehen möchte. Da würde ich noch einen längeren Zeitraum veranschlagen.

Gibt es eine Aussicht auf eine rein technische Lösung, die Deepfakes in der Praxis zuverlässig aufspürt?

Es kommt darauf an, wie zuverlässig die Erkennung sein soll. Deepfakes und ihre Erkennung werden wahrscheinlich nicht zu einem Punkt kommen, an dem eine der beiden Technologien die andere vollständig abhängt. In der Multimedia-Forensik kennen wir ja schon lange Fragestellungen wie die Erkennung von Bildmanipulationen, und bisher gibt es auch nach 20 Jahren Forschung keinen klaren Gewinner zwischen Manipulation und Erkennung. Aber natürlich werden die Methoden zur Erkennung auch immer besser werden und stetig weitere Faktoren miteinbeziehen.

Was raten Sie Unternehmen und Forschungseinrichtungen?

Wenn es darum geht, sich vor Deepfakes zu schützen, dann würde ich mich derzeit nicht darauf verlassen, mit einem technischen Verfahren Videos zu analysieren. Ich würde empfehlen, die Authentizität von Gesprächspartnerinnen und Gesprächspartnern mit geeigneten Protokollen zu prüfen, also beispielsweise Links zu Videokonferenzen nur von vertrauenswürdigen E-Mail-Adressen anzunehmen und die Integrität eines Videokanals zu prüfen. Aus Forschungssicht muss man bei der Erkennung sicher darüber nachdenken, welche Anhaltspunkte für Fälschungen noch betrachtet werden können. Bisher werden bei Deepfakes nur visuelle Daten manipuliert, aber nicht Verhalten. Daran erkennen dann menschliche Expertinnen und Experten Fälschungen, wenn sie die Personen gut kennen.

Portrait: © Josef Seitz/Fraunhofer SIT

Arbeite gemeinsam mit uns

IM AUFTRAG DER DEMOKRATIE!

Bewirb dich und komm in unser Team.

**Ob Ausbildung, Studium oder Direkteinstieg –
beim Verfassungsschutz erwarten dich vielfältige Einsatzmöglichkeiten.**

Bundesamt für Verfassungsschutz

WERDE VERFASSUNGSSCHÜTZER*IN.

Mehr Informationen unter
verfassungsschutz.de/karriere

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
verfassungsschutz.de