ZUKUNFTS STARK

SICHER IST?

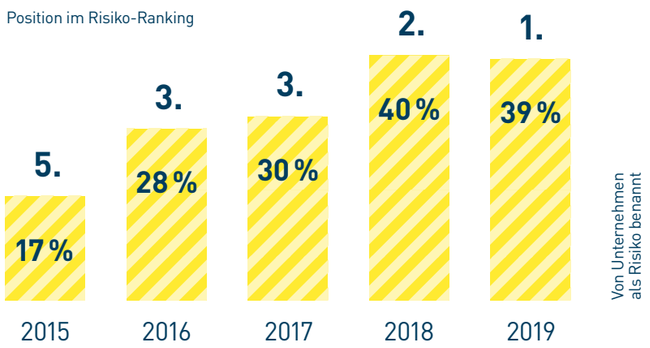
Ihr starker IT-Partner.
Heute und morgen.

BECHTLE

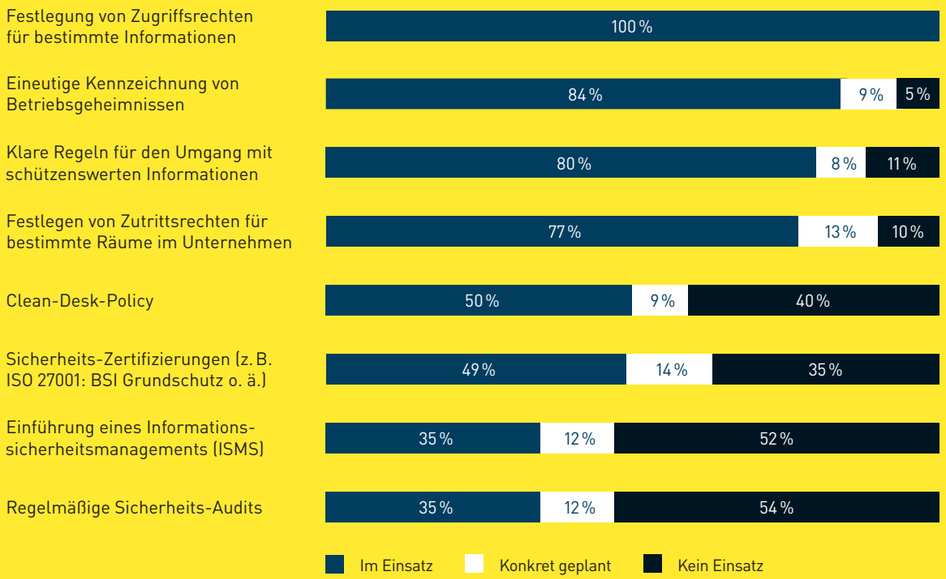
FÜNF GRÜNDE FÜR WIRTSCHAFTLICHE VERLUSTE NACH CYBERVORFÄLLEN.[7]

Betriebsunterbrechung	**69 %**
Reputationsverlust	55 %
Haftungsansprüche	48 %
Wiederherstellung	29 %
Bußgelder und Strafen	25 %

Risiko für Cybervorfälle weltweit immer höher eingeschätzt.[6]



WAS UNTERNEHMEN MACHEN, PLANEN, UNTERLASSEN.[5]



DAS GEHÖRT INS NOTFALLPAKET.

Empfehlung des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe

Grundvorrat an Lebensmitteln – für zehn Tage für eine Person:

20 Liter
Getränke (2 Liter pro Tag und Person).

0,357 kg
Fette, Öle.

2,5 kg
Obst, Nüsse.

4,0 kg
Gemüse, Hülsenfrüchte.

1,5 kg
Fisch, Fleisch, Eier, bzw. Volleipulver.

Alles Weitere: www.bbk.bund.de

2,6 kg
Milch, Milchprodukte.

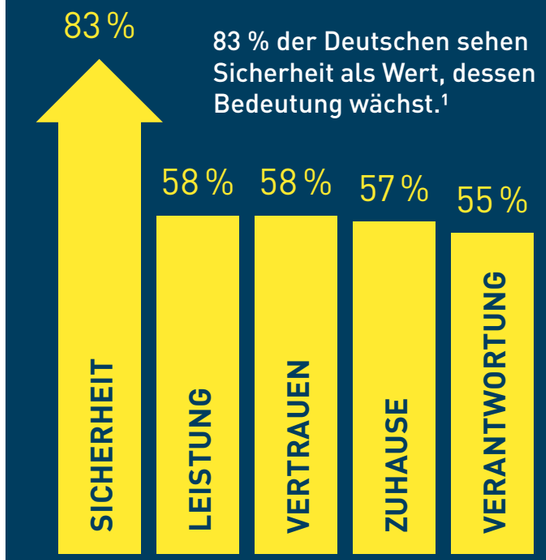
3,5 kg
Getreide, Getreideprodukte, Brot, Kartoffeln, Nudeln, Reis.

Sonstiges nach Belieben: z. B. Zucker, Süßstoff, Honig, Marmelade, Schokolade, Jodsalz, Fertiggerichte (z. B. Ravioli, Fertigsuppen), Kartoffeltrockenprodukte (z. B. Kartoffelbrei), Mehl, Instantbrühe, Kakaopulver, Hartkekse, Salzstangen …

QUELLEN 1 Gfk, CAPI BUS Umfrage 2016 | 2 Hasso-Plattner-Institut | 3 Statista | 4 Bundeskriminalamt | 5 Bitkom e.V. 2019
6 Allianz Risk Barometer 2019 | 7 Allianz Global Corporate & Specialty Figures

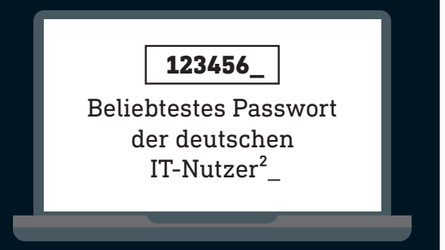
GESICHERTE DATEN.

TOP 5 DER WERTE.



83 % der Deutschen sehen Sicherheit als Wert, dessen Bedeutung wächst.[1]

30 MIO. IDENTITÄTS-DIEBSTÄHLE PRO MONAT.[2]



Beliebtestes Passwort der deutschen IT-Nutzer[2]_

5,2 Billionen $

geschätzter Umsatzverlust weltweit durch Cyberattacken in den Jahren 2019 bis 2023.[3]

geschätzter finanzieller Schaden durch Cyberkriminalität.[4]

Mehr als 90 % geschätzte Dunkelziffer bei Cyberkriminalität.[5]

87.106

FÄLLE VON CYBERKRIMINALITÄT 2018.[4]

RISIKEN, DIE DEUTSCHE UNTERNEHMEN AKTUELL SEHEN.[6]

BETRIEBSUNTERBRECHUNG 48 %

CYBERVORFALL 44 %

RECHTLICHE VERÄNDERUNGEN 35 %

NATURKATASTROPHEN 28 %

NEUE TECHNOLOGIEN 20 %

NICHTS RISKIEREN.
ALLES LESEN.

TOP-THEMA SICHERHEIT.

Atmen, essen, trinken, schlafen sind menschliche Grundbedürfnisse. Auf der nächsten Ebene der Bedürfnispyramide – nach dem US-amerikanischen Psychologen Abraham Maslow – steht schon die Sicherheit. Dazu zählen etwa materielle Grundsicherung, Arbeit, Wohnung, Gesundheit. Auch wenn man die Deutschen nach ihren wichtigsten Werten befragt, ist Sicherheit die ewige Nummer eins. Sie hat sogar an Bedeutung noch zugenommen. Vielleicht, weil die Welt sich schneller und stärker verändert und daher unsicherer erscheint.

Wir halten die Sicherheit auch in diesem Magazin hoch. Weil sie erfolgskritisch ist – und hochgradig ZUKUNFTSSTARK. In der IT, aber nicht nur. Wir präsentieren Projekte und gesellschaftliche Schutzräume, in denen Verbundenheit gelebt wird. Hier finden sich Konstruktionen für Gemeinschaften ganz unterschiedlicher Zusammenhänge – von innovativen Wohnformen bis zum generations- oder glaubensübergreifenden Brückenbau.

Was Bechtle selbst für IT-Sicherheit leistet, bildet den Kern unseres Schwerpunktthemas. Wir geben Einblick in unser allgemeines Verständnis davon und zeigen beispielhafte Herausforderungen auf. Wie gelingt es, mit einer präventiven Strategie Resilienz, also Widerstandsfähigkeit, aufzubauen? Wie begegnet man der manipulativen Kraft von Social Engineering? Was macht die Cloud wasserdicht und welchen Spuren gehen IT-Forensiker nach?

Und nebenbei geht's noch um Make-up und Bananenschalen, Sound Designer und Flugkapitäne, Bartverbote und knallende Kofferraumdeckel. Wie das zu verstehen ist? Das entdecken Sie sicher am liebsten selbst.

SICHER sein.

Willkommen auf der Suche nach dem Gelben vom Ei. Im Spannungsfeld zwischen Unsicherheit und Schutzbedürfnis, zwischen Komplexität und Wunsch nach Klarheit. Wir teilen unser Leben in sozialen Netzwerken, wollen aber unsere Privatsphäre gewahrt wissen und allzu persönliche Daten schützen. Unsere Gesellschaft diskutiert, ob öffentliche Videoüberwachung mehr Sicherheit oder Sozialkontrolle bedeutet, wägt zwischen Freiheit und Einschränkung ab. Und Unternehmen müssen Cyberattacken abwehren, ohne sich von globalen Wertschöpfungsketten abzuschotten. Was wir brauchen, sind intelligente Strategien, um in diesem Umfeld souverän zu agieren.

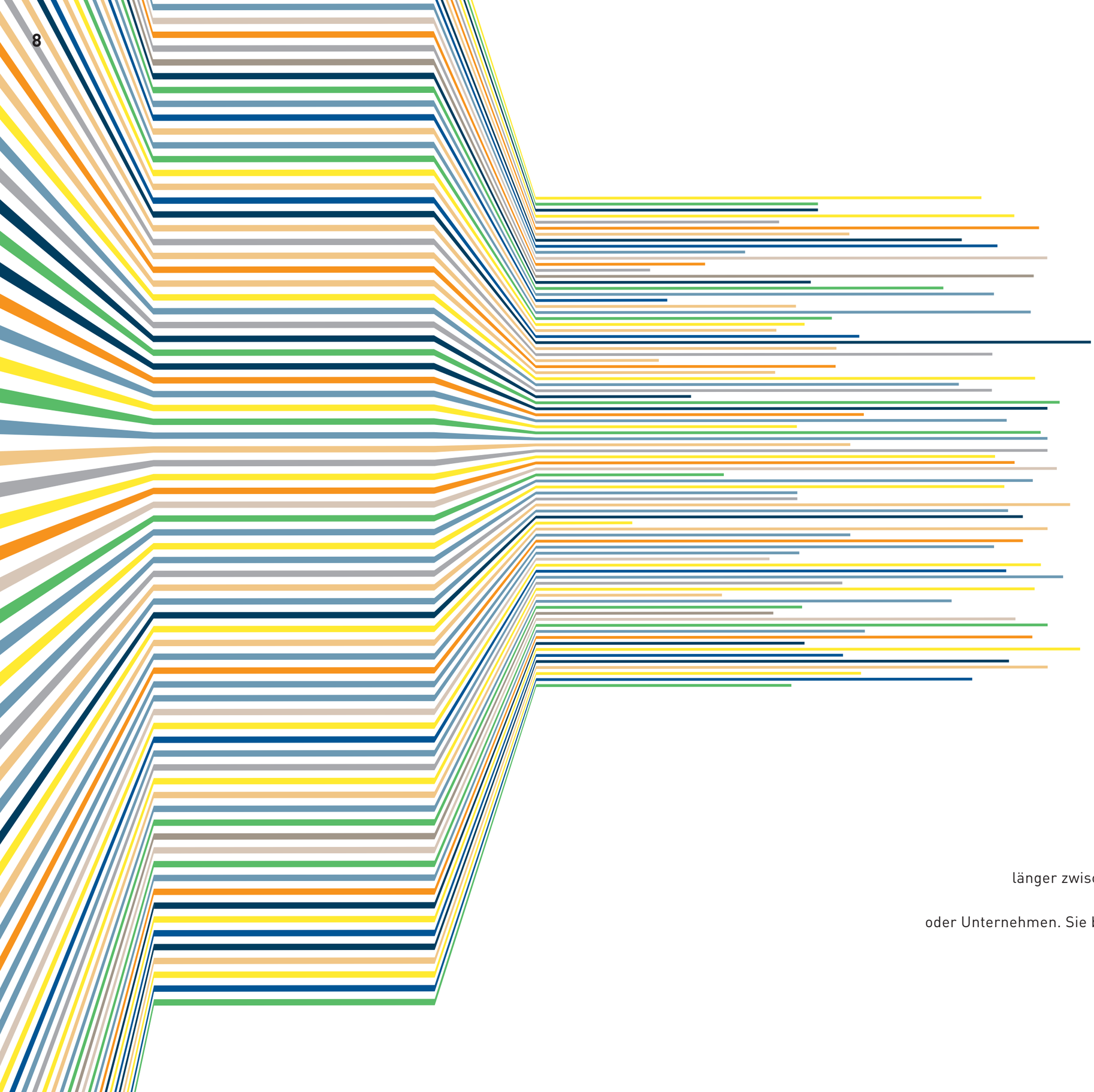
bleiben. OFFEN

Eins muss man Tesla Motors lassen: Das Unternehmen macht seine Technologiepatente offen zugänglich – mit dem Ziel, die Modernisierung der Mobilität insgesamt zu fördern und andere zur Mitwirkung einzuladen. Gleichzeitig ist Tesla mit dem automatisierten Fahren auf einem Gebiet unterwegs, das allerhöchste Sicherheitsanforderungen stellt. Das Beispiel kann als Anregung dienen, die eigenen Optionen zu durchdenken. Wie offen können wir (selbst) sein und was gewinnen wir (alle) damit? Welche Grenzen müssen wir ziehen, wo uns kompromisslos absichern? Und welche Regeln gelten zwischen den beiden Polen? Eindeutigkeit ist immer seltener zu haben. Wir sitzen dauerhaft zwischen den Stühlen, im Schwebezustand von sowohl – als auch, einer- und andererseits. Es ist wohl kein Zufall, dass die Quantenwelt im Begriff ist, spürbare Realität zu werden. Die Gleichzeitigkeit von Zuständen ist da Programm und soll zukünftige Rechnergenerationen befähigen, hochkomplexe Probleme im Nullkommanichts zu lösen.

Einstweilen müssen wir selbst mit vielfältigen spannungsreichen Anforderungen fertigwerden. Wie lässt sich in einer virtualisierten Welt mit unsichtbaren Bedrohungen gefühlte und faktische Sicherheit herstellen? Wie vermitteln wir zwischen flexiblen Beschäftigungsmodellen und Arbeitsplatzsicherheit? Was können wir unsere Sprachassistenten fragen, ohne zu viel über uns zu verraten? Wer hat die Macht über die Algorithmen, die uns Antworten geben? Wie viel Gewissheit finden wir in unseren Netzwerkgruppen und wie viel mehr Inspiration außerhalb?

Für den norwegischen Wirtschaftsphilosophen Anders Indset entspringt aus dem Wechselbad die Vision eines „Quantopia". Dort sollen Chaos und Stabilität zu einer Synthese finden. Sie basiert, man kann es sich schon denken, auf einer Quantenwirtschaft. Das Denkmodell entwickelt aus der Vieldeutigkeit einer nichtlinearen Welt das Potenzial für interdisziplinäres Zusammenwirken, das zu neuen, ungedachten Lösungsansätzen führt. Die können wir gewiss gebrauchen. Es gehört ein vertrauensvolles Miteinander dazu, auch aus gegensätzlichen Positionen heraus Optionen zu verhandeln und gemeinsam Lösungen zu entwickeln. So wie Unsicherheit zaudern lässt, verkennt Selbstgewissheit mitunter die Notwendigkeit von Veränderungen. Der bestmögliche Umgang mit Risiken braucht verschiedene Perspektiven. So kann der Diebstahl von Daten einen verheerenden Verlust bedeuten, während sich das gezielte Data Sharing gewinnbringend entwickelt und neue Allianzen ermöglicht. Der Korridor für Sicherheit mag ein schmaler Grat sein oder sich unvermutet weiten. Für den richtigen Weg helfen Leitlinien zur Orientierung, ja Regeln, aber auch die Offenheit für Diskussionen. Wissen erwerben und weitergeben, vertrauen und hinterfragen, einordnen und neu sortieren bilden beispielhafte To-dos. Die Zukunft ist eine spannende und widersprüchliche Unbekannte. Wer sich mit ihrem Charakter gut anfreunden kann, wird am ehesten sicher sein und offen bleiben.

Open Access und Urheberschutz, Autonomiebestreben und Globalisierung, Risikovermeidung und Innovation – wie passt das alles zusammen? Was vereint eine Welt der Gegensätze? Zuhören und mitreden, erproben und optimieren, verhandeln und austarieren – man kann viel dafür tun.



Wie Leitlinien zu Sicherheit führen.

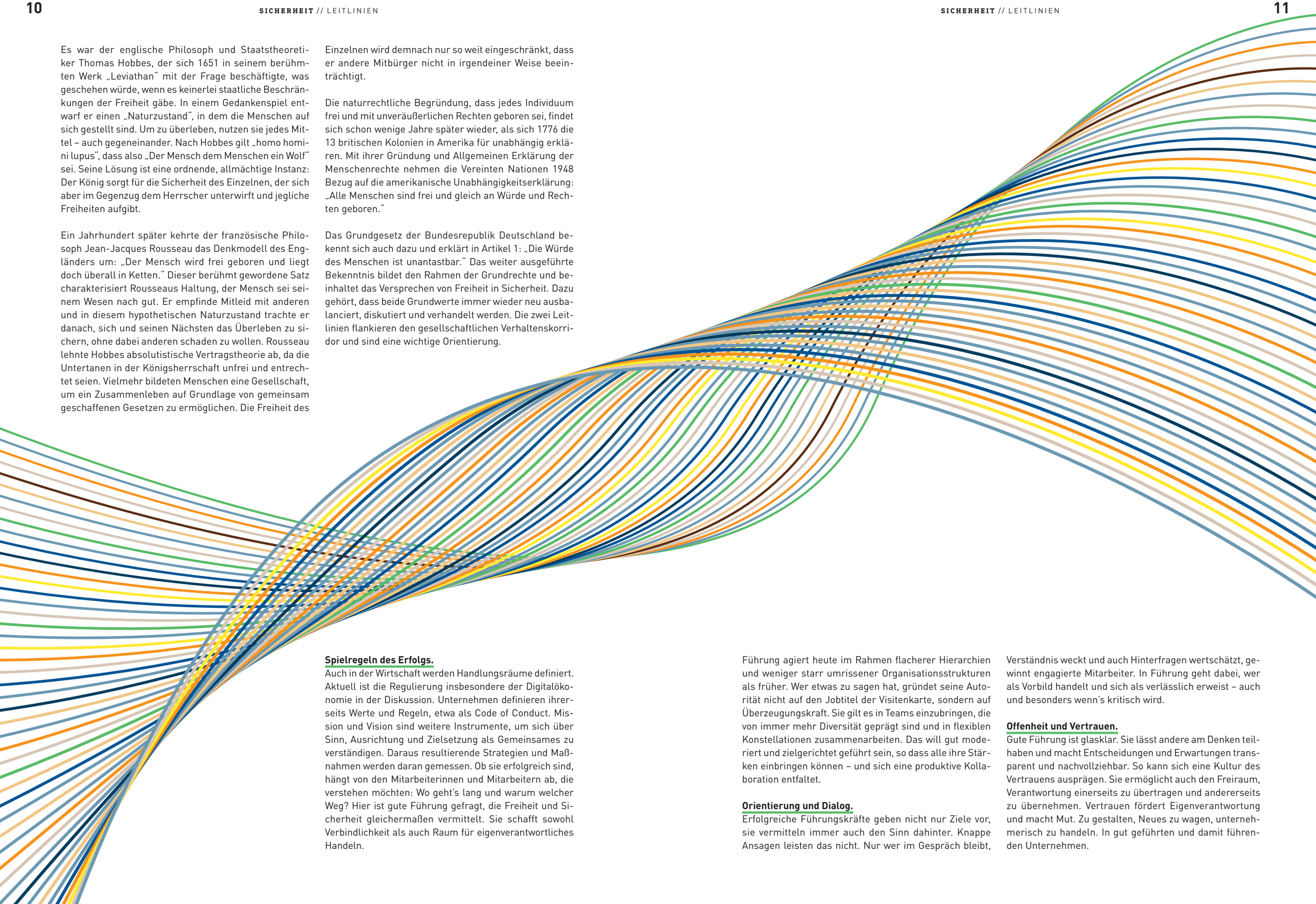
Unsere Geistesgeschichte balanciert schon
länger zwischen Freiheit und Sicherheit. An diesen Koordinaten
orientieren sich Individuen ebenso wie Staatswesen
oder Unternehmen. Sie bilden Fixpunkte für ein verbindliches Miteinander –
und ermöglichen Handlungskompetenz.

Es war der englische Philosoph und Staatstheoretiker Thomas Hobbes, der sich 1651 in seinem berühmten Werk „Leviathan“ mit der Frage beschäftigte, was geschehen würde, wenn es keinerlei staatliche Beschränkungen der Freiheit gäbe. In einem Gedankenspiel entwarf er einen „Naturzustand“, in dem die Menschen auf sich gestellt sind. Um zu überleben, nutzen sie jedes Mittel – auch gegeneinander. Nach Hobbes gilt „homo homini lupus“, dass also „Der Mensch dem Menschen ein Wolf“ sei. Seine Lösung ist eine ordnende, allmächtige Instanz: Der König sorgt für die Sicherheit des Einzelnen, der sich aber im Gegenzug dem Herrscher unterwirft und jegliche Freiheiten aufgibt.

Ein Jahrhundert später kehrte der französische Philosoph Jean-Jacques Rousseau das Denkmodell des Engländers um: „Der Mensch wird frei geboren und liegt doch überall in Ketten.“ Dieser berühmt gewordene Satz charakterisiert Rousseaus Haltung, der Mensch sei seinem Wesen nach gut. Er empfinde Mitleid mit anderen und in diesem hypothetischen Naturzustand trachte er danach, sich und seinen Nächsten das Überleben zu sichern, ohne dabei anderen schaden zu wollen. Rousseau lehnte Hobbes absolutistische Vertragstheorie ab, da die Untertanen in der Königsherrschaft unfrei und entrechtet seien. Vielmehr bildeten Menschen eine Gesellschaft, um ein Zusammenleben auf Grundlage von gemeinsam geschaffenen Gesetzen zu ermöglichen. Die Freiheit des Einzelnen wird demnach nur so weit eingeschränkt, dass er andere Mitbürger nicht in irgendeiner Weise beeinträchtigt.

Die naturrechtliche Begründung, dass jedes Individuum frei und mit unveräußerlichen Rechten geboren sei, findet sich schon wenige Jahre später wieder, als sich 1776 die 13 britischen Kolonien in Amerika für unabhängig erklären. Mit ihrer Gründung und Allgemeinen Erklärung der Menschenrechte nehmen die Vereinten Nationen 1948 Bezug auf die amerikanische Unabhängigkeitserklärung: „Alle Menschen sind frei und gleich an Würde und Rechten geboren.“

Das Grundgesetz der Bundesrepublik Deutschland bekennt sich auch dazu und erklärt in Artikel 1: „Die Würde des Menschen ist unantastbar.“ Das weiter ausgeführte Bekenntnis bildet den Rahmen der Grundrechte und beinhaltet das Versprechen von Freiheit in Sicherheit. Dazu gehört, dass beide Grundwerte immer wieder neu ausbalanciert, diskutiert und verhandelt werden. Die zwei Leitlinien flankieren den gesellschaftlichen Verhaltenskorridor und sind eine wichtige Orientierung.



Spielregeln des Erfolgs.
Auch in der Wirtschaft werden Handlungsräume definiert. Aktuell ist die Regulierung insbesondere der Digitalökonomie in der Diskussion. Unternehmen definieren ihrerseits Werte und Regeln, etwa als Code of Conduct. Mission und Vision sind weitere Instrumente, um sich über Sinn, Ausrichtung und Zielsetzung als Gemeinsames zu verständigen. Daraus resultierende Strategien und Maßnahmen werden daran gemessen. Ob sie erfolgreich sind, hängt von den Mitarbeiterinnen und Mitarbeitern ab, die verstehen möchten: Wo geht's lang und warum welcher Weg? Hier ist gute Führung gefragt, die Freiheit und Sicherheit gleichermaßen vermittelt. Sie schafft sowohl Verbindlichkeit als auch Raum für eigenverantwortliches Handeln.

Führung agiert heute im Rahmen flacherer Hierarchien und weniger starr umrissener Organisationsstrukturen als früher. Wer etwas zu sagen hat, gründet seine Autorität nicht auf den Jobtitel der Visitenkarte, sondern auf Überzeugungskraft. Sie gilt es in Teams einzubringen, die von immer mehr Diversität geprägt sind und in flexiblen Konstellationen zusammenarbeiten. Das will gut moderiert und zielgerichtet geführt sein, so dass alle ihre Stärken einbringen können – und sich eine produktive Kollaboration entfaltet.

Orientierung und Dialog.
Erfolgreiche Führungskräfte geben nicht nur Ziele vor, sie vermitteln immer auch den Sinn dahinter. Knappe Ansagen leisten das nicht. Nur wer im Gespräch bleibt, Verständnis weckt und auch Hinterfragen wertschätzt, gewinnt engagierte Mitarbeiter. In Führung geht dabei, wer als Vorbild handelt und sich als verlässlich erweist – auch und besonders wenn's kritisch wird.

Offenheit und Vertrauen.
Gute Führung ist glasklar. Sie lässt andere am Denken teilhaben und macht Entscheidungen und Erwartungen transparent und nachvollziehbar. So kann sich eine Kultur des Vertrauens ausprägen. Sie ermöglicht auch den Freiraum, Verantwortung einerseits zu übertragen und andererseits zu übernehmen. Vertrauen fördert Eigenverantwortung und macht Mut. Zu gestalten, Neues zu wagen, unternehmerisch zu handeln. In gut geführten und damit führenden Unternehmen.

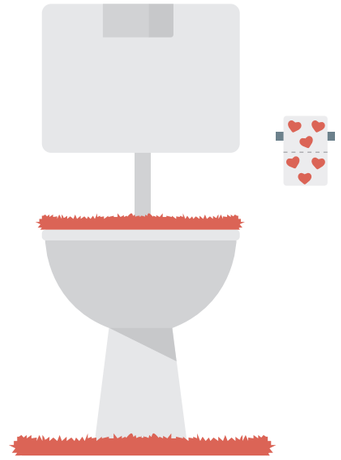
GESETZE AUS ABSURDISTAN.

Alles, was recht ist – manche Gesetze auf der Welt regeln ziemlich kuriose Sachverhalte. Vor Gericht könnte die Anklage zumindest auf Originalität plädieren. Eine kleine Auswahl:

Achtung, Radfahrer.
Im amerikanischen Bundesstaat Connecticut dürfen Radfahrer nicht schneller als 65 Meilen – also rund 100 km/h – unterwegs sein. Hier also nicht zu stark in die Pedale treten. Auf Helgoland ist Fahrrad fahren übrigens erst gar nicht erlaubt – Feuerwehr, Polizei und Ärzte ausgenommen.

Zum Sterben zu kalt?
Auf der norwegischen Insel Spitzbergen liegt Longyearbyen, einer der nördlichsten Orte der Welt. Weil der Boden zu jeder Jahreszeit gefroren bleibt, können Leichen weder begraben werden noch verwesen, heißt es. Ein Gesetz schreibe deshalb vor, auf dem Festland zu sterben. So kann man es jedenfalls im Internet an vielen Stellen nachlesen. In Wahrheit ist das Ganze ein immer wieder verbreiteter Mythos. In einer britischen Krimiserie wird dieser Umstand übrigens auch thematisiert. Die Stadt heißt hier allerdings „Fortitude“. Mal sehen, wann die Erwärmung des Permafrosts das Gerücht obsolet macht …

Schweizer Ordnung.
In der Schweiz ist es zwischen 22 Uhr und sieben Uhr verboten, Autotüren, Motorhauben oder Kofferraumdeckel zuzuknallen. Hier gilt Rücksichtnahme noch was. In Etagenwohnungen darf man während der Nachtruhe auch keine Toilettenspülungen betätigen. Die Geräuschentwicklung beim Wasserlassen bleibt außer Acht. In einigen Schweizer Kantonen ist das Tanzen an hohen Feiertagen wie Karfreitag verboten. Ansonsten kann man aber viel Spaß haben. Zum Beispiel beim Nacktwandern – außer in Appenzell Innerrhoden und Appenzell Ausserrhoden. Da darf man das wieder nicht. Apropos Toilettenspülung: Wer sie in Singapur nicht betätigt, zahlt umgerechnet 500 Euro Strafe. Öffentliche Örtchen werden regelmäßig von der Polizei observiert. Und noch ein Sternchen zum Tanzen: Auch Bayern und Baden-Württemberg verbieten so ein Gehopse an gesetzlichen Feiertagen.



Nix marsch, marsch.
Gemäß Paragraf 27 der deutschen Straßenverkehrsordnung ist es Wandergruppen verboten, im Gleichschritt über Brücken zu gehen. Das dürfte den meisten Wandersleuten wurst sein – solange man weiter im Chor singen darf. Aber Obacht: Das Tragen von Pappnasen ist dabei außer zu Karneval nicht erlaubt – sofern man Wandergruppen als öffentliche Veranstaltung ansieht. Ob es hierfür Präzedenzfälle gibt?

Kitzlig: Bärte.
In Eureka, Kalifornien, dürfen Männer mit Schnurrbart angeblich keine Frauen küssen. Ob das auch von Mann zu Mann gilt? Alabama verbietet, in der Kirche mit Bartattrappe zu erscheinen. Besucher der Messe könnten sonst was zu lachen haben. Und das Küssen unterliegt in manchen US-Bundesstaaten einer gesetzlichen Höchstdauer. Hier also beim Hochzeitskuss die Stoppuhr beachten.

AUSBUCHSTABIERT.

IT-Sicherheit ist ein Thema, das jeden angeht, der Computer benutzt – Laptops, Tablets, Smartphones, egal. Es betrifft also uns alle. Aber mal ehrlich, wer versteht schon viel davon? Dieses Magazin soll zu mehr Verständnis beitragen. Mal ausführlicher, mal kurz und knapp – wie hier. Ein paar Schlüsselbegriffe von vielen zur Einführung oder auch Hinführung zu den vertiefenden Beiträgen auf den Folgeseiten.

Crime-as-a-Service.
Im Internet gibt es nicht nur Software-as-a-Service für die Buchhaltung oder Produktionssteuerung, sondern auch „Killer-Applikationen" für kriminelle Dienste aller Art. Das Darknet stellt klickbare Malware oder Ransomware-as-a-Service bereit, um individuelle Attacken zu konfigurieren. Man kann auch Cybergangs buchen, die ihr Unwesen im Auftrag treiben. Gegen diese Form der digitalen Kriminalität hilft am besten **Security-as-a-Service,** auch zu finden auf Seite 20.

Datenschutz und Datensicherheit.
Das Wortpaar gehört zusammen, beide Begriffe bezeichnen aber unterschiedliche Aspekte von IT-Sicherheit. Datenschutz steht für die Einhaltung von Gesetzen und Vorschriften vor allem zum Schutz personenbezogener Daten. Grundlagen bilden zum Beispiel das Bundesdatenschutzgesetz BDSG und die neuere Datenschutzgrundverordnung DSGVO. Datensicherheit umschreibt hingegen vor allem technische Maßnahmen gegen Verlust oder Manipulation von Daten – sei es durch Betriebsstörungen, Cyberattacken oder einfach durch schusselige Mitarbeiter. Datenschutz wie Datensicherheit zu gewährleisten, ist beides gleich wichtig, ja elementar.

IT-Forensik.
Die noch junge Spezialdisziplin der Forensik untersucht Vorfälle in der IT, um Ursachen aufzuklären, ggf. gerichtsfeste Beweise zu sichern und, wenn möglich, Schäden zu minimieren oder verlorene Daten wiederherzustellen. Nicht immer steckt eine kriminelle Handlung dahinter, oft besteht aber der Verdacht, und manchmal kann man auch Täter dingfest machen. Es gilt auch, eine mögliche Schadenshöhe zu ermitteln und Haftungsfragen zu klären. Außerdem können analysierte Schwachstellen zukünftig besser geschützt werden. Anders als Gerichtsmediziner können IT-Forensiker in vielen Fällen einiges retten. Wie, steht auf Seite 34 ff.

Passwörter.
Die allgemeine Bequemlichkeit bei der Passwortvergabe erscheint wie ein wohlig schlafendes Faultier, das kein Weckruf der Welt aus der Ruhe bringt. Trotz unzähliger Berichte, Tutorials und Ratgeber, der Einfachheit halber werden immer noch schwache Passwörter eingesetzt. Als entscheidend wird die Güte von Passwörtern angesehen, die keinesfalls für mehrere Dienste genutzt werden dürfen. Jedes Passwort sollte mindestens 8-, besser 16-stellig und ein möglichst vielfältiger Mix aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen sein. Wem das zu kompliziert ist: Hilfe bieten Passwortmanager, die das alles verwalten. Dann muss man sich nur noch das Masterpasswort merken …

Security-as-a-Service.
Ganzheitliches IT-Sicherheitsmanagement als Servicemodell spezialisierter Dienstleister: Unternehmen oder öffentliche Einrichtungen geben den Schutz vor Cybercrime in besser qualifizierte Hände – von Experten, die immer auf der Höhe von Anforderungen und geeigneten Gegenmaßnahmen sind. Bei fast 320.000 neuen Schadprogrammen pro Tag ist das keine Kleinigkeit. Zur Abwehr sind Softwaresysteme nötig, die ständig aktualisiert werden müssen. Das ist bei Security-as-a-Service natürlich inklusive – und das Ganze mehr als lohnend, um den potenziell ruinösen Risiken durch **Crime-as-a-Service** zu begegnen.

Quantenkryptografie.
Die Welt der Quantenphysik ist ohnehin irgendwie kryptisch. Ein chaotisches Universum, in dem alles gleichzeitig schwarz und weiß sein kann? Für den naturwissenschaftlich mittelbegabten Verstand eine dunkle Materie. Wenn es so kompliziert ist, ahnen wir allerdings: Die Quantenverschlüsselung scheint schon sehr sicher zu sein. Dass Quanten andererseits das Potenzial haben, heute bestehende Kryptografiestandards zu knacken, kann man auf den Seiten 34–41 nachlesen.

Resilienz.
Der Begriff hat in den letzten Jahren vor allem im psychologischen Kontext immer mehr Verbreitung gefunden. Gemeint ist die mentale Widerstandsfähigkeit gegen Krisen und die Fähigkeit, daran zu wachsen. Früher hätte man vielleicht gesagt: „sich ein dickes Fell zulegen." Heute versteht man Resilienz auch als Qualität der IT, gegen Ausfälle und Angriffe gewappnet zu sein und sich auch prophylaktisch besser darauf einzustellen. Statt abzuwarten, dass etwas passiert, nimmt man damit eine deutlich aktivere Haltung ein. Dieser mentale Wandel korrespondiert auch mit der technischen Entwicklung. So soll künstliche Intelligenz dabei helfen, zukünftige Bedrohungen besser zu antizipieren. Mehr über Resilienz ab Seite 22.

Zwei-Faktor-Authentifizierung.
Für immer mehr Onlinedienste und Plattformen ist es nötig, sich in zwei Schritten zu authentifizieren. Nach Eingabe eines Passworts wird automatisch ein zusätzlicher Code generiert oder eine App aktiviert, um die Anmeldung zu bestätigen. In der Regel erfolgt das über ein Smartphone als zweites Endgerät, so dass potenzielle Angreifer in beide Systeme eindringen müssten. Das ist nun wirklich schwer machbar und die doppelte Absicherung ein sinnvolles Verfahren.

SICHER HEIT MIT STRUKTUR.

IT-SECURITY BY BECHTLE.

Wo fängt IT-Sicherheit an und wo hört sie auf? In unserer zunehmend digitalen Welt sind die Grenzen schwer auszumachen. Menschen, Endgeräte, Maschinen und Sensoren sind in physischen und virtualisierten Infrastrukturen global vernetzt – und angreifbar. Ein mitlesender Sitznachbar im Flugzeug kann ebenso Schaden anrichten wie ein Leck in der Cloud. Ein Druckerspeicher ist genauso ein Risiko wie der Maileingang. Zum Schutz dienen Virenscanner, umfassende Sicherheitstests – sogenanntes Penetration Testing, Zwei-Faktor-Authentifizierung und vieles mehr. Und es kommen immer neue Parameter hinzu, die es zu bedenken und schützen gilt. Angriffsmethoden und Verteidigungsmaßnahmen entwickeln sich wechselweise so schnell, dass man schwer folgen kann. Wer behält den Überblick und durchdringt alle Tiefen der Sicherheitsarchitektur?

Die Abbildungen zeigen „Forest of Numbers", eine Installation von Emmanuelle Moureaux. Fotos: Daisuke Shima.

Über 250 Experten für IT-Sicherheit haben auch angesichts immer neuer Bedrohungen den Durchblick.

Die Dimensionen von IT-Sicherheit sind komplex und allgegenwärtig. Sie umfassen nicht nur digitale Technologien, sondern auch allzu menschliches Verhalten. Bedrohungen umgeben Unternehmen und öffentliche Einrichtungen wie ein Netz, das gleichzeitig eine Vielzahl potenzieller Angriffspunkte berührt. Die Abwehrmechanismen müssen dementsprechend flexibel wie engmaschig sein, schwer durchdringbar und anpassungsfähig. Moderne IT-Sicherheitsstrukturen sind nicht mehr aus statischen Firewalls konstruiert, sondern ähneln eher dem Schutzschild des Raumschiffs „Enterprise“, nur permanent aufgespannt. Ständig werden Signale empfangen und Aktivitäten ausgelöst, aktuelle Angriffe abgewehrt, bevorstehende antizipiert und entstandene Schäden repariert. Das meiste davon geschieht automatisiert und erfordert immer weniger menschliche Eingriffe als vielmehr ein stringentes Management. Die IT-Organisation überwacht im Idealfall eine hochleistungsfähige „Security Engine“, die bei Auffälligkeiten oder Angriffen bereitstehende Instanzen einschaltet – sei es intern oder bei dafür zuständigen Dienstleistern. Um solche Sicherheitsstrukturen zu etablieren, bedarf es eines Netzwerks hochspezialisierter Experten und Architekten.

Security-as-a-Service.

Cyberkriminelle operieren ihrerseits zunehmend in vernetzten Strukturen von Spezialisten, die sich bedarfsweise für komplexe Attacken bilden. Diese liefern „Crime-as-a-Service“. Dem gilt es auf Augenhöhe zu begegnen – oder vielmehr überlegen zu sein. Bechtle hat dazu eine Community aus mehr als 250 Security-Spezialisten aufgebaut, die ihresgleichen sucht. Die Expertenorganisation organisiert sich in sechs Competence Centern, die regionalen Bechtle Systemhäusern angegliedert sind. 28 Security-Teamleiter führen schlagkräftige Einheiten, die sich je nach Anforderung flexibel zusammensetzen. Damit kann Bechtle „Security-as-a-Service“ anbieten – bis hin zur Übernahme der gesamten Betriebsverantwortung für die IT-Sicherheit, was eine große Entlastung bedeutet.

Denn die hohen Sicherheitsanforderungen erfordern und binden allerhand technische und personelle Ressourcen. Jedes Unternehmen, jede IT-Organisation sieht sich damit konfrontiert, dass Fachkräfte für Cybersicherheit Mangelware sind. Abgesehen davon kann es sich der breite Mittelstand gar nicht leisten, das Anforderungsspektrum mit eigenen Kapazitäten abzudecken. Bechtle unterstützt seine Kunden deshalb dabei, das jeweils passende „Betriebsmodell“ für IT-Sicherheit einzurichten. Mit dieser Organisationsberatung wird der Grundstein für eine Sicherheitsarchitektur gelegt, die für die Zukunft belastbar und ausbaufähig ist.

Auf der Höhe der Entwicklung.

Komplexe, hybride Infrastrukturen mit permanenten technischen Neuerungen, Updates und Upgrades sowie komplizierte und immer neue gesetzliche Rahmenbedingungen treffen auf agile und aggressive Angreifer. Dabei steht viel auf dem Spiel. Offensive Präventivmaßnahmen bilden die beste Verteidigung. Mit smarten und resilienten Strukturen und einem Team, das voll auf der Höhe ist und Expertise und Technologie bestmöglich vereint.

Bechtle bietet ein Ende-zu-Ende-Sicherheitsportfolio.
Mehr auf bechtle.com/security

RESILIENZ, DIE: PRÄVENTIVE SICHERHEITS STRATEGIE.

In vielen Lebensbereichen ist vorbeugender Schutz selbstverständlich: vor Krankheiten und Unfällen etwa. Autos stecken voller Sicherheitssysteme und Sensoren, die uns gegen Schäden abschirmen. Auch umsichtige Radfahrer sind vorsichtshalber behelmt unterwegs. Warum also ausgerechnet bei der IT unnötige Risiken eingehen?

Die Helmtechnologie von WaveCel bietet besonderen Schutz vor Verletzungen des Gehirns. Von der komprimierbaren Zellstruktur als Knautschzone wird die Aufprallenergie absorbiert.

Resilienz bezeichnet ein Konzept struktureller Widerstandsfähigkeit. In der Psychologie versteht man darunter die Fähigkeit von Menschen, mit Schwierigkeiten oder Stress umzugehen. Man kann das lernen und trainieren – und sogar daran wachsen, Krisen zu überwinden. In der Soziologie findet das Prinzip auch auf Organisationen, ja auf die Gesellschaft insgesamt Anwendung. Genauso lässt es sich auch auf die IT übertragen.

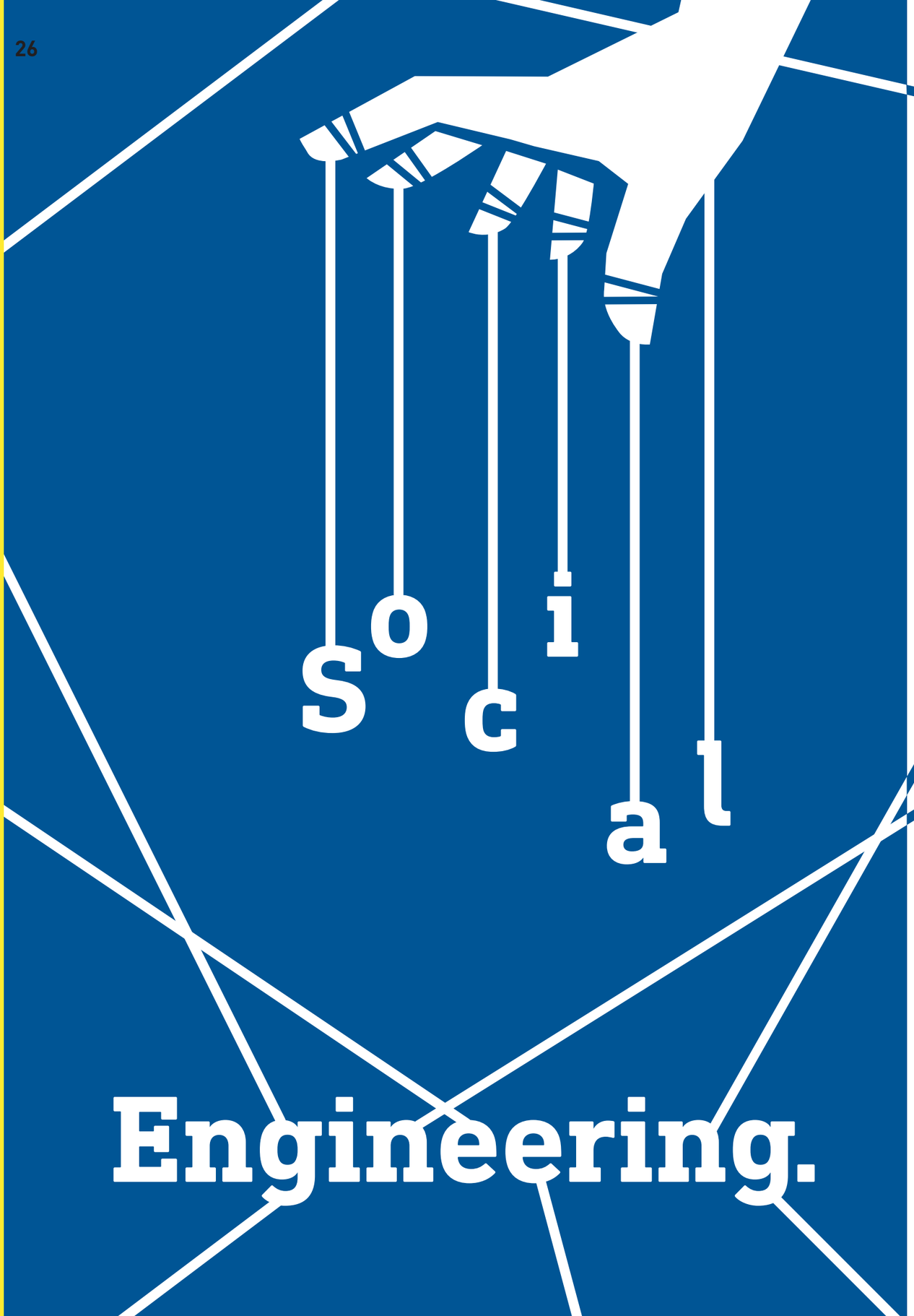
Die konzertierte Widerstandskraft.
Cyber Resilience – der vorbeugende Schutz der IT – umfasst damit die Menschen und Organisationen ebenso wie Infrastrukturen und Technologien. „Digitale Souveränität und Integrität der IT-Anwender sind sogar Schlüsselfaktoren, die oft zu wenig Beachtung finden“, so Tobias Dames, Resilienzexperte bei Bechtle. Wenn sich alle an Sicherheitsregeln hielten – vorausgesetzt, dass sie wüssten, wie –, sei dem größten Risiko schon mal vorgebeugt. Deshalb bilden Awareness-Trainings und Verhaltensschulungen zentrale Elemente einer Resilienzstrategie.

Den Kern härten.
Ein wichtiger Aspekt ist auch das Bewusstsein, dass es hundertprozentige Sicherheit nicht gibt, nicht geben kann. Tobias Dames und sein Team konzentrieren sich deshalb auf die Kernprozesse eines Unternehmens oder auch einer Behörde. Was muss immer funktionieren, was nicht unbedingt? Die Fertigung und die Logistik eines Teilezulieferers sind im Zweifel wichtiger als beispielsweise sein Bewerbermanagement.

Für den kritischen Kern gilt es, die größte Widerstandsfähigkeit zu entwickeln. Dazu wird gewissermaßen ein Schutzschild aus mehreren Schichten gebildet. Damit gibt es bei Ausfällen verschiedene Rückfalloptionen. Gleichzeitig können im Fallback-Modus fehlerhafte Funktionen oder beschädigte Systeme wiederhergestellt werden. Und Achtung: „Die Strukturen und Regeln hierfür müssen sorgfältig und transparent dokumentiert werden“, betont Tobias Dames. Ein guter Notfallplan gibt enorm viel Sicherheit – nicht nur gefühlt, sondern auch faktisch.

Wahrhaft wehrhaft.
Bechtle hat ein Framework entwickelt, um Cyber Resilience mit System umzusetzen. In einem initialen Assessment Center werden zunächst die für den Betrieb wesentlichen Prozesse identifiziert und die Sicherheitsanforderungen dafür definiert. Das dauert etwa drei bis fünf Tage. Dann stehen die Benchmarks. Dieser Herausforderungen nimmt sich ein Team aus Spezialisten verschiedenster Disziplinen an: Experten für Netzwerktechnik, Datensicherheit, Disaster Recovery, Business Continuity und Servicemanagement sind ebenso dabei wie Organisationsberater, Risikomanager, Business Coaches und Antimanipulationstrainer. Sie „impfen“ die Mitarbeiterinnen und Mitarbeiter und immunisieren die IT-Infrastrukturen und -Anwendungen – mit dem besonderen Fokus auf Geschäftskritisches. Unternehmen sichern so im Zweifelsfall ihr wirtschaftliches Überleben. Betreiber sogenannter kritischer Infrastrukturen – wie Energie- und Wasserversorger und Institutionen der inneren und äußeren Sicherheit – nehmen eine umso größere Verantwortung wahr, indem sie so resilient wie nur möglich aufgestellt sind. Gewiss macht Cyber Resilience nicht unverwundbar, aber Systeme und Organisationen generell weit weniger angreifbar – auch im Sinne eines ganzheitlichen Verständnisses von Compliance.

Voraussetzung für Resilienz ist das Umdenken von reaktiv zu proaktiv – unternehmensweit und mit strategischem Ansatz. Mit Ansage des führenden Managements.



Social Engineering.

Beim Social Engineering, einer modernen Form des Trickbetrugs, erschleichen sich Angreifer durch Lüge und Täuschung das Vertrauen einzelner Mitarbeiter von Unternehmen, bewegen sie etwa dazu, ihnen Zugang zum Firmennetzwerk zu verschaffen. Davor schützen kann sich nur, wer die größte Schwachstelle jeder Sicherheitskette stärkt: den Menschen. Wie gelingt das?

Enkeltrick 3.0. Um sich nicht betrügen zu lassen, sollte man vor allem zum richtigen Zeitpunkt die richtigen Fragen stellen. Genau das tat der Mitarbeiter eines US-Tabakkonzerns nicht, als er im Sommer vergangenen Jahres einen Anruf aus der eigenen IT-Abteilung erhielt. Der vermeintliche Kollege befragte ihn über sein E-Mail-Programm, das Betriebssystem, den VPN-Anbieter und vieles mehr. Er benötige diese Infos, um dem Angerufenen einen neuen Rechner beschaffen und konfigurieren zu können – den der sich offenbar sehnlich wünschte. So sehnlich, dass er weder sich noch dem Anrufer die naheliegende Frage stellte, warum um Himmels willen dieser über die Systeme so wenig wusste – obwohl er in der eigenen IT-Abteilung beschäftigt ist?

Die Geschichte ging gut aus und ist überhaupt nur bekannt geworden, weil der Anruf von der Hackerkonferenz Defcon in Las Vegas kam und niemanden schädigen, sondern – live vor Publikum – demonstrieren sollte, was alles möglich ist, wenn es einem Angreifer gelingt, Vertrauen aufzubauen – und es anschließend zu missbrauchen. Im Kern richten sich alle Social-Engineering-Angriffe auf die immer gleichen Einfallstore der menschlichen Seele: Neugier, den Wunsch nach Gemeinschaft und Miteinander, nach Anerkennung, nach Interesse an der eigenen Person und ihren Wünschen.

Lücken gibt's immer. Christoph Barreith, Solution Architect im Bereich Security/Network bei Bechtle, macht immer wieder die Erfahrung, dass Unternehmen sich weniger mit psychologischen Aspekten beschäftigen und stattdessen mehr oder weniger Geld und Zeit aufwenden, um technische Schwachstellen ihrer IT-Systeme zu identifizieren und zu beseitigen – um jeden erdenklichen automatisiert geführten Angriff abwenden zu können.

Echte Sicherheit kann diese Strategie nur teilweise bieten. Denn zum einen müssen die Mitarbeiter immer auf interne Datenbestände zugreifen, um ihre Arbeit zu erledigen. Zum anderen werden die Systeme durch Integration früher getrennter Systeme und durch Vernetzung immer mehr zusammengeführt. Außerdem lassen sich alle diese Zugänge auch deshalb nicht ständig und vollkommen wasserdicht sichern, weil gerade Unternehmen, die stark auf Digitalisierung setzen, ohne Zugänge auch zu sensiblen Daten gar nicht arbeitsfähig wären.

Eine weitere Herausforderung bei der Abwehr von Attacken gegen die eigenen Systeme durch Aushorchen, Lügen, Manipulieren und Erpressen liegt darin, so Christoph Barreith, „dass die Trennung zwischen Privatem und Geschäftlichem in Zeiten von Social Media immer mehr aufgehoben wird und dass die Menschen das auch nicht mehr trennen wollen."

Ein Klick mit Folgen. Viele geben großzügig Privates preis, weil sie dafür etwas zurückbekommen. Genau darin liegt die Gefahr: Wer über längere Zeit die Social-Media-Profile eines Menschen auswertet, lernt ihn dadurch gut kennen. Ihm dann eine E-Mail auf den Firmenaccount zu senden, die gezielt individuelle Sehnsüchte und Erwartungen anspricht, ist ein Leichtes. Sie verleitet den Empfänger dann dazu, jenen Link anzuklicken, der dem Angreifer – virtuell – das Tor zum Serverraum des Unternehmens öffnet.

Das kann zum Beispiel so aussehen: Ein Mitarbeiter, der sich auf Facebook stolz mit seinem neuen Dienstfahrrad präsentiert, wird kurz darauf per E-Mail aufgefordert, an einer Umfrage teilzunehmen: Wie er mit dem Fahrrad zufrieden sei und ob er unter folgendem Link eine Bewertung abgeben könne. Das klingt plausibel und unverfänglich – ist aber ein Trick, um Daten abzufischen oder ein Schadprogramm zu installieren.

Die Polizei schreibt keine E-Mails. Das Fahrradbeispiel zeigt, wie nützlich generelle „Security Awareness" ist, gesunde Skepsis, und zwar in beruflichen Zusammenhängen ebenso wie in privaten. Und diese Skepsis kann im Fall der Fälle die richtigen Fragen hervorbringen. Etwa: Woher weiß der (Fragesteller, Mailschreiber), was er zu wissen behauptet? Woher weiß er, dass das Fahrrad von meiner Firma stammt? Warum eigentlich interessiert er sich dafür? Gibt es darauf keine zufriedenstellenden Antworten, ist größte Vorsicht geboten.

Erst recht misstrauisch sollten natürlich Fragen oder Zutrittswünsche von Fremden machen, die nicht virtuell, sondern leibhaftig auftauchen, beispielsweise in Form von Handwerkern im stilechten Outfit, die behaupten, ganz schnell im Serverraum etwas reparieren zu müssen. Auch solche Angriffe gibt es immer wieder. Nicht selten werden sie durch vertrauensbildende E-Mail-Korrespondenz vorbereitet, einen Kommunikationsweg, der generell mit Vorsicht zu genießen ist. „Staatsanwaltschaft, Polizei und Finanzamt schreiben grundsätzlich keine E-Mails", so Solution Architect Christoph Barreith. Und auch der eigene Chef erteilt relevante Anweisungen, beispielsweise die, eine bestimmte Zahlung zu leisten, nicht per E-Mail. Und wenn doch, dann sollten die Mitarbeiter mit ihm darüber sprechen. Gefundene USB-Sticks auf oder vor dem Firmengelände sollten direkt bei der IT-Abteilung abgegeben werden, ohne am eigenen Rechner prüfen zu wollen, wem dieser USB-Stick gehört – auch wenn er mit „FKK Urlaub Korsika 2019" beschriftet ist.

Manipuly – das üble Spiel.
Social Engineering steht – wenn auch nicht wörtlich übersetzt – für „soziale Manipulation". Gemeint ist jedwede Beeinflussung anderer mit dem Ziel, sie zur Preisgabe vertraulicher Informationen, zur Freigabe von Geldern oder zum Kauf bestimmter Güter zu bewegen.

Sensibilisierung mit Spaßfaktor. Die Security Awareness Trainings von Bechtle arbeiten mit ganz unterschiedlichen Ansätzen, um Sensibilität für die beschriebenen Gefahren zu wecken. Dabei spielen E-Learnings schon deshalb eine zentrale Rolle, weil selbst bei einem Mittelständler unmöglich alle Mitarbeiter Präsenzveranstaltungen besuchen könnten. Weil aber jede und jeder potenzielles Ziel von Angriffen sein kann, „müssen auch alle darauf vorbereitet werden", so Volker Wörtmann, Leiter des Bechtle Training Centers in Neckarsulm.

Und diese Vorbereitung ist am wirkungsvollsten, wenn sie – auch – Spaß bringt. Deshalb arbeitet Bechtle mit Gamification, setzt also auf Spiel- und Wettbewerbselemente, lässt die Teilnehmer zum Beispiel um den Highscore für die meisten richtig beantworteten Fragen kämpfen. Ober führt sie in einen virtuellen Schulungsraum, in dem Gefahrenquellen versteckt sind, herumliegende USB-Sticks oder eine an den Aktenschrank gepinnte Liste mit Kennwörtern. Auch beliebt: Die ausgehängte „Blacklist" mit Telefonnummern besonders unangenehmer Kunden und Lieferanten …

Laufen die entsprechenden Schulungen zu konventionell ab, dann „lesen die Teilnehmer irgendwann ihre E-Mails, anstatt bei der Sache zu sein", so Volker Wörtmann. Und klicken dabei vielleicht genau auf jenen Anhang, den sie besser ignoriert hätten …

Security Awareness Training.
Das Trainingskonzept von Bechtle beinhaltet eine Kombination aus maßgeschneiderten Classroom Trainings, E-Learnings und Live Online Trainings. Viele Unternehmen führen diese Maßnahmen bereits im Kontext Arbeitssicherheit durch und kennen daher schon das Verfahren der Schulung. Die angebotenen Trainings ermöglichen eine realitätsnahe Anpassung an individuelle Gegebenheiten und Anforderungen des betreffenden Unternehmens und eine schnelle Identifikation mit dem Thema. Indem das Unternehmen selbst erstellte Phishingmails an Mitarbeiter verschickt und den Umgang damit anschließend bewertet, kann es den Erfolg der Trainings realitätsnah überprüfen. Auch bei solchen Checks stehen Christoph Barreith und Volker Wörtmann und ihre Teams mit Rat und Tat zur Seite.

DIE CLOUD WASSER DICHT MACHEN.

Der Zug zur Cloud ist stark. Die Angebote sind ja auch zahlreich, vielfältig und inzwischen einfach verfügbar. Genauso selbstverständlich, wie man private Urlaubsfotos in der Cloud verwaltet, lassen sich auch geschäftsrelevante Dienste nutzen. Solche Software-as-a-Service ist ruckzuck produktiv und schnell mit Unternehmensdaten gefüttert. Und dann muss man dafür sorgen, dass es aus der Cloud nicht plötzlich Probleme hagelt.

Es beginnt oft mit einem Test-Account. Der kostet erstmal nichts und ermöglicht, einen Cloud Service unverbindlich auszuprobieren. Wie funktioniert das? Wie kann ich damit umgehen? Könnte das für uns passen? Und weil es verschiedene vergleichbare Angebote gibt, werden die auch gleich mal ausgecheckt. Diese Versuche führen oft zu nichts weiter als toten Test-Accounts, in denen trotzdem Unternehmensdaten erfasst sind – und die online bleiben und damit Sicherheitsrisiken bilden.

Im anderen Fall wird ein Dienst ausgewählt und in der Folge dauerhaft eingesetzt. Über der Einfachheit wird versäumt, dabei auch Sicherheitsaspekten nachzugehen – läuft ja. So kommt eins zum anderen und schnell entsteht ein Wildwuchs an cloudbasierten Anwendungen, die nicht sauber in IT-Infrastrukturen integriert sind. „What you see is what you get" stimmt hier nur an der Oberfläche, denn mitgeliefert wird ein schlecht geschützter Zugang zu den eigenen Datenbanken.

Der einfache Zugang zu Cloud-Diensten ist von Anbieter- wie Nutzerseite gleichermaßen gewollt. Da erscheint kein Warnschild, bevor man loslegt: ACHTUNG, SICHERHEIT BEACHTEN! Also legt man los.

Mal eben durchstarten?
Je nach Organisationsgrad des Unternehmens werden hier unterschiedliche Standards gelebt. Start-ups mit „Macher"-Mentalität sehen das meist locker. Junge Gründer, die es privat nicht anders gewohnt sind, nehmen Datenschutz und -sicherheit oftmals nicht so genau. Mit einem schnellen Wachstum steigen dann auch die Risiken einer unübersichtlichen Wolkenformation. Man könnte sich vorstellen, dass das irgendwann auch für die Unternehmensbewertung relevant wird …

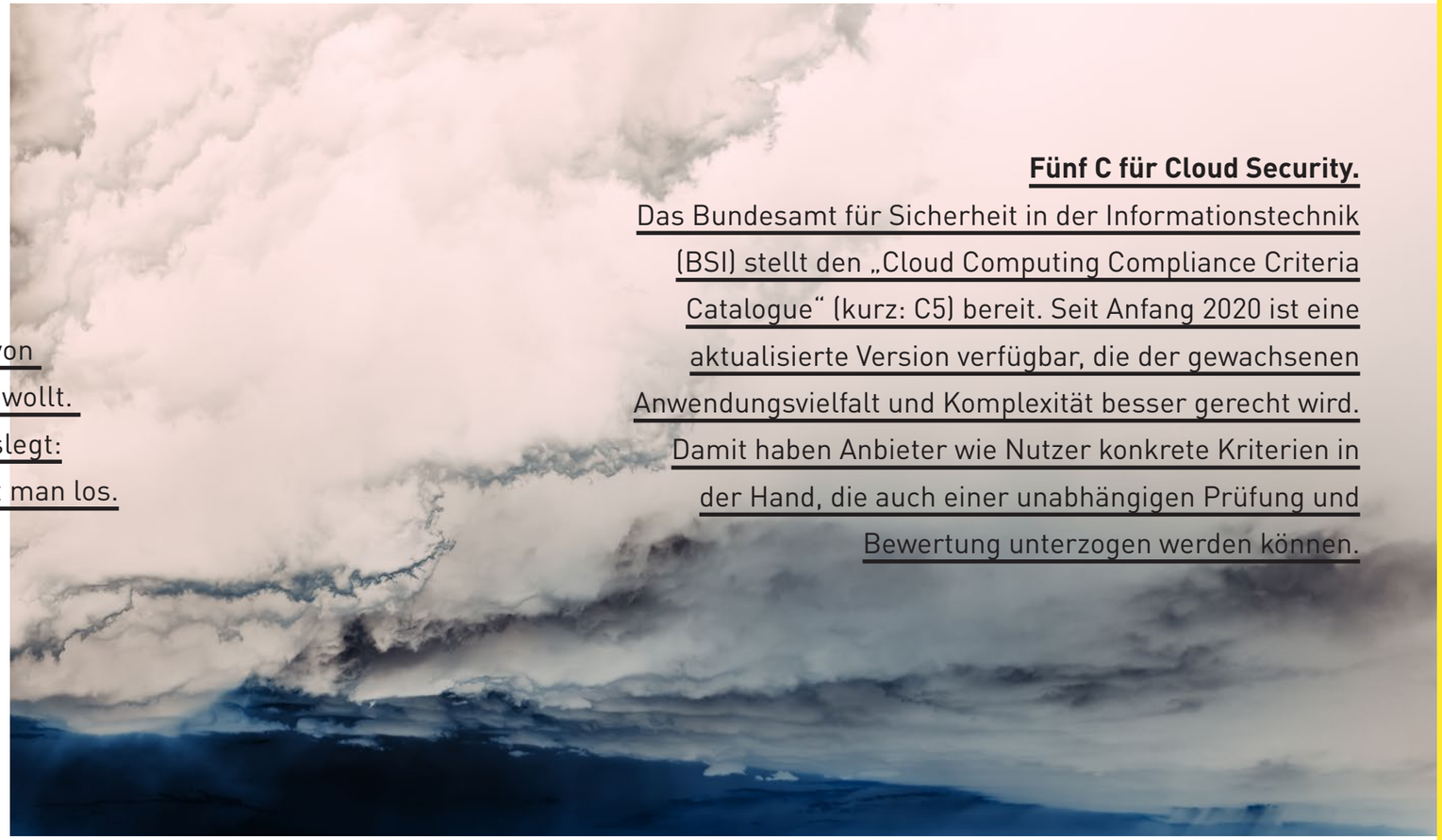
Aber auch in etablierten Firmenstrukturen wird nicht unbedingt regelgerecht agiert. Etwa, indem Fachbereiche Cloud Services nutzen, ohne die IT-Abteilung zu involvieren. Die kann dann auch keine Sicherheitsmaßnahmen treffen. Zudem ist den Anwendern oft nicht klar, was mit den Daten in der Cloud weiter passiert.

Die alte Schule der IT war da noch von anderem Schlag: Ohne Administrator ging gar nichts. Da konnte man höchstens mit dem Finger auf den Schreibtisch trommeln und hoffen, dass irgendwann die Software aktualisiert wird. Diese Zeiten sind Gott sei Dank vorbei. Cloud-Lösungen bieten automatisierte Updates. Sie unterliegen überhaupt ständigen Änderungen – nicht nur der Nutzungsbedingen, denen man vielleicht ungelesen zustimmt. Was als Selbstläufer erscheint, erfordert deshalb fortgesetzt Aufmerksamkeit.

Die Strukturen dahinter.
Man darf nie vergessen: Die Public-Cloud-Anbieter betreiben ihre Rechenzentren nach eigenen Regeln. Weltweit verteilt, ohne dass man wüsste, auf welchen Servern hochgeladene Daten liegen oder von welchem Land ins nächste diese, etwa bei einer technischen Störung, verschoben werden. Dabei kann auch schon mal eine Firewall außen vor bleiben oder eine Anwendung zeitweise nicht erreichbar sein. Diese Umstände kann man nicht beeinflussen. Was aber geht: eine eigene Sicherheitsarchitektur für die Cloud-Nutzung aufbauen und konsequent auf allen Ebenen durchsetzen.

Grundlage dafür bildet die Bewertung des eigenen Schutzbedarfs. Erst dann kann man sinnvoll planen. Das wird aber oft nicht gemacht. So kommt es, dass dann E-Mail-Services ohne ausreichende Mail Protection, virtuelle Server ohne Firewall und Datenbankinstanzen ohne Datensicherung betrieben werden. Die einfachsten Vorkehrungen sind keineswegs selbstverständlich: Zwei-Faktor-Authentifizierung, Passwortrichtlinien, personalisierte Administratorzugänge und granulare Administratorrollen – so viel sollte eigentlich selbstverständlich sein. Was auch oft übersehen wird: Viele Cloud Provider bieten automatische Test-Tools, um die Sicherheit der Konfiguration zu bewerten. Das ist schon hilfreich.

Alles in allem will der Umgang mit Cloud Services noch geübt sein. Das Angebot ist breit zugänglich und schneller gewachsen als das Verständnis für eine sichere Handhabung und Integration in Unternehmensstrukturen. Wer will, findet dabei nicht nur beratende Unterstützung. „Wir helfen unseren Kunden, für ihre Sicherheitsanforderungen die passenden Cloud Services zu identifizieren und auch sicher zu konfigurieren", erklärt Christian Dittrich, Leiter des Bechtle Competence Centers Security in Köln. „Geeignete Security-Software überwacht dann einen möglichen Datenabfluss und entdeckt gefährliche Download-Links. Auf Wunsch erstellen wir auch monatliche Security-Audits." Bechtle übernimmt auch die Betriebsverantwortung und sorgt dafür, dass die Sicherheit immer auf dem neusten Stand ist. Wer allein im Self-Service unterwegs ist, muss Änderungen, Aktualisierungen und Sicherheitsaspekte auch selbst im Auge behalten. Man hat eben immer die Wahl: machen oder machen lassen.



Fünf C für Cloud Security.
Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt den „Cloud Computing Compliance Criteria Catalogue" (kurz: C5) bereit. Seit Anfang 2020 ist eine aktualisierte Version verfügbar, die der gewachsenen Anwendungsvielfalt und Komplexität besser gerecht wird. Damit haben Anbieter wie Nutzer konkrete Kriterien in der Hand, die auch einer unabhängigen Prüfung und Bewertung unterzogen werden können.

FRISCH GEHACKTES:

GEFUNDENES FRESSEN FÜR FORENSIKER.

Beim deutschen Tatort wird die „SpuSi“ gerufen, in amerikanischen Serien kommen die knallharten Teams von der CSI. Forensiker sind aus den Krimiprogrammen nicht wegzudenken. In der IT gehören sie zu den meistgesuchten Spezialisten überhaupt. Bei Ermittlungsbehörden wie in Unternehmen. Denn zum einen wird die Wirtschaft massiv von Cyberkriminalität bedroht, zum anderen ist heute bei fast jeder Straftat das Smartphone Gegenstand der Spuren- und Beweissicherung. Hinzu kommen die zahlreichen Fälle, in denen bei Firmen Schäden entstehen, weil Mitarbeiter leichtsinnig oder fahrlässig mit Daten umgehen.

Es muss also nicht mal unbedingt kriminelle Energie im Spiel sein, wenn Christoph Boser oder Steffen Steitz alarmiert werden. Im wachsenden Team der IT-Forensiker bei Bechtle sind sie die Erfahrensten, in jedem Ermittlungsumfeld und auch als Sachverständige und Gutachter bei Gericht tätig. Leider schätzen die beiden übereinstimmend, dass neun von zehn Unternehmen nicht imstande wären, den Ursachen und Quellen von Datenverlusten oder anderen „Digitalschäden“ mit System nachzugehen. Tatsächlich ist ein streng methodisches Vorgehen nötig, schon um Ermittlungsmaßnahmen für mögliche Rechtsverfahren unangreifbar, mithin gerichtsfest zu machen. „Secure-Analyse-Present“ – kurz S-A-P – heißt das hierfür gegebene Verfahren. Dabei gilt es im ersten Schritt, von relevanten Daten ein forensisches Duplikat zu erstellen, das nachweislich mit dem Original übereinstimmt. Bei der Datenübertragung schließen deshalb „Write Blocker“ mögliche Manipulationen aus. Dieser Vorgang wird zusätzlich, wie viele weitere Arbeitsschritte auch, fotografiert und immer protokolliert. Eine umfassende Dokumentation ist wichtig, damit die Beweiskette nicht geknackt werden kann, wenn die Ergebnisse – gegebenenfalls vor Gericht – präsentiert werden müssen. Staatsanwaltschaft, Richter und Anwälte brauchen eine nachvollziehbare und wasserdichte Faktenlage – nicht jeder Jurist kann auch nebenbei noch IT-Experte sein. Die forensische Analyse selbst kann je nach Komplexität der Untersuchung Stunden, Tage oder auch Wochen dauern; unabhängig davon ist nach Artikel 33 DSGVO für datenschutzrelevante Incidents eine Meldepflicht von 72 Stunden einzuhalten. Ein umfangreiches Instrumentarium an forensischen Softwarestandards ermöglicht es, den Hergang zu rekonstruieren – und in vielen Fällen auch, verloren geglaubte Daten wiederherzustellen. Welches Equipment dabei zum Einsatz kommt, ist nicht zuletzt eine Frage von Erfahrung und Fingerspitzengefühl der Experten.

Tatsächlich geht manches bei Ermittlungen so zu, wie man sich das vorstellt. Steht zum Beispiel ein Mitarbeiter unter Verdacht oder ist auch nur sein PC betroffen, wird der „Tatort“ erstmal gesichert, das Büro abgeschlossen oder der Arbeitsplatz abgesperrt. In vielen Fällen ist es wichtig, dass der Rechner keinesfalls ausgeschaltet wird, weil bei Malware sonst häufig wichtige Spuren gelöscht werden – dann unwiederbringlich.

Der digitale Röntgenblick.

Die Spurensuche muss gegebenenfalls weite Teile einer IT-Infrastruktur durchleuchten. Besonders raffinierte Angriffswerkzeuge wie die neueste Generation von „Emotet“ können – meistens unbemerkt – weite Teile eines Netzwerks infizieren und tief in viele Anwendungsprogramme eindringen, zumal beispielsweise Emotet als „Dropper“ noch weitere modulare Malware nachlädt. So werden etwa Mails und Adressbücher ausgespäht und für nachfolgende Angriffe genutzt oder die abgefischten Dateien auch weiterverkauft. Ein solcher Angriff kann also riesige Kreise ziehen und erfordert eine forensische End-to-End-Analyse. Für diese integrierte Gesamtbetrachtung gibt es entsprechende Softwaretools wie X-Ways oder Nuix – im Rennen gegen die Angreifer gilt es aber noch leistungsfähiger zu werden. So wird intensiv an Standardisierung und Automatisierung, auch mittels künstlicher Intelligenz, gearbeitet. Im Gegensatz zu den klassischen SIEM(Security Information and Event Management)-Systemen können selbstlernende Lösungen den Netzwerkverkehr analysieren und sogar bislang unbekannte Angriffsmethoden detektieren und frühzeitig Alarm schlagen. Kreative Cyberkriminelle finden trotzdem immer wieder mögliche Angriffspunkte – und immer mehr Mittäter. Die digitale Verbrechenssparte ist längst, auch im Rahmen organisierter Kriminalität, hochlukrativ.

IT-Forensik kann hierbei viel zur Aufklärung und gelegentlich auch zur Überführung von Tätern beitragen. Bisher haben viele Unternehmen hauptsächlich in präventive Maßnahmen investiert. Als Spezialdisziplin muss Forensik ergänzender Teil eines nachhaltigen Sicherheitskonzepts von Prevention – Detection – Response sein. Dazu gehört noch viel mehr: die Ausprägung von Resilienz, die Sensibilität für Social Engineering wie beispielsweise auf den Vorseiten beschrieben und eine insgesamt noch viel eingehendere Beschäftigung mit IT-Sicherheit.

Aus Schaden wird man klug.

Die forensische Aufklärung geht in vielen Fällen mit einem gewaltigen Schock der betroffenen Organisation einher. Oft zeigt sich, wie wenig geschützt und vorbereitet man war. Insofern ist der Einsatz von Christoph Boser oder Steffen Steitz oft ein Weckruf. Spätestens dann wird über ein Sicherheitskonzept nachgedacht. Eins zu haben und auch konsequent umzusetzen, ist übrigens nicht zuletzt wichtig, um eine Cybercrime-Versicherung abschließen zu können. Damit Schäden abgedeckt werden, die trotz aller Schutzmaßnahmen noch entstehen können. Denn hundertprozentige Sicherheit gibt es nicht. Man kann nur bestmöglich vorsorgen. IT-Forensiker können ein Lied davon singen.

Die Spurensucher.

Christoph Boser ist Senior Consultant bei Bechtle in Offenburg und gleich dreifach zertifiziert: als Datenschutzbeauftragter, IT-Sachverständiger Forensik und IT-Datenschutzauditor. Steffen Steitz ist IT Solution Architect bei Bechtle in Chemnitz und berät und unterstützt wie sein Kollege Unternehmen und Behörden in Sachen IT-Sicherheit nicht nur generell, sondern auch speziell mit forensischen Einsätzen. Außerdem übernimmt er bei betroffenen Unternehmen auch das Krisenmanagement. Beide gehören zum schnell wachsenden Bechtle Competence Center Cyber Crime & Defense.

Die Einsnulleinsnull als digitale Notrufnummer gibt es noch nicht. Gleichwohl gilt für viele Zwischenfälle, die den Datenschutz betreffen, eine Pflicht zur Meldung an die Behörden innerhalb von 72 Stunden. Bei Nichteinhaltung dieser Meldepflicht muss mit empfindlichen Strafen gerechnet werden.

Wenn die Datenträger physikalisch nicht defekt sind, gelingt es den IT-Forensikern bei Bechtle in gut 90 % aller Fälle, verloren geglaubte Daten wiederherzustellen.

DER QUANTEN DUALISMUS.

Mit Quantencomputern ist wohl zu rechnen. Wann wir davon profitieren, weiß zwar noch niemand, wofür wir sie nutzen werden, kann man sich aber schon vorstellen. So wie Quanten selbst gleichzeitig mehrere Zustände haben können, sind ihre Einsatzmöglichkeiten nicht nur vielfältig, sondern auch mehrdeutig. Denn der Quantensprung in der Leistungsfähigkeit ermöglicht einerseits, komplexere Probleme denn je zu lösen – und andererseits, jede heute eingesetzte Verschlüsselungstechnologie zu knacken. Fragt sich, wer womit zuerst am Start ist.

Google nahm 2019 in Anspruch, mit seinem Quantenprozessor „Sycamore“ erstmals die sogenannte Quantenüberlegenheit erlangt zu haben: per Definition die Lösung einer Rechenaufgabe, für die der bisher schnellste Computer der Welt 10.000 Jahre benötigt hätte. Ob das im Vergleich tatsächlich amtlich ist, mag strittig sein. Dass „Sycamore“ nach 200 Sekunden das Ergebnis präsentierte, gilt gleichwohl als wichtiger Durchbruch: ein „Sputnik-Moment“. Jetzt geht es darum, die Stabilität der filigranen Quantenzustände so zu verbessern, dass ein fehlerfreies gewünschtes Verhalten erzielt wird.

Ein Quantenbit, kurz Qubit, kann anders als herkömmliche Bits gleichzeitig 0 und 1 sein. Diesen Simultanzustand nennt man Superposition. Indem mehrere Qubits miteinander verschränkt werden, vervielfachen sich diese Zustände. Ein Algorithmus ermöglicht, dass damit parallel und rasend schnell Daten verarbeitet werden können. Diese Leistung steigt mit jedem zusätzlich verschränkten Qubit exponentiell. Der aktuelle Rekord liegt mit Googles „Sycamore“ bei 53 Qubits. Allerdings beträgt dessen Fehlerrate immer noch 0,3 Prozent. Damit sind drei von tausend Rechenoperationen falsch. Zu viel – und damit bisher nicht ausreichend zuverlässig.

Ein Resultat von Googles Forschung ist auch, dass die Quantentechnologie mit einem Mal einer breiten Öffentlichkeit bewusst wurde. Kein Medium von Relevanz, das nicht darüber berichtet hätte. So könnte eine Diskussion über den sinnvollen Einsatz, die Herausforderungen und auch mögliche Gefahren ihren Anfang nehmen. Gesichert gilt, dass Quantencomputer besonders von Nutzen sind, um riesige Datenmengen, insbesondere mit komplexen wechselnden Abhängigkeiten, zu verarbeiten. Anwendungsbeispiele sind die Steuerung von Verkehrsnetzen und Logistiksystemen. Oder die Entwicklung von Pharmazeutika, die auf individuelle Krankheitsbilder von Patienten zugeschnitten werden. Generell könnte man ganz neue Herausforderungen und Problemlösungen in Chemie, Biologie und Physik damit angehen und beispielsweise bisher undenkbare Werkstoffe und Materialien kreieren. Ein sich anbietender Nutzen liegt in der Analyse komplexer Märkte, etwa der Finanzwirtschaft, und auch in der Weiterentwicklung künstlicher Intelligenz durch maschinelles Lernen.

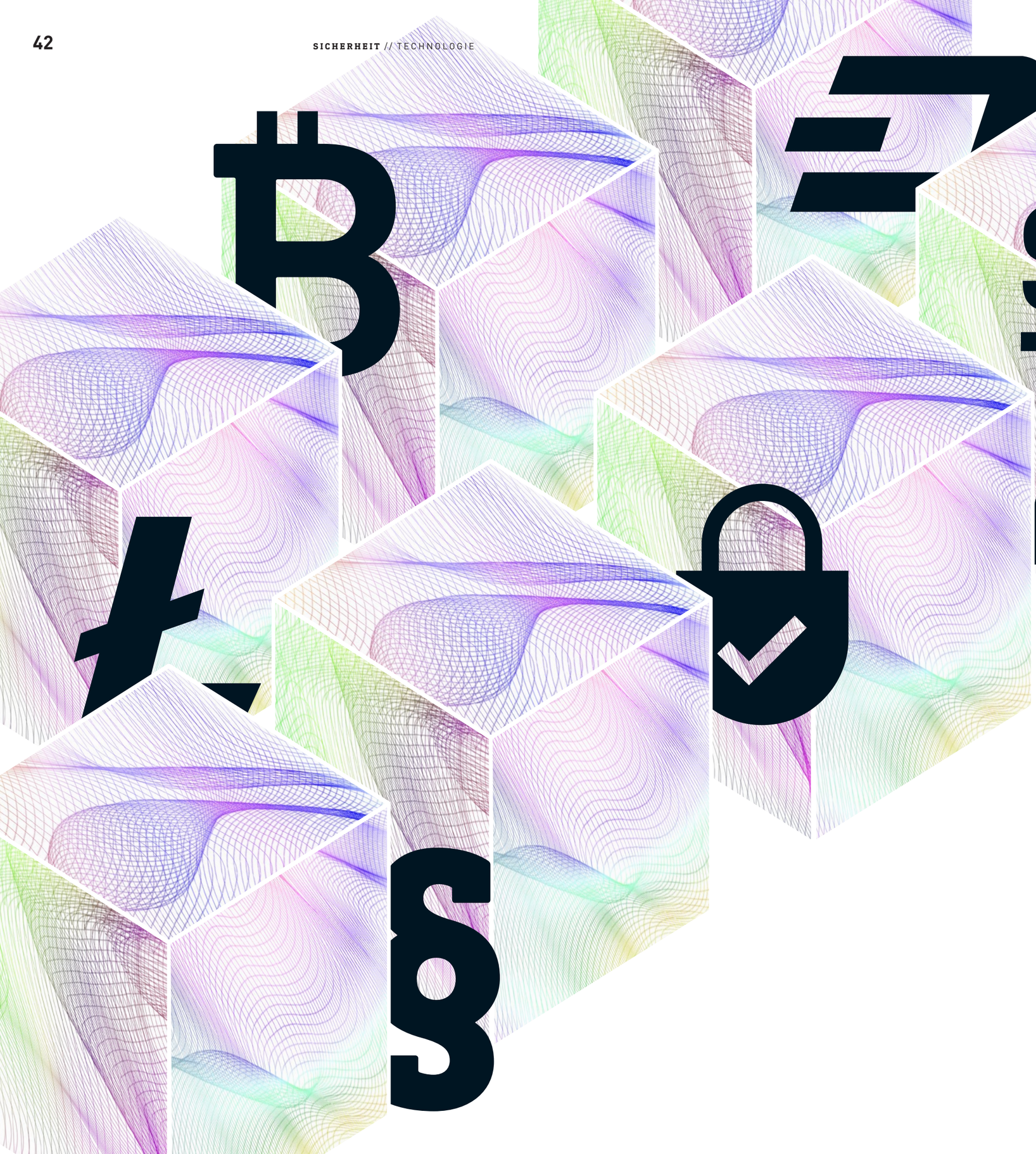
Europa gilt als weltweit führend in der Quantenphysik – mit rund 50 % aller wissenschaftlichen Publikationen und fast 40 % der Forscher in diesem Bereich. Auch Deutschland sieht sich gut aufgestellt. Die Bundesregierung hat zudem ein Rahmenprogramm mit konkreten Maßnahmen und Zielen definiert und in der laufenden Legislaturperiode 650 Millionen Euro für Forschungszwecke bereitgestellt. Ein breites Spektrum an Forschungsinstitutionen wirkt dabei mit: von der Max-Planck-Gesellschaft über die Fraunhofer-Gesellschaft und Helmholtz-Gemeinschaft bis zur Deutschen Forschungsgesellschaft und anderen. Auch strategische Partnerschaften treiben die Entwicklung voran. So kooperiert beispielsweise die Bundeswehr mit IBM beim Betrieb eines Quanten-Hubs am Forschungsinstitut Cyber Defence CODE in München.

Schlüssel zur Sicherheit.

Zur hochsicheren Datenübertragung wird schon heute im kleinen Maßstab, etwa von Banken und Regierungen, Quantenkryptografie bzw. Quantenschlüsselverteilung (QKD – Quantum Key Distribution) eingesetzt. Vereinfacht gesagt, werden dabei die verschränkten Quantenobjekte, z. B. Photonen, an zwei verschiedenen Orten vermessen. Der einwandfreie Zustand bestimmter Parameter bestätigt die Sicherheit. Die Reichweite der QKD-Anwendungen mittels Glasfaser ist allerdings noch beschränkt. Der Clou des Verfahrens: Im Unterschied zur klassischen Kryptografie bilden keine mathematischen Prinzipien, sondern physikalische Naturgesetze die Grundlage – wie generell bei Quantentechnologien.

Das Potenzial zur Entschlüsselung ist die Schattenseite der Einsatzgebiete. Funktionierende Quantencomputer wären imstande, herkömmliche Verschlüsselungsverfahren problemlos „auszurechnen“. Noch ist das nicht möglich. Man geht von Computern mit mindestens mehreren tausend Qubits aus, die dafür erforderlich wären. Abgesehen davon wäre der theoretisch erforderliche Stromverbrauch absurd hoch. Sorgen macht das möglicherweise zukünftige Entschlüsseln heute langfristig angelegter kryptografischer Sicherungen – etwa von Satelliten mit ihren langjährigen Laufzeiten. Daher werden schon Lösungen einer „Postquantenkryptografie“ entwickelt, die vor hypothetischen Quantenangriffen schützen. Und das deutsche Pilotprojekt „QUBE“ verfolgt konkret das Ziel einer QKD-gesicherten Satellitenplattform.

Computer und Kommunikation – aber auch messtechnische Anwendungen – werden mithilfe der Quantenphysik intensiv weiterentwickelt. Die weltweit darin investierten Ressourcen sind immens. Die USA und China unternehmen hier viel. Insbesondere unter Sicherheitsaspekten ist schon jetzt ein Wettrennen (oder: Wettrüsten?) im Gang. Aber auch vielfältige Verbesserungen ganzer Technologiezweige stehen in Aussicht. Ein weites Feld zu erforschender Möglichkeiten bietet spannende Perspektiven, die es von uns allen zu verfolgen lohnt – auch wenn es etwas kompliziert erscheint. Ein ganz großes Ding, die kleinen Elementarteilchen.



SICHERE TRANS AKTIONEN.

Die Blockchain zur sicheren, schnellen und transparenten Abwicklung von Transaktionen gewinnt an Bedeutung. Ihre Unabhängigkeit von vermittelnden Plattformen könnte ein neues Paradigma setzen. Für die Nutzung von Blockchains prädestiniert sind vor allem unternehmensübergreifende dezentrale Netzwerke – etwa in der Logistik, einer zukünftigen Energiewirtschaft, aber auch in klassischen Produktionsprozessen, die immer mehr vom Internet der Dinge geprägt sind. Wie alltagsnah ist das? Und wie kann die Blockchain sinnvoll in bestehende Unternehmensprozesse integriert werden?

Mit Blockchains lässt sich praktisch jede Transaktion digital abbilden. Ob dabei Geld oder Güter bewegt werden, ist egal. Ist ein Vertrag erfüllt, können Rechnungen binnen Sekunden bezahlt sein. Banken, die mitverdienen, und komplizierte Auslandsüberweisungen kann man sich dabei sparen. Ein passendes Buzzword hat sich dafür schon gefunden: das „Internet der Werte“.

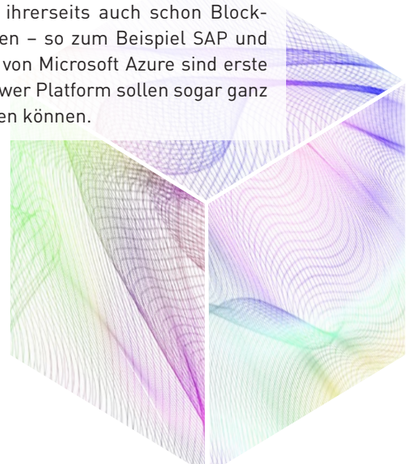
Die vertrauensvolle Kooperation in vernetzter Dezentralität ist bei Bechtle seit langem gelebter Alltag. Jetzt könnte sich das Prinzip auch mehr und mehr in der Technologiewelt durchsetzen: mit Etablierung der Blockchain. Das Konzept als solches ist ja gar nicht so neu und wurde schon 2008 von Satoshi Nakamoto beschrieben – seinerzeit zur Einführung des Bitcoins. In der öffentlichen Wahrnehmung stand der Aspekt der Kryptowährung auch stark im Vordergrund – nicht unbedingt zu Recht. Denn im Kern ist die Blockchain eine Datenbank zum Speichern und Verwalten von Daten – nur nicht wie üblich mit zentralen Servern, sondern in Datensatzblöcken auf viele Rechner verteilt.

Alle Teilnehmer des Netzwerks verfügen über dieselbe Kopie der Blockchain und verifizieren die Echtheit der hinterlegten Daten untereinander, auch jeweilige Änderungen und Aktualisierungen. Es gibt keine vermittelnde Instanz, so dass Blockchains flexibel zu allen möglichen Zwecken gebildet werden können. Manipulationen von außen lassen sich praktisch ausschließen, weil alle dezentralen Einheiten unmöglich, noch dazu gleichzeitig, zu beeinflussen sind.

Fix und fair.

Die Peer-to-Peer-Mechanik der Blockchain kann sich beispielsweise in Logistikprozessen entfalten. Hierin sind, oft länderübergreifend, zahlreiche Akteure involviert: diverse Produktionsunternehmen, Speditionen, Verteilzentren, Zustelldienste und andere mehr. Ohne sich auf eine Abwicklungsplattform verständigen zu müssen oder sich mit E-Mails nebst Anhängen, mitgeführten Papieren und häufig noch Faxen zu verzetteln, werden alle Abläufe per Blockchain abgebildet. Immer aktuell, für alle Beteiligten transparent und revisionssicher. Vom einzelnen Paket über Paletten und Container bis zu ganzen Schiffsladungen lassen sich beliebige Liefereinheiten erfassen und lückenlos verfolgen. Dabei können alle möglichen Konditionen und Parameter als Vertrag hinterlegt werden. Individuell für jeden Lieferprozess.

Prinzipiell ist das Verfahren auf das komplette Supply Chain Management, ja den gesamten Produktlebenszyklus, übertragbar. Unternehmen nutzen aber natürlich hierfür längst eingeführte Softwaresysteme, die wieder mit anderen Geschäftsprozessen verbunden sind. Davon wird man sich kaum abkoppeln können und wollen. Die führenden Systemanbieter integrieren ihrerseits auch schon Blockchain-Lösungen in ihre Anwendungen – so zum Beispiel SAP und Microsoft. Für die Cloud-Umgebung von Microsoft Azure sind erste Features verfügbar. Auf Basis der Power Platform sollen sogar ganz leicht Blockchain-Apps erstellt werden können.

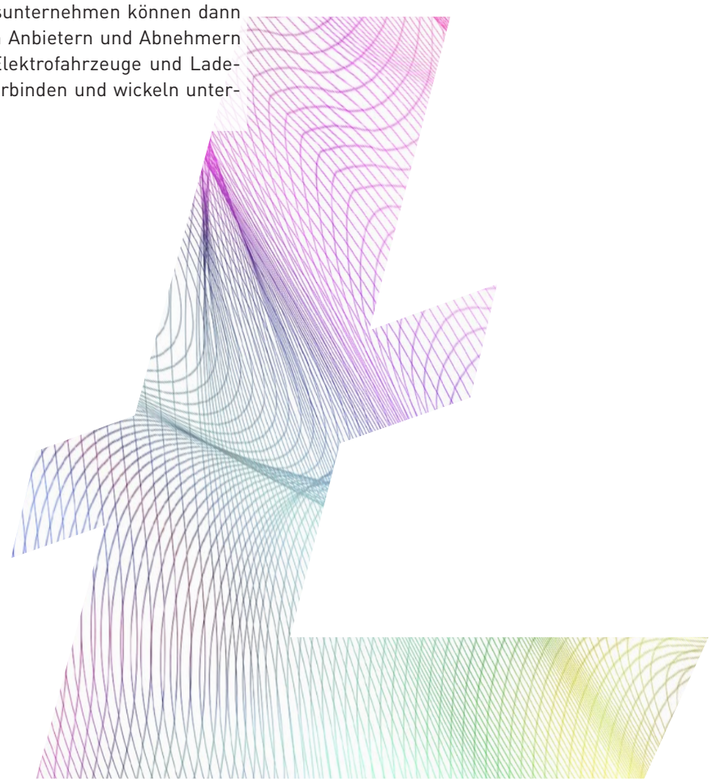


Auch in das Internet of Things kann die Blockchain-Technologie sinnvoll eingebunden werden. In Fertigungsprozessen erzeugte Maschinendaten etwa zur Produktqualität können in Blockchains hinterlegt und dokumentiert werden, damit alle Beteiligten des Wertschöpfungsnetzes darauf Zugriff haben. So kann sich jeder zu jeder Zeit davon überzeugen, ob die Dinge laufen, wie sie sollen. Damit entstehen wasserdichte Fertigungsprotokolle. Schummeln ist an keiner Stelle möglich.

Geschäftige Geräte.

Die Maschinen selbst sollen auf diesem Weg auch untereinander kommunizieren und in der Blockchain hinterlegte sogenannte „Smart Contracts“ selbstständig ausführen. Ein solcher Mikrovertrag kann zum Beispiel besagen, dass Maschine A, wenn sie Nachschub braucht, ihn bei Maschine B bestellt. Ganz automatisch. Es kann auch sein, dass Maschine B ihre Leistung an Maschine A verkauft. Die Abrechnung und Zahlung kann dann per Kryptowährung erfolgen. Klingt doch smart. Ach ja: Wenn Maschinen wie angedacht besteuert werden, hängt man eben noch die entsprechende Blockchain dran.

In der Energiewirtschaft findet sich noch ein großes Einsatzgebiet. Mit der erwarteten Dezentralisierung und viel kleinteiligerer Produktion regenerativer Energien ist der Markt zukünftig wie gemacht für das Peer-to-Peer-Prinzip der Blockchain. Ohne Umwege über Energiebörse und Versorgungsunternehmen können dann Strom und Wärme zwischen beliebigen Anbietern und Abnehmern gehandelt und verteilt werden. Auch Elektrofahrzeuge und Ladestationen lassen sich via Blockchain verbinden und wickeln untereinander smarte Tankverträge ab.



Am Stromverbrauch muss gedreht werden.

Die Energieeffizienz der Blockchain-Technologie lässt – noch – sehr zu wünschen übrig, schon wegen der Vielzahl benötigter Clients. Das gilt insbesondere für den ursprünglich eingeführten Algorithmus, mit dem Konsens über eine Transaktion erzielt wird: Dabei müssen Teilnehmer einen „Proof of Work“ durchführen und eine Rechenaufgabe lösen, um den Vorgang zu bestätigen – wie beim Schürfen von Bitcoins. Der Energieverbrauch einer massenhaft verbreiteten Nutzung von Blockchains wäre so gar nicht darstellbar. Deshalb wird intensiv an immer besseren Konsens-Algorithmen gearbeitet, die weniger Ressourcen verbrauchen.

ZEICHEN VON SICHERHEIT.

ZERTIFIZIERTE SICHERHEIT.

Siegel geben Sicherheit – auch in der Informationstechnologie. „IT-Security made in Germany“ spiegelt nicht zuletzt die hohen Standards von Datenschutz und Datensicherheit in Deutschland wider. Außerdem verbindet sich damit das landestypische Qualitätsversprechen der hiesigen Industrie. Mit Unterstützung von Bundeswirtschafts- und Bundesinnenministerium wird das Siegel vom Bundesverband IT-Sicherheit e.V. (TeleTrust) getragen. Auch Bechtle zählt zu den Verbandsmitgliedern.

SICHERE PRODUKTE.

Egal, ob Toaster, Föhn, Wasserkocher, Kinderspielzeug oder sonst ein Produkt: Das GS-Zeichen garantiert „Geprüfte Sicherheit“ gemäß Produktsicherheitsgesetz (ProdSG). Unter Berücksichtigung deutscher und europäischer Normen soll es von Staats wegen Leib und Leben schützen.

FAIR GEHANDELT.

Wer sichergehen will, Produkte zu kaufen, für die ihre Erzeuger einen angemessenen Preis erzielen, achtet auf das Fairtrade-Siegel. Es kennzeichnet überwiegend Lebensmittel, Kosmetika und Textilien, aber auch Gold. Neben den ökonomischen Kriterien werden soziale und ökologische Standards zugrunde gelegt. Insbesondere sollen damit die Arbeitsbedingungen in Entwicklungs- und Schwellenländern verbessert und Kleinproduzenten unterstützt werden.

TOPARBEITGEBER.

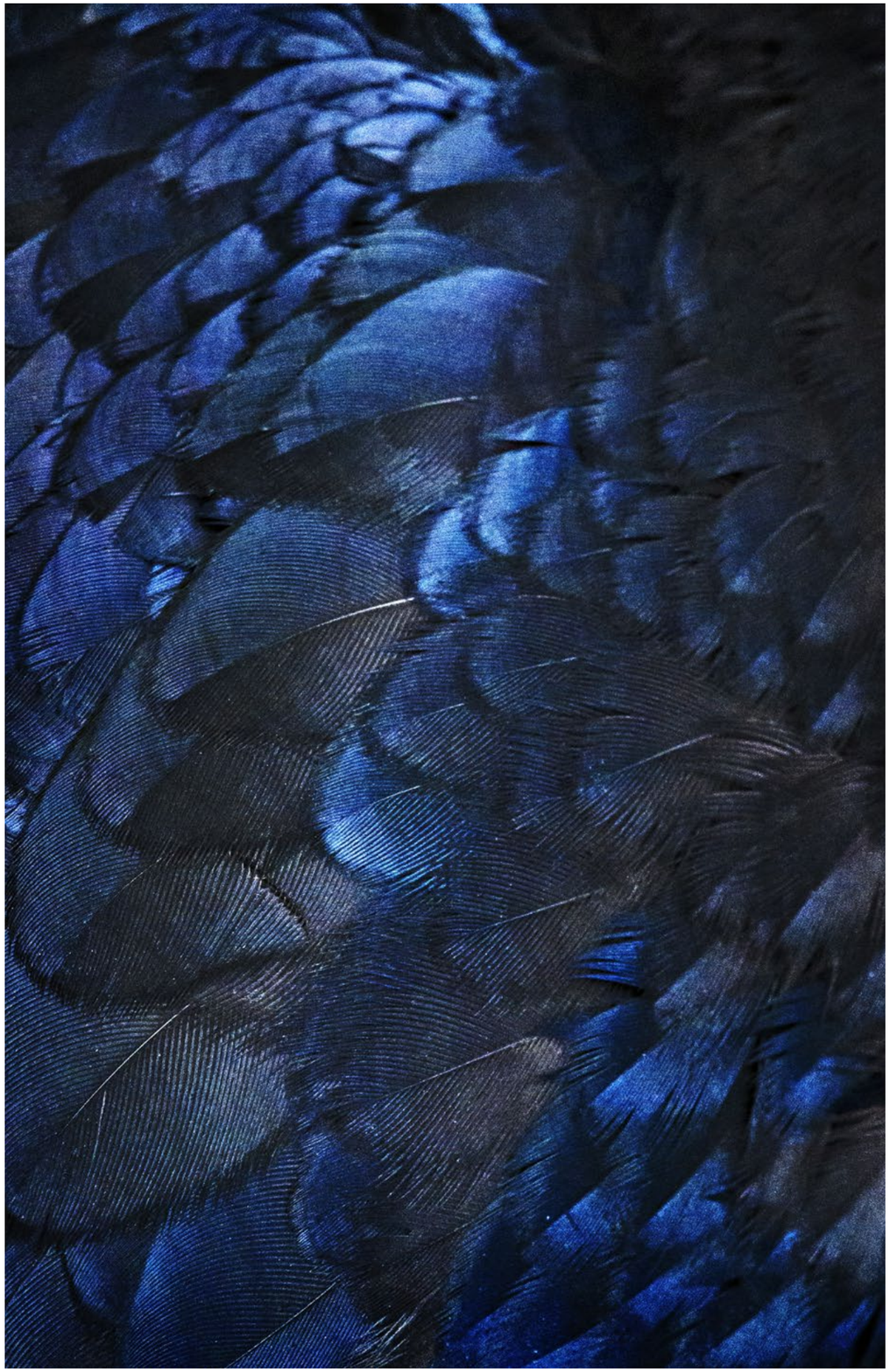
Fachkräfte, insbesondere im Bereich IT, sind heute Mangelware. Deshalb ist es besonders wertvoll, sechs Jahre in Folge als „Best Recruiter“ ausgezeichnet zu werden. Demnach gelingt es Bechtle kontinuierlich, seine Qualitäten als Arbeitgeber gut rüberzubringen und damit Bewerber und Mitarbeiter zu gewinnen. Allein 2019 sind über tausend neue Kolleginnen und Kollegen dazugekommen. Übrigens: Wir suchen weiterhin.

ECHT BIO.

Es gibt jede Menge verschiedene Kennzeichnungen biologischer Lebensmittel. Am meisten verbreitet ist das sechseckige deutsche Bio-Siegel in Verbindung mit dem EU-Bio-Logo, auch Euro-Blatt genannt. Umschreibungen wie „kontrollierter Anbau“ oder „alternative Haltung“ sind hingegen gar nichts wert. Im Vergleich zum staatlichen Bio-Label gibt es aber viel strengere, vor allem der Anbauverband Demeter setzt höchste Standards.

DAS PAPIERSIEGEL.

Das Magazin, das Sie in Händen halten, wurde auf FSC-Papier gedruckt. Es stammt demnach aus zertifizierter nachhaltiger Forstwirtschaft gemäß dem Forest Stewardship Council. Der FSC-Standard erfordert die Einhaltung von zehn Prinzipien zum Schutz der Wälder vor Abholzung. Zwar gibt es auch Kritik daran, dass die Vergabe des Siegels nicht immer konsequent sei – ein besserer Standard hat sich jedoch noch nicht etabliert.



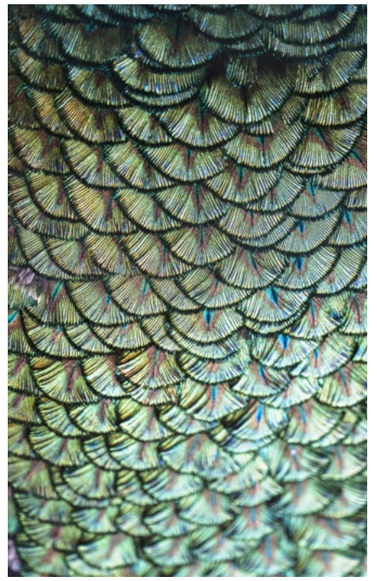
KOLKRABE
HERKUNFT: WELTWEIT

NACHHALTIG BEFLÜGELT.

Wer Ziele hat und konsequent einem Weg dahin folgt, erreicht mehr als jemand mit weniger planvollem Vorgehen. Genau so funktioniert nachhaltiges Unternehmertum. Mit einer klaren Vision für die nächste Dekade und dem wirtschaftlichen Freiraum für darauf ausgerichtete Investitionen. Das gibt Sicherheit für die Zukunft und bietet langfristige Perspektiven für die Mitarbeiterinnen und Mitarbeiter. Getragen von der Unternehmensvision 2030, werden das bei Bechtle immer mehr.

STRUKTURELLE VERLÄSSLICHKEIT.

Kommt der Zug – pünktlich? In der richtigen Wagenreihung? Hält die Partei, die ich gewählt habe, ihre Wahlversprechen? Erfüllt der Stürmer meiner Lieblingsfußballmannschaft seinen Vertrag? Wird die Großbaustelle der Stadt frist- und kostengerecht fertig? Fällt heute kein Unterricht aus – und wie viele Schüler schwänzen aber? Kommt der Elektriker wie angekündigt oder bleiben die Herdplatten kalt? Komme ich rechtzeitig zu meinem Termin oder ist mal wieder Stau? Worauf man sich verlassen kann, sind nicht ganz unwichtige Fragen der Sicherheit im Alltag.



PFAUENHAHN
HERKUNFT: INDIEN, SRI LANKA

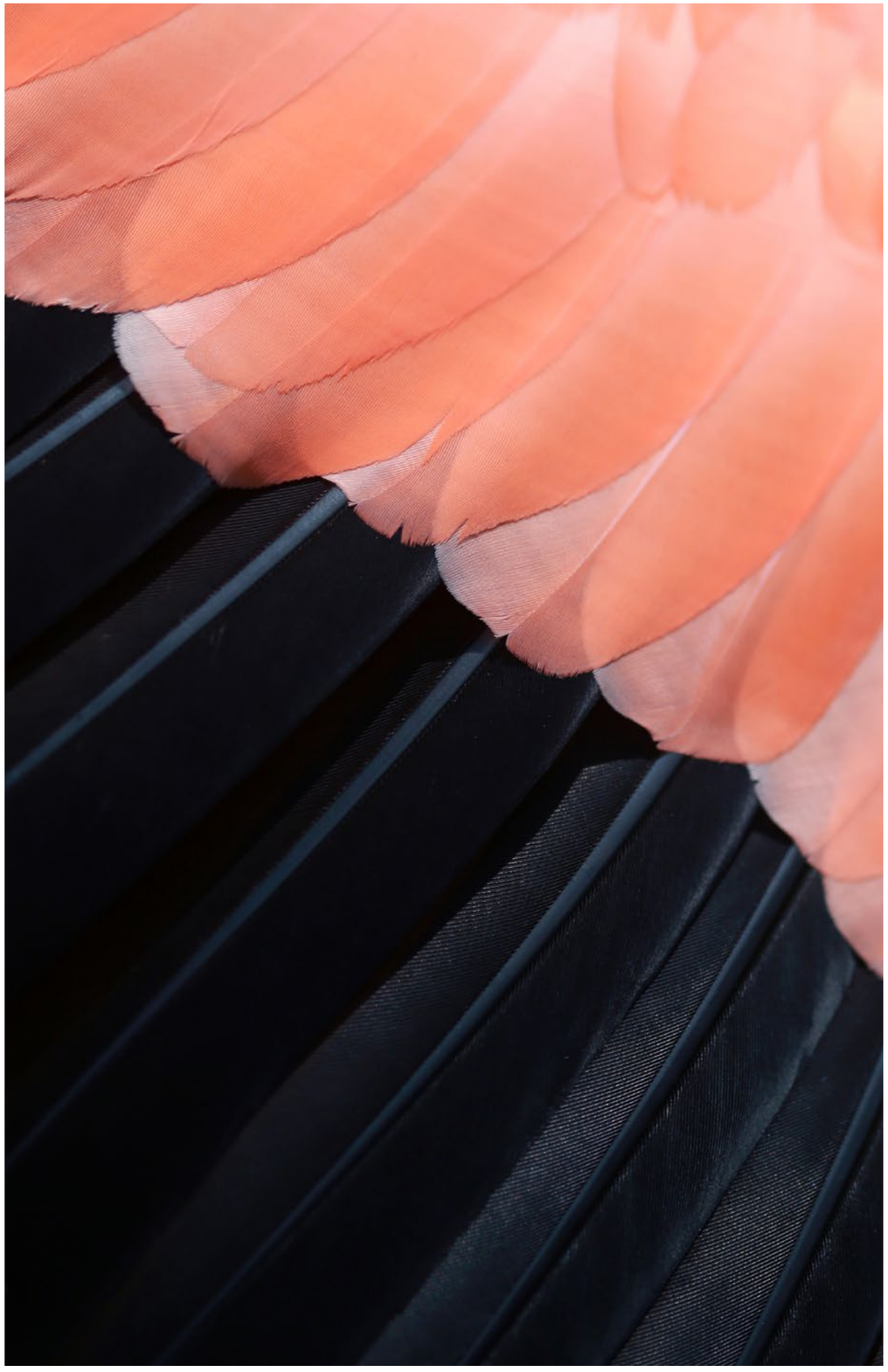
ÖFTER MAL KUSCHELN.

In diesen disruptiven Zeiten heißt es immer wieder: Raus aus der Komfortzone! Gemütlich verharren ist im Job auf Dauer nicht drin. Umso wichtiger wird es, sich zum Ausgleich Schutzzonen zu schaffen, in denen man zur Ruhe kommen und sich erden kann. Ob das beim Yoga, Mittagsspaziergang oder Jodeln passiert, ist egal. Hauptsache: Rein in die Komfortzone!

SILBERFASAN
HERKUNFT: SÜDOSTASIEN

WISSEN TRÄGT WEITER.

Ausbildung und lebenslanges Lernen sind in unserer komplexen Welt Schlüsselkompetenzen. Erworbenes Wissen und die Fähigkeit, es auszubauen, bilden die Eintrittsvoraussetzungen für ein erfolgreiches Berufsleben. In dessen Verlauf erfordern jedoch immer schnellere Veränderungen und die fortgesetzte Digitalisierung, sich weiterzuentwickeln und dazuzulernen oder sich ganz neue Fähigkeiten anzueignen. Auch für unser Weltverständnis müssen wir mit Informationen souverän umgehen können: sie beschaffen, bewerten und einordnen – auch um Fehlinformationen nicht auf den Leim zu gehen. In der Zusammenarbeit gilt es, Wissen nicht für sich zu behalten und zu horten, sondern gezielt zu teilen. So kann Team-Intelligenz ein Vielfaches daraus machen. Nicht zuletzt: Etwas zu wissen, ermöglicht die Entscheidungssicherheit, das Richtige zu tun. Und fundiertes Handeln ist ein kostbarer Wertbeitrag in volatilen Zeiten.



FLAMINGO
HERKUNFT: AFRIKA, ASIEN, EUROPA

INDONESISCHER ARGUSFASAN

HERKUNFT: INDONESIEN, SÜDOSTASIEN

WILDER TRUTHAHN

HERKUNFT: USA

ABGETAUCHT.

Die Tiefen der Ozeane bergen vielerlei Risiken. Klimatische Veränderungen bedrohen die Ökosysteme und Temperaturströme. Während Pflanzen und Spezies dezimiert werden, siedeln auf dem Meeresboden zunehmend artfremde Strukturen. Die Rede ist dabei von tausenden Kilometern Glasfaserkabeln, von denen immer mehr das Internet über alle Kontinente verbinden. Diese vor Datenspionage und Sabotage zu schützen, ist eine bedeutende Sicherheitsanforderung. Denn ohne Seekabel ist nicht nur das Serien-Streaming gefährdet.

WAHRES BEWAHREN.

Viele von uns haben reichlich Dinge um sich. Vieles davon braucht wahrscheinlich kein Mensch – aber sie sind uns lieb und teuer. Sich zum Wert von Dingen selbst zu befragen, ist eine gute Übung für die Hygiene von Haben und Sein. Die japanische Kultur kennt für die Verbundenheit mit den Dingen den Begriff „Aichaku". Welche Gegenstände wecken in uns Gefühle, Fürsorge und den Wunsch, sie ein Leben lang zu besitzen? Die Beschäftigung damit ist ein schönes Stück Selbstversicherung.

WAS BIETET SCHUTZ?

DIE NESTWÄRME.

Nicht nur Küken brauchen sie, um schlüpfen und sich entwickeln zu können: die Nestwärme. Auch menschlicher Nachwuchs benötigt die Geborgenheit und Wärme seiner Eltern, um groß und stark zu werden. Ist es aber allzu gemütlich, dann droht das Nesthäkchensyndrom. Die Kinder werden nie richtig flügge und verkümmern in der Obhut ihrer Eltern. Oder sie genießen einfach das Leben im Hotel Mama. In der Tierwelt sind solche Eigenheiten nicht bekannt.

DER NOTRUF.

Notrufsäulen sind die orangefarbenen Retter an den Autobahnen. Einerseits ist es natürlich gut, dass es sie gibt. Andererseits will kein Autofahrer je in die Sprechmuschel um Hilfe rufen müssen. Die Frage ist, wie lange sie überhaupt noch existieren werden. Denn dank Smartphones und Autos, die über Internet verfügen: Wer braucht die SOS-Säulen eigentlich noch? Vielmehr dürfte ihnen doch schon bald das gleiche Schicksal wie den Telefonzellen beschieden sein, die ja auch gänzlich verschwunden sind. Wahrscheinlich trauert man ihnen dann ein wenig nach.

DER FINGERHUT.

Es gibt sie in den erstaunlichsten Ausführungen: Fingerhüte. Im weltweit einzigen Fingerhutmuseum in Creglingen kann man die Extravagantesten von ihnen bewundern. Schon vor 2.500 Jahren nutzten Menschen Fingerhüte aus Bronze zum Nähen. Um 1500 entdeckte Paracelsus das Metall Zink. Nun fertigte man in Serie Messingprodukte wie den Fingerhut. Wo heute noch genäht wird, findet man auf jeden Fall einen kleinen Helm für die Fingerkuppe.

DAS MAKE-UP.

Übersetzt heißt es auch: etwas erfinden, konstruieren. Das geschminkte Gesicht präsentiert ein idealisiertes Bild und zeigt eine Fassade, die vor den Blicken der Außenwelt abschirmt. Make-up verbindet Selbstschutz und Selbstinszenierung. Wie viel davon ist schön? In sozialen Medien lässt sich kaum noch jemand „ungephotoshoppt" sehen. In Asien gilt das sogar als schlechtes Benehmen – so als ginge man nackt aus dem Haus. Dabei kann uns doch die „ungeschminkte Wahrheit" einander näherbringen.

DER SCHIRM.

Im 19. Jahrhundert kamen Schirme in Mode, die mit einem metallenen Erdungsband ausgestattet waren. Angeblich boten sie so Schutz vor Blitzen. Das war höchst fragwürdig. Ansonsten sind aber Parapluies, wie sie in Frankreich heißen, lange Zeit auch ein Modeaccessoire in London und Paris gewesen, bei denen es weniger auf den Schutz vor Sonne und Regen ankam als vielmehr auf Sicherheit vor den strengen Blicken modebewusster Passanten. Heute sind vor allem Knirpse gefragt, weil unauffällig, leicht zu verstauen und weil sie etwa bei Flugreisen kaum ins Gewicht fallen.

DER ALU-HUT.

Es gibt immer mal Bilder, in denen verstrahlte Typen einen aus Aluminium gebastelten Hut aufhaben, damit ihre Gedanken nicht von Aliens gelesen werden können. Man schützt damit angeblich seine Hirnströme vor Telepathie. Ja, natürlich schirmt Aluminium, sofern es dick genug ist, gewisse Radiowellen ab oder sorgt für Funken in der Mikrowelle. Ob deswegen Alu-Hüte bei einer Invasion von Außerirdischen genügend Schutz bieten, darf bezweifelt werden. Kein Wunder, dass ihre Träger nicht den besten Ruf genießen, gelten sie doch als wunderlich und Verschwörungstheorien zugeneigt. Dann lieber ein lustiges Gesicht aufsetzen.

DIE NATURVERPACKUNG.

Dass die Banane so schön in Schale daherkommt, ist natürlich praktisch: Verpackung inklusive. So wird nicht gleich ungewollt Brei daraus. Was hier automatisch ökologisch an Bäumen wächst, findet zunehmend Anwendung bei der Materialherstellung: mit biologischen Verpackungen aus Algen, Bambus, Hanf oder auch Zuckerrohr. Der Plastikbann treibt diese Entwicklung des Naturschutzes nun umso stärker voran.

Das WIR leben.

Sicherheit in Verbundenheit.

Es gehört zur menschlichen Natur, Gemeinschaften zu bilden, um darin Geborgenheit und Sicherheit zu finden. Schon der griechische Philosoph Aristoteles charakterisierte den Menschen als „zoon politikon“: ein soziales Wesen. Der familiäre Verbund bildet die Keimzelle des Zusammenlebens – und immer noch ihren harten Kern. Zusammenhalt findet man heute aber auch in vielerlei anderer Form. Vom Fußballverein bis zur Multigenerationen-WG, von der Kirchengemeinde bis zur Facebook-Gruppe, von der Hardrockband bis zum Kleingartenverein. Man sucht und braucht Gemeinsamkeiten. Dringender denn je. Denn unsere Gesellschaft vereinzelt in immer mehr Singlehaushalten. Einsamkeit ist wie Burnout zum Begriff geworden. Ältere Menschen bleiben oft für sich und werden allein gelassen.

Gleichzeitig ist die Welt von Partikularinteressen geprägt – nach dem Motto: „Wenn jeder an sich denkt, ist an alle gedacht.“ Individualismus und Autonomiebestreben stellen sich der als fremdbestimmt empfundenen Globalisierung entgegen. Für alle, die ihr Glück dennoch nicht allein suchen wollen, sondern in Verbundenheit leben möchten, gibt es Anknüpfungspunkte. Historische wie zukunftsweisende. So erleben Genossenschaften eine Renaissance, um sowohl Wohnen als auch Unternehmen mit mehr Gemeinsinn zu organisieren. Nachbarschaften werden digital vitalisiert, sei es, um Straßenfeste und Fahrdienste zu koordinieren oder um gegenseitig Gartenwerkzeuge auszuleihen. Das Teilen von Dingen und Erlebnissen ist in vielen Bereichen ein Faktor für mehr Miteinander. Mehr und konkrete Verbundenheit findet sich in den beispielhaften Projekten auf diesen Seiten.

Im Kinderhaus KINJA des Heilbronner Neckarbogens besuchen 80 Kinder die Kita. Außerdem wohnen hier alleinerziehende Mütter und Väter mit ihrem Nachwuchs.

Das Vereinswesen hat seine Wurzeln im aufgeklärten Bürgertum und war schon im 18. Jahrhundert ständeübergreifend aufgestellt. Diese Tradition hat sich bis heute erhalten. In Vereinen kommen alle Gesellschaftsschichten zusammen – sie haben buchstäblich etwas Vereinendes. Hier kann man noch aus seiner Filterblase heraustreten und milieuübergreifend singen, kickern, synchronschwimmen und vieles mehr. In Deutschland ist die Mitgliedschaft in rund 580.000 Vereinen möglich.

Das Stadtquartier Neckarbogen.
In Nachbarschaft der Bundesgartenschau 2019 errichtete die Stadt Heilbronn ein neues Quartier mit 22 Gebäuden für 3.500 Bewohner und 1.000 Arbeitsplätze. Schon bei der Projektentwicklung waren neben Architekten und Stadtplanern die Bürger gefragt. Mit zahlreichen Gesprächsrunden, Informationsveranstaltungen, Workshops, Ausstellungen, BUGA-Cafés sowie Rundgängen stellte man immer wieder Transparenz und Nähe zum Bauprojekt her. Gemeinsam wurden innovative Konzepte für die Nutzung, Mobilität und Energie entwickelt. Zudem sollte gewährleistet sein, dass sich die Anzahl der Mieter und Eigentümer die Waage hält und die soziale Mischung stimmt. Hier sollen Menschen mit unterschiedlichen Berufen, unterschiedlichen Alters und diverser Familienstrukturen auf Dauer leben. Und wenn sich die Lebenssituation der Bewohner ändert, sollen sie nicht wegziehen müssen, weil auch die Wohnungen selbst schnell und einfach veränderbar sind. So können größere Wohnungen zu Ein-Zimmer-Apartments verkleinert oder diese umgekehrt vergrößert werden. Eine Anpassungsfähigkeit, die in solcher Konsequenz und Größenordnung im Wohnungsbau Maßstäbe setzt.

Wohngemeinschaften en gros.
Sicherer und adäquater Wohnraum, insbesondere in Ballungszentren, ist aktuell eine der elementaren gesellschaftlichen Herausforderungen. Den großen Städten geht die Lebendigkeit der sozialen Mischung verloren, wachsende Ungleichheiten segregieren die Einwohnermilieus voneinander. Eine große Lücke tut sich auch zwischen Stadt und Landleben auf. Die Arbeitsmöglichkeiten und Infrastrukturen „in der Pampa" veröden immer mehr. Doch langsam beginnt sich mit der Digitalisierung eine neue Land-Wirtschaft zu entwickeln. Denn dem Laptop ist es egal, wo er genutzt wird. So werden jenseits der Speckgürtel neue Lebensgemeinschaften kultiviert. Und auch in den urbanen Zentren tut sich was. Innovative Wohnprojekte wachsen zwar noch nicht wie Pilze aus dem Boden, aber immerhin …

Beim „Radeln ohne Alter" kutschieren ehrenamtliche Rikschafahrer und -fahrerinnen Bewohner von Alten- und Pflegeheimen. Unterwegs werden Erlebnisse und Lebensgeschichten geteilt.

Das Singen im Chor schafft Verbundenheit und beschert Glückshormone. Mi-mi-mi-mitmachen!

Das Erlangen der Staatsbürgerschaft macht amtlich, dass Menschen dazugehören, eine Heimat gefunden haben. Das Land, in dem man lebt, verbrieft damit Rechte und Pflichten, Sicherheit und Verbundenheit. Der Landespass ist Ausweis gegenseitiger Verlässlichkeit von Staat und Bürgern und nicht zuletzt ein Dokument gesellschaftlicher Stabilität.

Die Zürcher Kalkbreite.
Schon 2014 setzte ein gemeinschaftliches Projekt in Zürich auf eine ganz eigene Wohnungslösung. Auf dem sogenannten Kalkbreite-Areal der schweizerischen Stadt entstand in den vergangenen Jahren eine Wohngenossenschaft mit 256 Bewohnern. Um einen großzügigen Hof stehen hier mehrere vierstöckige Neubauten, in denen sich Groß-WGs, Familien- und Clusterwohnungen befinden. Letztere sind kleinste Apartments mit Kochnische und Bad. Erbaut wurde der Komplex nach dem Minergie-Eco-Standard. Auf den Dächern stehen Fotovoltaik-Anlagen, statt mit Autos bewegen sich die Bewohner ausschließlich mit dem Velo. Der Kalkbreite-Genossenschaft ist der ökologische Aspekt ihres Projekts wichtig. Wer ein Auto besitzt, kann nicht Teil dieser Gemeinschaft werden. Wer hier lebt, hat im Schnitt 32 Quadratmeter private Wohnfläche zur Verfügung. Etwa 800 Quadratmeter sind dagegen für Gemeinschaftsräume reserviert, wie etwa Meditationsräume, Näh- und Bügelzimmer, eine Sauna und ein Fitnessraum. Eine eigens geschaffene Vermietungskommission wacht darüber, dass die soziale Mischung in der Kalkbreite gewahrt wird. Junge Studenten leben hier neben einkommensschwachen Arbeitern oder einer eritreischen Familie. Ein interner Solidaritätsfonds federt Einkommensunterschiede ab und übernimmt in manchem Fall einen Teil der Miete.

nebenan.de ist eine Digitalplattform für organisiertes nachbarschaftliches Miteinander. Hier kann man Informationen austauschen, Veranstaltungen organisieren, Dinge leihen und verkaufen, Gruppen für gemeinsame Hobbys bilden und so auch zwischenmenschliche Nähe herstellen.

Der Hammerhof in der Nähe von Nürnberg beherbergt kreatives Unternehmertum rund um ein altes Gasthaus. Als „Zuhause für Gesellschaftsgestalter".

Stadt, Land, Flow.
Coworking Spaces haben Konjunktur. In der Stadt schon länger, auf dem Land immer mehr. Einen kleinen Ballungsraum bildet der Hohe Fläming südwestlich von Berlin. Im „COCONAT" in einem ehemaligen Gutshaus mieten sich Coworker oder auch Teams von Großunternehmen ein paar Tage ein, um allein oder zusammen naturnah zu arbeiten. Das geplante „KoDorf" geht noch weiter. Hier entstehen kleinere Wohnhäuser und großzügige Gemeinschaftsflächen für Büros, Werkstätten, eine Dorfschenke, Yoga-Räume, vielleicht ein Kindergarten. Die Baugruppe entscheidet das gemeinsam.

17.000 Quadratmeter Idylle.
Am Zernsee in Brandenburg hat sich die Genossenschaft Uferwerk gegründet, um ihren Mitgliedern ein nachhaltiges Wohnen zu ermöglichen. Auf einem 17.000 Quadratmeter großen ehemaligen Fabrikareal leben über 160 Menschen unterschiedlicher Generationen zusammen. Es gibt Singleapartments, WGs und Familienwohnungen. Gemeinsam setzen die Bewohner auf ökologische Stromerzeugung, Bio-Lebensmittel von Landwirten aus der unmittelbaren Umgebung und aufs Teilen, etwa von Monatskarten für Bus und Bahn oder mittels Carsharing. In einem Sammelraum stellen die Mitglieder Sachen ab, die sie nicht mehr brauchen: Bücher, Kindersitze, Drucker, Fernseher, Kleidung, Fahrräder … Jeder kann sich hier nehmen, was er braucht. Oft frühstücken die Genossen zusammen, gemeinsam pflegt man den Garten, organisiert Feste am Ufer oder macht in großen Gruppen Yoga. Das Ganze wirkt wie eine einzige Idylle. Und falls es doch mal Streit gibt, kommt das eigens etablierte Moderatorenteam zum Einsatz und schlichtet.

Gemeinschaftsgärten zur Erbauung und Selbstversorgung wachsen überall. Hier Urban Gardening am Münchener Ackermannbogen.

Generationsverträge.
Die bayrische „Solidaris" ist eine gemeinnützige Einrichtung, die Senioren und Studierende zusammenbringt. Dazu bietet sie unter anderem das „Dialog-Stipendium" an. Wer sich mindestens 40 Stunden pro Semester der Betreuung von Senioren widmet, bekommt dafür 500 Euro. Das lohnt sich vor allem ideell und verbindet die Lebenswelten von Alt und Jung. Beim Projekt „Wohnen für Hilfe" leben die Generationen unter einem Dach. Wer im Alter Platz hat und Gesellschaft sucht, überlässt Studierenden ein WG-Zimmer – für kein Geld. Als Gegenleistung zählt Unterstützung im Alltag – je Quadratmeter Wohnfläche eine Stunde im Monat. Das in Kiel gestartete Modell ist inzwischen in mehr als dreißig deutschen Städten etabliert.

Das Solidarprinzip.
Sicherheit in Verbundenheit bieten auch Solidarsysteme wie Arbeitslosen-, Renten- und Krankenversicherungen. Das bedingungslose Grundeinkommen ist ein aktuell diskutiertes weitreichenderes Konzept. Aber auch politische und militärische Bündnisse wie EU und NATO sind dem Solidarprinzip verpflichtet.

Wer Gemeinsamkeit sucht, wird an vielen Orten fündig. Dabei kann es umso interessanter sein, im ganz Anderen Verbindungen zu entdecken, die das eigene Leben überraschend bereichern.

Überreligional: House of One.
In Berlin bauen Juden, Christen und Muslime ein gemeinsames Haus. Unter seinem Dach sollen eine Synagoge, eine Kirche und eine Moschee entstehen. Hier können sich Menschen der unterschiedlichen Religionen begegnen, besser kennen und verstehen lernen. Das „House of One" hat seinen Platz in bester Lage der Hauptstadt zwischen Alexanderplatz und Museumsinsel. Der Standort sorgt also schon mal für Sichtbarkeit des überkonfessionellen Miteinanders. So könnte die Gemeinschaft der Religionen Symbolkraft und Vorbildcharakter entwickeln.

Das Mehrreligionenhaus ist noch im Werden. Es soll von Grund auf mit traditionellen Ziegeln gemauert werden.

DIE WELT VERDREHER

Ist das wahr? Kann das sein? Was stimmt hier – nicht? Im digitalen Kosmos schwirren jede Menge Halbwahrheiten und Lügen umher. Manche sind offensichtlich, viele dumm (aber trotzdem massenhaft verbreitet), nicht wenige aber auch immer raffinierter. Fake News sorgen für eine allgemeine Verunsicherung. Unser Vertrauen, auch in vermeintliche Fakten, wird von Zweifel und Misstrauen unterminiert – sofern wir nicht leichtgläubig übernehmen, was uns in den Kram passt. Denn unser Gehirn ist auf Bestätigung aus, schon weil das einfacher zu verarbeiten ist. Aber das ist häufig zu einfach.

Wie kann man dem persönlich begegnen? „Think twice" ist die oberste Devise. Also umschalten vom automatischen Reaktionsmodus auf kritisches Hinterfragen. Das ist sicher mühsamer und setzt außerdem guten Willen voraus, mögliche Fehlinformationen nicht weiterzuverbreiten. Denn natürlich sind Fake News interessengeleitet. Es soll ja manipuliert werden – im Zweifel im Sinne der eigenen Sache. Die Folgen erleben wir als gravierend. Auf persönlicher Ebene etwa durch Mobbing. Die Dreistigkeit, mit der dabei auch unverkennbare Realitäten umgekehrt als Fakes bezeichnet werden, ist erschütternd. Unsere Grundlagen für Glaubwürdigkeit sind einem multiplen Beben ausgesetzt, auf dem schiefe Weltbilder fußen. Das geradezurücken, ist eine Gemeinschaftsaufgabe der Zivilgesellschaft, von Medien und sozialen Netzwerken, von Organisationen und auch von Unternehmen. Letztere schon deshalb, weil sie sich darauf einstellen sollten, selbst Ziel von Desinformationskampagnen zu werden. Um das Image zu schädigen, die Marktstellung zu schwächen, den Aktienkurs zu manipulieren, Unruhe bei den Mitarbeitern zu stiften – wir werden es wohl oder übel erleben. Zeit also, sich darüber Gedanken zu machen, wie man damit am besten umgeht.

Unternehmen organisieren ihre Kommunikation zunehmend in modernen Newsrooms. Hier laufen, wie in den Redaktionen von Medienhäusern, alle Fäden zusammen. In erster Linie mit dem Ziel, unternehmensrelevante Informationen und Botschaften in den verschiedensten Formaten und auf den geeigneten Kanälen koordiniert auszuspielen. Der Newsroom ist vor allem Sender. Zukünftig wird auch die Empfängerfunktion eine größere Rolle spielen. Früher hieß das „Presseclippings" – die gesammelte Berichterstattung über das Unternehmen in zumeist gedruckten Medien. Heute geht es um Echtzeitbeobachtung aller wichtigen Kommunikationsplattformen, insbesondere von

Social Media. Und das nicht nur nebenbei. Es braucht aufmerksame Analysten, Bewertungssysteme, definierte Handlungsoptionen und Reaktionsketten – die ganze Klaviatur professioneller Medienbeobachtung. Unterstützung kommt dabei von künstlicher Intelligenz. Selbstlernende Systeme sollen immer besser helfen, zumindest Auffälligkeiten zu identifizieren. Endgültige Bewertungen und das Lesen zwischen den Zeilen bleiben aber bis auf Weiteres selbstdenkenden Menschen vorbehalten.

Automatismen und Roboter kommen auf allen Seiten verstärkt zum Einsatz. Social Bots verbreiten Informationen effizient in hoher Frequenz und präzise auf gewünschte Zielgruppen zugeschnitten. Sie von menschlichen Absendern zu unterscheiden, erfordert auch wieder eine spezifische Expertise. So entwickelt sich ein hybrides Gemenge von Menschen und Maschinen, die gemeinsam und gegeneinander, kreuz und quer um die Deutungshoheit vor allem im Netz kämpfen. Da müssen wir durch. Mit kühlem Kopf, aktiv und planvoll.

Lügen haben kurze Beine, sagt man. Aber sie verbreiten sich digital vernetzt und automatisiert rasend schnell. Sie einzufangen und richtigzustellen, ist zu einer bleibenden Herausforderung geworden.

Beispielhafte Falschspieler.

Big Business Fake.
Sie war der Traum des Silicon Valley: Elizabeth Holmes. Eine schöne junge Frau, intelligent und charismatisch. Sie brach ihr Studium an der Eliteuni Stanford ab, um ihr Unternehmen „Theranos" mit einer solch revolutionären Idee zu gründen, die sogar Steve Jobs in den Schatten gestellt hätte. Holmes versprach, mithilfe eines Blutentnahmestifts, den man kurz in den Finger sticht, eine Blutanalyse zu ermöglichen, die schnell und schmerzfrei sein sollte. Über 70 verschiedene Tests sollten möglich sein mit nur wenigen Tropfen Blut. Bakterien wie Viren würden schneller erkannt, als ein Arzt eine Spritze aufziehen könne. Eines Tages könnten Patienten den Test selbst durchführen und die Ergebnisse einfach hochladen, um sie von einem Arzt bewerten zu lassen.

Es gibt Aufnahmen, da sieht man Elizabeth Holmes neben dem Expräsidenten Bill Clinton auf einem Podium sitzen. Clinton präsentiert Holmes als Wunderkind. „Sag, wie alt du warst, als du dein Unternehmen gegründet hast!" Holmes antwortet scheinbar verlegen: „Ich war 19 Jahre alt." Beifall brandet auf. Viele sind beeindruckt von der Unternehmerin. So übernahmen unter anderem die Exaußenminister der USA George Schultz und Henry Kissinger im Unternehmen Aufsichtsratsposten. Börsengiganten investierten hunderte von Millionen US-Dollar in Theranos. Darunter Medienmogul Rupert Murdoch und Wall-Street-Legende Warren Buffet. Zeitweise überstieg Theranos Börsenwert die Marke von fünf Milliarden Dollar. Allein, es war alles eine gigantische Lüge. Denn nichts von dem, was Holmes versprach, stimmte auch nur ansatzweise. Sie log einfach und baute auf die Hoffnungen und Erwartungen der Menschen.

Roboter mit zwei Gesichtern.
Social Bots machen sich als digitale Helfer nützlich, um Serviceleistungen zu automatisieren und zu verbessern. Sie können aber auch als leistungsfähige Manipulationsmaschinen agieren. Denn die Roboter verbreiten bestimmte Inhalte gleich massenhaft und können die Wahrnehmung der Öffentlichkeit oder eines bestimmten Teils davon maßgeblich prägen. So stellte 2017 die Oxford University in einer Studie fest, dass der Kurznachrichtendienst Twitter während des US-Wahlkampfs millionenfach mit Falschnachrichten und Verschwörungstheorien geflutet wurde. Die Forscher befanden, dass die Fake News massenhaft von Bots geteilt wurden, die von russischen Servern oder von unseriösen Nachrichtenseiten stammten. Ebenso musste Facebook einräumen, als Plattform für Manipulation genutzt worden zu sein.

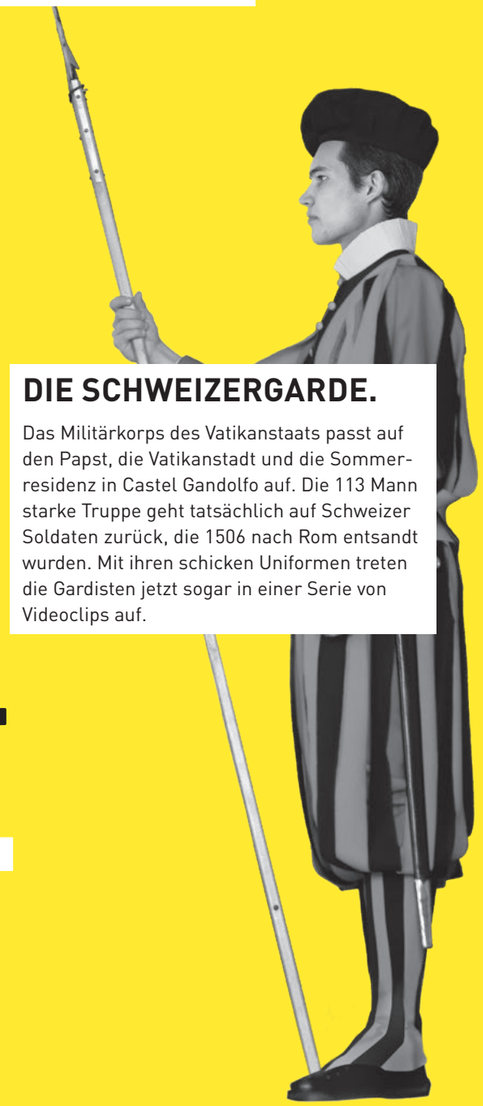
Social Bots sind nicht die erste und nicht die letzte Erfindung mit zweischneidigen Ausprägungen. Es kommt darauf an, ob man damit Gutes oder Schlechtes bewirken will. Zukünftig werden beide Seiten verstärkt von den virtuellen Meinungsmachern vertreten. Umso mehr bleiben menschliche Stimmen gefragt, humanistischen Perspektiven gebührend Gehör zu verschaffen.

DIE SOUNDDESIGNER.

Neue Technologien erweitern die Anwendungsfelder der kreativen Arbeit mit Klängen und Geräuschen. Heute umfasst die Arbeit des Sounddesigners nicht nur die klassischen Bereiche wie Film oder Theater, sondern auch Computerspiele oder Soundscapes, die an den verschiedensten Orten für die akustische Atmosphäre sorgen. Sicherheitsrelevant ist die Tongestaltung etwa in der Automobilindustrie. Hier wird nicht mehr nur der Sound zuklappender Türen designt, sondern auch die Tonpalette für eigentlich geräuschlos fahrende Elektroautos komponiert. Elon Musk hat ja jetzt auch sprechende Autos angekündigt. Egal, in welcher Stimmlage: Hauptsache nicht mit dem Vokabular vieler Autofahrer.

DIE ORDNER.

Sie sind die wahren Helden im Fußballstadion. Maximal nervenstark müssen die Ordner 90 Minuten (oder auch länger) mit dem Rücken zum Spiel stehen. Anstatt Tore zu sehen, heißt das: die Fans im Auge behalten, die vielleicht Bengalos zünden und Schmährufe abfeuern. Aber manchmal rollt auch „La Ola" durchs Oval. Und dann ist die Welt in Ordnung.



DIE SCHWEIZERGARDE.

Das Militärkorps des Vatikanstaats passt auf den Papst, die Vatikanstadt und die Sommerresidenz in Castel Gandolfo auf. Die 113 Mann starke Truppe geht tatsächlich auf Schweizer Soldaten zurück, die 1506 nach Rom entsandt wurden. Mit ihren schicken Uniformen treten die Gardisten jetzt sogar in einer Serie von Videoclips auf.

SECURITY @ WORK.

DER FLUGKAPITÄN.

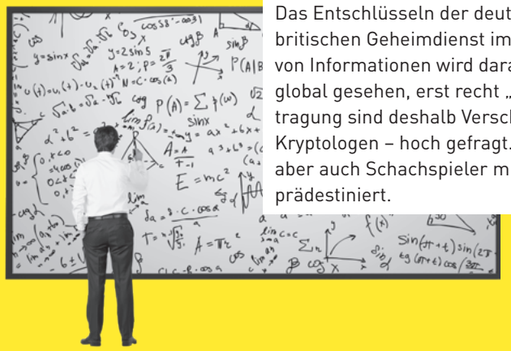
Manfred Müller ist Flugkapitän und Leiter der Flugsicherheitsforschung der Deutschen Lufthansa. Er hat erforscht, dass die wichtigsten Sicherheitsfaktoren bei aller Flugzeugtechnik menschlicher Natur sind: Disziplin, Engagement, soziale Kompetenz, Kooperation – kurz DESK, wie das programmatisch benannt ist. Kann man auch außerhalb des Cockpits gut gebrauchen.

DAS KONTROLLWESEN.

Spätestens bei der nächsten großen Rückrufaktion oder wenn in der Tagesschau vor Fremdkörpern in bestimmten Lebensmitteln gewarnt wird, merkt man wieder: Viele Dinge werden gründlich unter die Lupe genommen. Das gibt uns die Sicherheit, dass in Ordnung ist, was nicht beanstandet wird. Deshalb danke an alle, die ihre Prüfstempel wohlüberlegt aufdrücken.

DER BLINDENHUND.

Vor rund hundert Jahren trat der erste ausgebildete Blindenführhund seinen Dienst an. Heute begleiten in Deutschland geschätzte 3.000 Blindenhunde sehbehinderte Menschen durch den Alltag. Dafür bedarf es einer umfassenden Ausbildung schon im Welpenalter. Sehbehinderte lernen ihrerseits unter anderem 40 Signale, um dem Hund ihre Absichten mitzuteilen und mit seiner Hilfe sicher ans Ziel zu gelangen. So steht der beste Freund den Menschen treu zur Seite. Und wer so viel leistet, darf sich auch mal selbst belohnen. Wie der Helfer auf vier Pfoten, der sein Frauchen immer wieder zum Leckerli-Fachgeschäft führt.



DIE KRYPTOGRAFEN.

Das Entschlüsseln der deutschen Chiffriermaschine Enigma durch den britischen Geheimdienst im Zweiten Weltkrieg ist legendär. Die Macht von Informationen wird daran besonders deutlich. Heute sind Daten, global gesehen, erst recht „kriegsentscheidend". Für ihre sichere Übertragung sind deshalb Verschlüsselungsexperten – Kryptografen oder Kryptologen – hoch gefragt. Beste Berufsaussichten für Mathematiker, aber auch Schachspieler mit ihrer Fähigkeit zur Mustererkennung sind prädestiniert.

Herausgeber
Bechtle AG
Bechtle Platz 1, 74172 Neckarsulm
Tel. +49 7132 981-0
bechtle.com
zukunftsstark@bechtle.com

Konzept, Redaktion, Text, Gestaltung
waf.berlin

Illustrationen
Klappen vorn/hinten, S. 12–13, S. 26–29:
waf.berlin

Bildrechte
Umschlag Illustration Hoodie/Flamme: Noma Bar; S. 4–7 Eier und Federmesser: Sarah Illenberger; S. 18–21 Zahleninstallation: Emmanuelle Moureaux (Design), Daisuke Shima (Foto); S. 22–25 Fahrradhelm: Trek, Tonträger WaveCel.; S. 30–33 Sturmwolken: Xuanyu Han/gettyimages; S. 34/35 Kriminaltechniker: Monty Rakusen/gettyimages; S. 38–41 Dynamische Streifen: aaaaimages/gettyimages; S. 42–45 Fluid Trends colourful background: oxygen/gettyimages; S. 48 Kolkrabe: Vicki Jauron, Babylon and Beyond Photography/gettyimages; S. 49 Blauer Pfauenhahn: Stephan Mentzner/mauritius images; S. 50 Silberfasan: Marianne Purdie/gettyimages; S. 51 Flamingofedern: Alicia Bock/stocksy; S. 52 indonesischer Argusfasan: Sebastian Frölich/mauritius images; S. 53 Wilder Truthahn: Daniela Duncan/gettyimages; S. 54 Nest mit Eiern: malerapaso/istock; Sonnenschirm: s-cphoto/istock; Lippenstift: PLAINVIEW/istock; S. 55 Notrufsäule: ollo/istock; Fingerhut: PhotographyFirm/istock; Alu-Hut: Adobestock; Bananen: TeamDAF/istock; S. 56/57 Familie beim Essen: Hinterhaus Productions/gettyimages; S. 58 Neckarbogen: stadtsiedlung/Reinraum GmbH; Uferwerk: Mirko Kubein; S. 59 Kalkbreite: Genossenschaft Kalkbreite, Volker Schopp; Chor: Maskot/gettyimages; S. 60 Hammerhof: Daniel Zenker/KU Büro für Umsetzung GmbH; Radlerin: Radeln ohne Alter e.V.; Ackermannbogen Gemeinschaftsgarten: Ackermannbogen e.V.; S. 61 Mehrreligionenhaus: House of One/Kuehn Malvezzi; S. 62 Megaphon: Noma Bar; S. 66 Kopfhörer: benimage/istock; Schweizergarde: Hermann Dobler/imageBROKER/mauritius images; S. 67 Sonnenbrille: istock; Lebensmittelkontrolleurin: SeventyFour/istock; Blindenhund: andresr/istock; Tafel mit kryptografischen Formeln: ismagilov/istock

Druck
DBM Druckhaus Berlin-Mitte GmbH, Berlin
Papier: „Circle Offset Premium White"; die Papierqualität „Circle Offset Premium White" ist mit dem Europäischen Umweltzeichen (Euroblume) ausgezeichnet: Zertifizierungs-Nr. SR/11/003

RECYCLED
Papier aus Recyclingmaterial
FSC® C013894
FSC www.fsc.org

Falls Sie ein weiteres Exemplar des Magazins wünschen, bekommen Sie hier ein neues: zukunftsstark@bechtle.com. Oder Sie laden das Magazin als PDF herunter:
bechtle.com/zukunftsstark

91%

der Cyberangriffe beginnen mit einer Phishing-Mail.[1]

61%

der Unternehmen haben keinen Krisenplan für einen Cyberangriff.[2]

41 % DER UNTERNEHMEN GLAUBEN, DASS IHRE DATEN SICHER SIND …

ABER **49 %** VERFÜGEN NICHT ÜBER DIE NOTWENDIGEN IT-SECURITY-SKILLS.

UND **59 %** DER UNTERNEHMEN SIND UNSICHER UND WISSEN NICHT, OB IHRE DATEN SICHER SIND.[3]

Das BSI verzeichnet im Durchschnitt fast **320.000 neue Schad-programme pro Tag.**

2019 wurden rund **114 Mio. neue Schadprogramme registriert.**

Insgesamt sind damit über **900 Mio. Malware-Varianten** im Umlauf.[4]

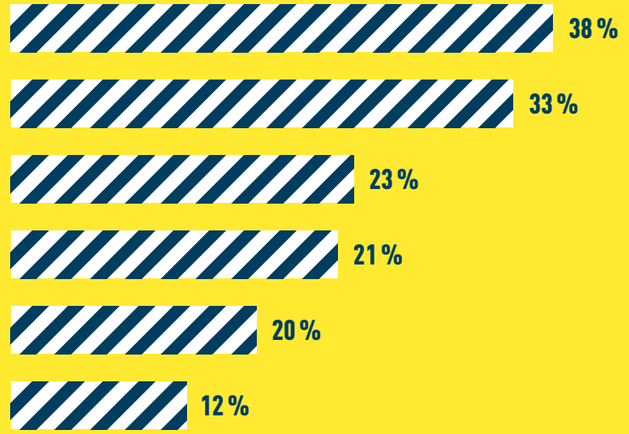
55 % weltweiter Unternehmen erlebten innerhalb von 12 Monaten einen oder mehrere Cyberangriffe.[5] In Deutschland sind es sogar **81 %** der Unternehmen.[6]

Das Bundeskriminalamt erfasste 2018

Fälle
von Cybercrime, geht aber von einer hohen Dunkelziffer aus.[4]

QUELLEN 1 cybersecurityventures.com | 2 willistowerswatson.com | 3 nttsecurity.com | 4 Bundesamt für Sicherheit in der Informationstechnik | 5 smallbiztrends.com | 6 Images Secure | 7 Bitkom Research / F-Secure

Von Unternehmen genannte Gefahrenquellen.[7]



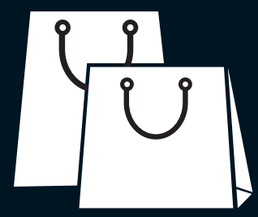
Aufdeckung krimineller Angriffe durch[7]

In deutschen Regierungsnetzen wurden 2019

ca. 770.000 Mails

mit Schad-programmen abgefangen.[4]

„Black Fridays“ und **„Cyber Mondays“** sind Spitzenzeiten für DDos*-Attacken.[4]



* Distributed Denial of Service

JÄHRLICHER GESAMTSCHADEN DER DEUTSCHEN WIRTSCHAFT DURCH SABOTAGE, DATENDIEBSTAHL, SPIONAGE – ANALOG UND DIGITAL.[7]


RESILIENZ
SICHERHEIT
VERBUND
ENHEITSO
CIALENGIN
ELERINGIT
FORENSIK
QUANTENTE
CHNOLOGIE
BLOCKCHAIN
bechtle.com
Ihr starker IT-Partner.
Heute und morgen.
BECHTLE