RADAR

CYBERSECURITY

WARUM SICHERHEIT MEHR ERFORDERT ALS TECHNOLOGIE

RADAR
#4

CYBERSECURITY

WARUM SICHERHEIT MEHR ERFORDERT ALS TECHNOLOGIE

2019
In Zusammenarbeit zwischen Allreal
und dem Think Tank W.I.R.E.

«DO YOU TRUST THIS COMPUTER?»

Diese Standardfrage stellen uns Smartphones heute, wenn sie mit einem bisher unbekannten Computer verbunden werden. Viele Nutzer mögen sich über diese Fragerei ärgern, doch die Frage unserer digitalen Helfer ist mehr als berechtigt. So wären die Betreiber des Romantik Hotels Jägerwirt in Österreich rückblickend wohl froh gewesen, sie hätten mit einem engagierten Nein geantwortet. Das Hotel hatte mit dem Ziel, zu den digitalen Vorreitern zu gehören, elektronische Türschlösser installiert. Als die Gäste eines Abends in ihre Zimmer zurück wollten, waren diese verriegelt. Der Grund dafür war eine Cyberattacke – gekoppelt an Lösegeldforderungen in Bitcoins.[1]

Der Fall des Hotels ist keine Ausnahme. Die Zahl von Cyberangriffen wächst mit besorgniserregender Geschwindigkeit. Jedes Unternehmen wird heute durchschnittlich 232-mal jährlich angegriffen, Tendenz stark steigend. Über 800 Millionen Schadprogramme sind heute im Umlauf.[2] In der Schweiz sind nach Schätzungen 40 % der Unternehmen betroffen.[3] Der damit ver-

bundene Verlust wurde vor mehreren Jahren allein in Deutschland auf 55 Milliarden Euro beziffert, die effektive Summe dürfte heute wesentlich höher sein. Je weiter die digitale Transformation voranschreitet und je mehr Prozesse von Organisationen durchdrungen werden, desto grösser wird die Gefahr. Natürlich sind nicht nur Unternehmen, sondern auch Private betroffen, zum Beispiel wenn persönliche Daten gestohlen werden oder wenn wir durch die zunehmende Vernetzung unseres Umfelds bald die Kontrolle über unsere Alltagsinfrastruktur verlieren. Fahrzeuge, die fremdgesteuert werden können, Türschlösser, die blockiert oder für nicht autorisierte Personen geöffnet werden: In einer vollständig vernetzten Welt – für viele Länder und Organisationen eine zentrale Zukunftsvision – wächst darum nicht nur die Chance für mehr Effizienz und Einfachheit, sondern auch die Gefahr von massiven Blackouts. Der Zusammenbruch kritischer Infrastruktur wie die Energie- oder Wasserversorgung, oder auch die Möglichkeit zur Manipulation von Wahlen, wie sie Geheimdienste in unzähligen Ländern vermuten: Je weiter das Internet und die digitalen Netzwerke unseren Alltag durchdringen, desto verletzlicher werden wir.

Angesichts dieser neuen Bedrohungslage hat die Sensibilisierung für Cyberrisiken in den letzten Jahren stark zugenommen und zu einem regelrechten Wett-

rüsten geführt. Die Angreifer haben dabei aber nach wie vor die besseren Karten. Die wachsende Komplexität der Systeme macht die Risiken unüberschaubar. Auch fehlt es – trotz der Allgegenwärtigkeit des Themas – vielerorts noch immer an mangelndem Bewusstsein, gerade auch in Führungspositionen. Ohne die aktive Aufmerksamkeit aller Mitarbeiter beim Anklicken von E-Mails haben clevere Phishing-Nachrichten leichtes Spiel und Malware infiziert innert Sekunden ein gesamtes Netzwerk. Doch selbst wenn es uns gelingt, alle unsere Alltagsaktivitäten zu kontrollieren: Die Vielfalt und Breite der möglichen Angriffspunkte nimmt laufend zu. Oftmals gelangen Angreifer nicht über das eigene System zu einem Unternehmen, sondern über das von Zulieferern oder Kunden.

Angesichts dieser Ausgangslage und mit Blick auf das hohe Tempo der digitalen Transformation müssen wir uns eingestehen, dass Cyberangriffe Teil unseres Alltags sein werden. Das Anstreben einer absoluten Sicherheit ist nicht realistisch. Dies bedeutet, dass wir Sicherheitsstrategien neu definieren und auf die künftigen Rahmenbedingungen ausrichten müssen. So ist der Versuch, allein mit technischen Hilfsmitteln alle Risiken zu eliminieren, nicht umsetzbar. Auch würden die dadurch entstehenden Einschränkungen noch mehr aufs Spiel setzten: einen weitgehenden Verlust von Freiheit und, daran gekoppelt, eine rückläufige Innova-

tionsfähigkeit. Bereits heute verhindern starre Copyright-Systeme von Soft- und Hardware, dass digitale Geräte verbessert werden können – zum Schutz vor Konkurrenten. Statt auf die Verhinderung von Angriffen zu fokussieren, müssen wir also die Handlungs- und Gestaltungfähigkeit von Menschen, Organisationen und Ländern stärken.

Damit dies trotz des allgegenwärtigen Gefühls der Bedrohung gelingt, müssen wir wieder lernen zu vertrauen. Die wachsende gesellschaftliche Verunsicherung führt auf Dauer zu kurzfristigem und vergangenheitsorientiertem Denken. Denn wenn man davon ausgeht, dass neue Geschäftsideen von Computern gestohlen werden, werden sie gar nicht erst entwickelt. Hier gilt es anzusetzen. Eine intelligente Sicherheitsstrategie umfasst mehrere Dimensionen und so gut wie alle Bereiche unseres Alltags. Sie liegt nicht, wie oftmals angenommen, in der alleinigen Verantwortung von IT-Experten. Was es braucht, ist eine kulturelle Transformation hin zu einem sinnvollen Umgang mit Risiken, die uns dazu bewegt, im Umfeld von hoher Dynamik und potenziellen Angriffen Neues zu wagen und – auf kalkulierbarer Basis – auch Risiken einzugehen. Dies erfordert nicht nur die Kenntnis der verschiedenen Cyberrisiken, sondern auch ein übergeordnetes Verständnis für die langfristigen wirtschaftlichen, gesellschaftlichen, technologischen und politischen Rah-

menbedingungen, die unsere Welt und unsere Wahrnehmung von Sicherheit prägen werden.

Vor diesem Hintergrund nähert sich diese RADAR-Publikation dem Spannungsfeld zwischen Sicherheit, Cyberrisiken und Vertrauen auf mehreren Ebenen an. Weshalb Sicherheit in einem globalen Kontext neu definiert werden muss und welche globalen Herausforderungen auf uns zukommen, zeigt das Interview mit Myriam Dunn Cavelty, Dozentin für Sicherheitspolitik am Center for Security Studies der ETH Zürich. Der kanadische Science-Fiction-Autor, Netzaktivist und Blogger Cory Doctorow erklärt im Gespräch, warum der einseitige Fokus auf den Schutz von digitalen Rechten die Verbesserung von Sicherheitstechnologien sogar beeinträchtigt. Der Cyber-Security-Experte Dr. Raphael M. Reischuk vom IT-Unternehmen Zühlke präsentiert konkrete Eckpunkte für den Aufbau einer nachhaltigen Sicherheitsstrategie. Und Dr. Stephan Sigrist, Gründer und Leiter des Think Tanks W.I.R.E., erläutert, warum der Umgang mit Cybersecurity einer neuen, intelligenten Risikokultur bedarf und wie wir dabei von den Strategien der Natur lernen können.

Viel Vergnügen bei der Lektüre! Und: Trauen Sie nicht jedem Computer!

Allreal & W.I.R.E.

1 https://www.wired.co.uk/article/austria-hotel-ransomware-true-doors-lock-hackers

2 https://www.handelsblatt.com/politik/deutschland/it-sicherheit-zahl-der-cyberangriffe-auf-unternehmen-und-regierung-gestiegen-seehofer-plaediert-fuer-aktive-cyberabwehr/23174732.html

3 https://www.nzz.ch/wirtschaft/cyberattacken-gehoeren-zum-geschaeftsalltag-ld.1450578

CYBERSECURITY

WARUM SICHERHEIT MEHR ERFORDERT ALS TECHNOLOGIE

14
VERTRAUEN STATT FIREWALL
Essay von Stephan Sigrist

32
DIE BEDROHUNG IM KOPF – WARUM WIR DIE SICHERHEIT NICHT EINZELNEN PERSONEN ÜBERLASSEN DÜRFEN
Interview mit Myriam Dunn Cavelty

46
EIN FUSSABDRUCK FÜR DATENSAMMLER
Interview mit Cory Doctorow

60
RAUS AUS DER BEQUEMLICHKEIT – ECKPFEILER FÜR EINE NACHHALTIGE CYBERSTRATEGIE
Beitrag von Raphael M. Reischuk

„Intelligenz ist nicht die Fähigkeit, Informationen zu speichern, sondern zu wissen, wo man sie findet.“

Albert Einstein
Deutscher Physiker (1879 –1955)

VERTRAUEN STATT FIREWALL

Essay von Stephan Sigrist

Die Vernetzung von Daten und Infrastruktur wird zur Voraussetzung für eine erfolgreiche digitale Wirtschaft und Gesellschaft. Doch die dadurch entstehende Komplexität der Systeme macht einen technischen Schutz vor Hackingattacken fast unmöglich. Investitionen in IT-Sicherheit werden wichtiger, reichen aber nicht aus. Um langfristig Freiheit und Innovationsfähigkeit zu erhalten, braucht es einen Wertewandel weg von einer Maximierung von Schutz hin zu einem intelligenten Umgang mit Risiken. Die zentrale Grundlage für die Gestaltung der Zukunft: eine Gesellschaft, die kritisch ist, aber auch den Mut besitzt, zu vertrauen.

Der Aufstieg des Internets ist durch eine Vielzahl von neuen Gestaltungsmöglichkeiten geprägt, die die Welt in den letzten 30 Jahren nachhaltig verändert haben. In den 1990er-Jahren brachte der freie Zugang zu weltweiten Informationen den ersten Durchbruch, gefolgt von der Aktivierung der Massen, die jeden einzelnen Menschen zum Sprachrohr machte und es erlaubte, eigene Inhalte zu verbreiten und diese einer globalen Gesellschaft zu präsentieren. Aktuell erweitert sich das Internet um eine weitere Dimension in die physische Realität, indem neben Computern immer mehr digitale Schnittstellen wie intelligente Kühlschränke, Fahrzeuge oder medizinische Geräte integriert werden.

BRAVE NEW OPEN WORLD

Die unterschiedlichen Nutzungs- und Anwendungsmöglichkeiten der digitalen Vernetzung prägen mittlerweile alle Bereiche unseres privaten und beruflichen Lebens von der Partnersuche bis zur Vermögensverwaltung oder der Instandhaltung von industriellen Maschinen. Es ist kaum mehr möglich, diese Vielfalt der Nutzungsmöglichkeiten in ihrer Gesamtheit zu erfassen. Dennoch gibt es eine grundlegende Gesetzmässigkeit, die das Wesen der Digitalisierung kennzeichnet: Es ist die Öffnung von abgeschlossenen Strukturen – in der Gesellschaft, der Wirtschaft, der Wissenschaft und der Politik. Dies ist die tatsächliche revolutionäre Triebkraft, die die Welt grundlegend verändert hat und es auch in Zukunft weiter tun wird. Zwar ist die Sturm-und-Drang-Zeit des jungen, wilden Internets, in der Musik in grossem Stil weltweit illegal verbreitet wurde und Zeitungen ihr Wissen kostenlos zu Verfügung stellten, in vielen Sektoren vorbei. An ihre Stelle traten Geschäftsmodelle, deren Convenience, gekoppelt an leistungsstarke Schutzsysteme, dazu geführt haben, dass Millionen von Menschen nicht mehr illegal herunterladen, sondern mit Plattformen wie Spotify oder Netflix streamen. Doch losgelöst davon führt die fortschreitende, globale Vernetzung von Menschen, Objekten und Infrastruktur zu einer

nicht aufhaltbaren Öffnung von technischen und sozialen Systemen.

AUF DEM WEG ZUR TOTALEN VERNETZUNG

Der Grund dafür liegt nicht nur in einem evolutionär definierten Verständnis von Fortschritt, wodurch die menschliche Natur nach Grösserem strebt, beispielsweise indem sich kleinere Einheiten zu Strukturen zusammenschliessen, vergleichbar mit dem Zusammenschluss von Zellen zu Mikroorganismen und letztlich zu Flora und Fauna. Er liegt auch in der simplen betriebswirtschaftlichen Maxime des kontinuierlichen Wachstums, das – in der digitalen Wirtschaft mehr denn je – die Skalierung von Prozessen und das Erschliessen von neuen und grösseren Märkten erfordert. Die zentrale Voraussetzung dazu ist eine konstante Erweiterung der Netzwerke mit dem Aufbau von Schnittstellen zu neuen Ökosystemen als Grundinfrastruktur von Wirtschaft und Gesellschaft. Aktuell werden in allen Sektoren – von Banken bis zur Medizin – spezifische Lösungsansätze entwickelt, die einzelne Bereiche einer Wertschöpfungskette digitalisieren: zum Beispiel die Möglichkeit, Zahlungen durch Smartphones zu steuern oder den Gesundheitszustand von chronisch kranken Menschen zu überwachen. So spannend und clever

die einzelnen Konzepte sind, in der grossen Mehrheit werden sie nur dann einen echten Nutzen stiften, wenn sie in eine grössere Struktur eingebunden sind. Allein sind die neuen Tools mehrheitlich irrelevant. Doch mit der daraus resultierenden Anzahl neuer Verknüpfungen wächst nicht nur das Potenzial für Innovation, sondern auch die damit verbundene Komplexität, die in ihrer Gesamtheit in einem globalen Kontext kaum noch überschaubar sein wird.

DAS ENDE DER SICHERHEIT

Als Folge dieser schnell fortschreitenden Vernetzung, die auf der Öffnung von bestehenden Strukturen beruht, zeichnet sich als Kehrseite der Medaille von Wachstum und Effizienz ein wachsendes Sicherheitsrisiko ab, da die Eintrittspforten für Angriffe zahlreicher und durch die höhere Komplexität kaum kontrollierbar sein werden. Die Folge: Cyberrisiken, wie sie schon heute durch Datendiebstahl oder das Hacken von digitaler Infrastruktur bestehen, werden in absehbarer Zukunft weiter zunehmen – mit derselben exponentiellen Dynamik, wie sich die neuen Netzwerke verbreiten. Mit Blick auf das Ziel, Milliarden von Wohnungen, Büros, Fahrzeugen, Brieftaschen und Herzschrittmachern digital zu steuern und zu vernetzten, zeichnet sich eine

düstere Prognose ab: Die Vorstellung von Sicherheit im digitalen Raum muss grundlegend revidiert werden, sprich, sie kann nicht garantiert werden. Der Mechanismus dahinter ist einfach: Wenn in einem Gebäude mehr Türen eingebaut werden, um mehr Besucher zu empfangen, steigt die Wahrscheinlichkeit, dass das Gebäude auch von unbefugten Personen betreten wird. Grosse Datenleaks, aber auch Angriffe auf Spitäler, bei denen mit dem Shutdown von kritischen Systemen Geld erpresst wurde, haben zu einer wachsenden Sensibilisierung und höheren Investitionen in sichere technische Infrastruktur geführt. Zwar sind noch längst nicht alle Organisationen, öffentlich wie privat, auf einem ausreichenden Sicherheitsstandard, doch die Notwendigkeit, Schutzmechanismen aufzubauen, ist zweifelsohne erkannt. Der Investor Warren Buffett bezeichnete Cyberattacken gar als eine der «grössten Bedrohungen für die Menschheit».[1] Diese Einschätzung ist insbesondere dann nachvollziehbar, wenn der Zusammenbruch von kritischer Infrastruktur der Energie- oder Wasserversorgung oder von Mobilitätssystemen zu einer realen Gefahr wird. Dass als Reaktion darauf ein Aufrüsten von Sicherheitstechnologie gefordert wird, ist nur logisch. Es ist von Megatrends die Rede; Banken setzen Fonds mit entsprechenden Themenschwerpunkten auf und IT-Unternehmen rüsten mit neuen Lösungsansätzen auf.

Das Problem liegt allerdings darin, dass technische Lösungen allein nicht ausreichend sein werden, weil sie angesichts der wachsenden Komplexität der Systeme keinen 100 %igen Schutz bieten können. Zwar wurde die Blockchain aufgrund der dezentralen, parallelen Speicherung von Daten auf unzähligen Rechnern lange als absolut sichere Grundlage gefeiert. Heute gehen Wissenschaftler jedoch davon aus, dass auch hier keine lückenlose Sicherheit mehr besteht, wenn sich Quantencomputer mit einer wesentlich höheren Rechenleistung künftig durchsetzen sollten.[2] So beunruhigend diese Entwicklung ist, sie ist mit einem kritischen Blick auf die Geschichte und die heutige Realität nicht neu. Eine absolute Sicherheit gab es nie. Nur haben wir heute – obwohl wir sicherer sind als je zuvor in der Menschheitsgeschichte – die Toleranz gegenüber von Risiken massgeblich verloren.

ILLUSION EINER KONSTANTEN STABILITÄT

Der wachsende Anspruch an die Sicherheit in der Wohlstandsgesellschaft hat in den letzten Jahren paradoxerweise zu einer zunehmenden Verunsicherung geführt. Die Finanzkrise der späten Nullerjahre kann als Wendepunkt verstanden werden, der den Übergang von den relativ stabilen wirtschaftlichen und politi-

schen Verhältnissen der Nachkriegszeit zu der viel zitierten VUCA-Welt[3] der Gegenwart markiert. Ausgelöst durch die Vertrauenskrise in Banken und politische Eliten, die anhaltenden Migrationsströme sowie den Ausblick auf den angekündigten Verlust von bis zu 60 % der heutigen Stellenprofile als Folge der Automatisierung hat sich eine weitreichende Verunsicherung breitgemacht. Diese hat in vielen Ländern zum Aufstieg von Populisten geführt, die in ihren Wahlversprechen – rund um den Brexit in Grossbritannien oder Donald Trumps «America First»-Politik – eine Rückkehr in die stabilen Verhältnisse der letzten Jahrzehnte versprechen, in Realität durch Abschottungsmassnahmen aber zu einer weiteren Destabilisierung der politischen und wirtschaftlichen Rahmenbedingungen beitragen. Entstanden ist ein Teufelskreis von einer wachsenden Sehnsucht nach Stabilität, wobei der Versuch, diese wiederherzustellen, die bestehenden tragenden Fundamente von Wirtschaft und Politik weiter aushöhlt und damit die Verunsicherung weiter nährt.

VON TRANSPARENZ ZU WERTEN

Der Aufbau einer nachhaltigen Sicherheitsstrategie erfordert vor diesem Hintergrund mehr als technische Massnahmen zur Abwehr von Cyberattacken. Wir müs-

sen unser Verständnis von Sicherheit neu definieren. Denn mit der Verstärkung traditioneller Schutzmechanismen werden auch die Kernwerte unserer Gesellschaft wie Freiheit und die Möglichkeit zur Weiterentwicklung massgeblich beeinflusst. Das Gefühl von Sicherheit, dieses Grundvertrauen in die eigene Umgebung, das Unternehmen, den Nachbarn, ist die notwendige Basis, auf der Menschen und Organisationen Neues wagen und dafür Risiken eingehen – die Voraussetzung für Innovation und gesellschaftlichen Zusammenhalt. Fehlt dieses Vertrauen, droht ein Verlust der Anpassungsfähigkeit an sich verändernde Umstände sowohl bei Individuen, Organisationen und Ländern.

Als Währung für dieses Vertrauen hat sich in den letzten Jahren die Transparenz durchgesetzt. Im Umfeld von hoher Komplexität und oftmals undurchsichtigen Marktbedingungen der digitalen Wirtschaft ist sie zweifelsohne notwendig, damit wir beispielsweise in ein Uber-Fahrzeug einsteigen oder online bei einem Menschen etwas kaufen, den wir nie zuvor gesehen haben. Die Transparenz über Bewertungen von anderen Nutzern greift hier vor und schafft die Voraussetzung für die Abwicklung eines Geschäfts. Nur: Präzise genommen ist Transparenz nicht die Grundlage für Vertrauen, sondern ihr Ersatz. Wer sich nur dann auf etwas Neues einlässt, wenn er zuvor die Gewissheit hat, dass

in der Vergangenheit vergleichbare Transaktionen erfolgreich durchgeführt wurden, vertraut nicht, sondern verlangt Fakten. Diese sind per Definition vergangenheitsorientiert. Wer allein auf Transparenz als Grundlage für Sicherheit setzt, kann nur historisch argumentieren und verliert die Basis für Schritte nach vorn, ins Unbekannte. Das verbindende Element, das Vertrauen ohne Fakten ermöglicht, sind Werte, die, wenn sie glaubwürdig gelebt werden, das Vertrauen schaffen, mit einer Organisation oder einem Menschen eine geschäftliche oder private Bindung einzugehen.

VON DER NATUR LERNEN

Im Kern einer zukunftsgerichteten Sicherheitsstrategie im Zeitalter der Cyberrisiken steht also nicht nur das Maximieren von Sicherheit, sondern auch die Fähigkeit, intelligent mit Risiken umzugehen. Dies heisst nicht, dass das Vermeiden von Angriffen kein zentraler Eckpfeiler bei der Festlegung der Handlungsfelder ist, sondern dass eine nachhaltige Sicherheitsstrategie auf mehreren Dimensionen erfolgen muss:

1. Stärken von Werten: Im Kern gilt es, sich der Verwundbarkeit bewusst zu werden und zu akzeptieren, dass Risiken und Unsicherheit der zwingende

Gegenpol von Wachstum und Lebensqualität sind. Wer keine neuen Gerichte kostet, isst für den Rest des Lebens dieselben Speisen, wer keine neuen Produkte entwickelt, wird keine neuen Märkte erobern, sondern nur die bestehenden bespielen. Handelszölle oder die Entkopplung vom Internet, wie es das russische Regime plant, bringen darum langfristig kaum einen Mehrwert. Das Fundament für den Umgang mit Unsicherheit bilden die grundsätzlichen Werte einer Organisation oder einer Nation, die für das nötige Vertrauen sorgen, das wir in einer dynamischen, digitalen Welt benötigen.

2. Digitale Netzwerke schützen: Der Aufbau und das kontinuierliche Pflegen von Cyberabwehrsystemen wird für Individuen genauso wie für Organisationen zur Normalität. Digitale Inhalte und Infrastruktur, die exponiert sind, erfordern adäquaten Schutz, der mit Investitionen verbunden ist. Hier sind Unternehmen wie Bürger gefordert. Die Wissenschaft und Innovatoren liefern die Grundlagen für neue Abwehrsysteme, die vernetzte Herzschrittmacher ebenso schützen können wie autonome Fahrzeuge oder elektronische Patientendossiers. Der Staat hat die Aufgabe, eine stabile und zukunftsgerichtete Infrastruktur aufzubauen. Der Nutzen dieser Tools und Lösungen wird aber insbesondere dann eintreten, wenn sie auf

die Verhaltensweisen im Alltag der Menschen ausgerichtet sind und von diesen auch verwendet werden.

3. Intelligent vernetzen: Mit der Akzeptanz, dass digitale Inhalte oder Strukturen grundsätzlich angreifbar sind, ergibt sich im Umkehrschluss die Frage, ob schützenswerte Inhalte oder Objekte nicht auch offline bleiben können. Denn nicht alles, was digitalisierbar ist, muss es auch werden. Dies erfordert eine differenzierte Entscheidung, welche Daten und welche Prozesse zwingend über digitale Systeme laufen müssen oder besser analog bleiben. Eine Grundlage dafür ist der Fokus auf den realen Mehrwert für Nutzer. Zu oft werden heute technische Lösungen als Selbstzweck etabliert.

   Intelligente Netzwerkstrukturen aufzubauen erfordert aber noch weitere Sicherheitsmassnahmen. Mit immer grösseren Netzwerken wächst auch die Notwendigkeit, an neuralgischen Stellen Unterbrüche zu installieren, die – vergleichbar mit einem Dominospiel – den Kollaps des Gesamtsystems verhindern, wenn ein Teilsystem nicht mehr funktioniert. Gleichzeitig gilt es auch restriktive Schutzprogramme bei Soft- oder Hardware zu limitieren, da diese durch die Beschränkung des freien Wettbewerbs die Verbesserung von Systemen behindern.

4. Schäden verhindern: Im grösseren Kontext dürften die wirkungsvollsten Massnahmen darin liegen, nicht erst Schadensbekämpfung zu betreiben, sondern das Eintreten von Risiken zu verhindern oder zu minimieren. Ein nachhaltiger Schutz vor Terrorismus wird nie durch Waffengewalt möglich sein, sondern nur durch das Auflösen von politische Spannungen. Diese Erkenntnis lässt sich zumindest teilweise auf Cyberrisiken übertragen, indem beispielsweise organisationsintern vernachlässigte oder unseriöse Mitarbeiter identifiziert und betreut werden. Studien belegen, dass bis zu 50 % der Angriffe durch Insider erfolgen.[4] In diesem Kontext entstehen für Versicherungen neue Geschäftsfelder, die Organisationen dabei unterstützen, Gefahren zu erkennen, bevor sie auftreten.

Ein abschliessender Blick über den Tellerrand der Sicherheitsdiskussion offenbart, dass sich solche mehrdimensionalen Sicherheitsstrategien längst und über einen sehr langen Zeitraum erfolgreich etabliert haben. Der menschliche Organismus verfügt mit seinem Immunsystem über ein breites Repertoire an unterschiedlichen Lösungsansätzen, die von der Schutzmauer der Haut über T-Zellen-basierte Angriffssysteme bis hin zu Antikörpern bei einem Erstkontakt mit einem Risiko Präventivreaktionen auslösen, um bei einem späteren

Angriff bereit zu sein. Die Zusammensetzung dieser unterschiedlichen Massnahmen sollte bei Organisationen, ähnlich wie bei biologischen Organismen, auf der Ausrichtung auf die spezifische Umgebung beruhen. Hierzu braucht es sicherheitsorientierte Ökosysteme, bestehend aus mehreren Akteuren mit unterschiedlichen Kompetenzen wie Cyberabwehr und Krisenkommunikation sowie Strategen, die vorausschauend mögliche Bedrohungsszenarien identifizieren. Gerade letztere Kompetenz – die Antizipation – haben wir Menschen einem Organismus voraus. Und diese gilt es zu nutzen.

DR. STEPHAN SIGRIST ist Gründer und Leiter des Think Tank W.I.R.E. Er analysiert seit vielen Jahren interdisziplinär Entwicklungen in Wirtschaft, Wissenschaft und Gesellschaft und beschäftigt sich schwergewichtig mit den Folgen der Digitalisierung in den Life Sciences, Financial Services, Medien, Infrastruktur und Mobilität. Er ist Herausgeber der Buchreihe ABSTRAKT und Autor zahlreicher Publikationen sowie Keynote-Referent an internationalen Tagungen. Mit W.I.R.E. berät er Entscheidungsträger bei der Entwicklung von langfristigen Strategien, begleitet Innovationsprojekte und unterstützt Unternehmen bei der Neugestaltung von zukunftsorientierten Räumen für Mitarbeiter und den Austausch mit Kunden. Nach seinem Biochemie-Studium an der ETH Zürich und einer Dissertation am Collegium Helveticum war er in der medizinischen Forschung von Hoffman-La Roche tätig. Danach arbeitete er als Unternehmensberater bei Roland Berger Strategy Consultants und am Gottlieb Duttweiler Institute.

1 https://www.businessinsider.com/warren-buffett-cybersecurity-berkshire-hathaway-meeting-2017-5

2 https://www.nature.com/articles/d41586-018-07449-z

3 VUCA ist ein Akronym für die englischen Begriffe «volatility» (Volatilität,Unbeständigkeit), «uncertainty» (Unsicherheit), «complexity» (Komplexität) und «ambiguity» (Mehrdeutigkeit).

4 https://www.mckinsey.com/business-functions/risk/our-insights/insider-threat-the-human-element-of-cyberrisk

„Viren schaden nicht, Unwissenheit schon!“

Virenentwickler
Anonym

DIE BEDROHUNG IM KOPF – WARUM WIR DIE SICHERHEIT NICHT EINZELNEN PERSONEN ÜBERLASSEN DÜRFEN

Interview mit Myriam Dunn Cavelty

Die Sicherheit nimmt weltweit zu. Und doch fühlen wir uns immer unsicherer. Myriam Dunn Cavelty, stellvertretende Leiterin am Center for Security Studies der ETH Zürich, erklärt warum, kritisiert den einseitigen Sicherheitsdiskurs und plädiert für die Schaffung von interdisziplinären Centers of Trust zur Verbesserung der Cybersicherheit.

Wenn wir den Gesamtblick einnehmen: Wie gefährlich leben wir heute?

MYRIAM DUNN CAVELTY: Den Statistiken zufolge leben wir zumindest in der westlichen Welt so sicher wie noch nie. Die individuelle Wahrnehmung weicht jedoch oft von diesen Fakten ab und zahlreiche Bürger nehmen die Welt als unsicherer wahr als früher. Einer der Gründe für dieses Missverhältnis ist die globale Medienlandschaft und -berichterstattung, die die Wahrnehmung auf beängstigende Vorfälle wie Naturkatastrophen, Terrorismus usw. lenkt und wir uns dadurch auch von weit entfernt liegenden Ereignissen bedroht fühlen. Die Empfindung der Menschen und die realen Begebenheiten klaffen in der Folge immer weiter auseinander, mit Folgen für die Politik und Gesellschaft.

Welche Aufgaben ergeben sich daraus und welche Blind Spots übersehen wir?

Die zentralen Herausforderungen sind heute vor allem sozialer Natur: Unzufriedenheit durch ökonomische Ungleichheiten in der Welt führen zu einer neuen Welle radikaler Politik und allgemeiner sozialer Unruhe. Gegen diese Tendenz anzutreten, um mehr soziale Kohäsion bzw. eine demokratische Debattenkultur zu erreichen, ist eine der grossen Aufgaben der Zukunft. Eine weitere Herausforderung wird es sein, den Unsicherheitsdiskurs kritisch zu hinterfragen. Die heutige Diskussion ist durch viel Angstmache und eine hohe Sensibilität auf alle Arten von Bedrohungen geprägt. Das ist ein Problem: Wer setzt die Prioritäten? Das ist meiner Meinung nach der Blind Spot: Wir meinen zwar, objektiv Gefahren und Risiken zu kennen, denken aber zu wenig darüber nach, wie diese auf unsere Agenden kommen – und wie sie politisch ausgenutzt werden.

Wer wäre denn verantwortlich, einen solchen Diskurs zu leiten und welche Handlungsfelder ergeben sich daraus für Politik, Unternehmen und Individuen?

Im Zeitalter von Fake News traut niemand niemandem mehr, und schon gar nicht trauen wir der Politik – etwas überspitzt gesagt. Man müsste einen Prozess starten, um unterschiedliche Gruppen von Personen dazu zu bringen, über gesellschaftliche Zusammenschlüsse und Austauschformen gesellschaftliches Vertrauen zu

stabilisieren und auszubauen. Der Sicherheitsdiskurs sollte nicht an einzelnen Personen oder Institutionen, sondern gesellschaftsübergreifend stattfinden und als gemeinsame Aufgabe angesehen werden.

Welche Rolle spielt denn konkret die Cybersicherheit in Bezug auf die Sicherheitsthematik? Handelt es sich um eine Schlüsselherausforderung oder eher um einen Hype?

Cybersicherheit besitzt viele Aspekte eines Hypes, aber nicht nur. Die Schwierigkeit besteht darin, dass viele Seiten der Gefahr nicht einfach zu erkennen sind und es insbesondere in Bezug auf staatliche Aktionen und Intentionen in diesem Bereich eine grosse Unsicherheit gibt. Für die meisten Menschen sind kriminelle Betrüger die Hauptgefahr. Aus der Analyse der Vorfälle der vergangenen zehn Jahre ist allerdings bekannt, dass vor allem die Nachrichtendienste das grösste Schadenspotenzial haben. Das sind Einheiten, die geheim bleiben möchten und eine hohe Machtkonzentration haben. Wenn wir diese Tatsache mit dem Wissen respektive Unwissen im Bereich Cybersicherheit kombinieren, haben wir ein sehr einseitiges Bild der Bedrohungslage, das über Marktlogiken gespiesen wird. Denn Unternehmen, die uns über Cybersicherheit und -risiken informieren, haben mehrheitlich ein Eigeninteresse und wollen ihre Produkte verkaufen. Zahlreiche Vorfälle werden gar nie öffentlich bekannt oder be-

schrieben. Insbesondere Angriffe auf NGOs und zivile Organisationen werden zu wenig erfasst. Wir wissen deshalb nicht genau, wie gross die Gefahr ist und was wir wissen, ist nicht objektiv. Durch Zusammenschlüsse regionaler, wissenschaftlicher Institutionen, NGOs und Personen aus dem Technologiebereich in Form eines Labs oder Hubs könnten alternative Daten generiert und mehr Transparenz sowie eine globalere Sichtweise in die aktuell politisch gefärbten und einseitigen Informationen gebracht werden. Es finden diesbezüglich erste regionale Initiativen und Diskussionen zwischen verschiedenen Universtäten statt, die darauf abzielen, sogenannte Centers of Trust zu bilden.

Was wäre die konkrete Aufgabe eines solchen Center of Trust?

In den letzten Jahren wurden immer häufiger auf höchster Ebene Schuldzuschreibungen von Cybervorfällen gemacht, mit teilweise weitreichenden Konsequenzen. Das nennt man öffentliche Attribution. Auf der Basis der veröffentlichten Informationen sind die Schuldzuweisungen aber nicht überprüfbar. Diese mangelnde Transparenz ist ein Problem für die demokratische Willensbildung und insbesondere für die politische Legitimität der gewählten Gegenmassnahmen. Universitäten sind nicht die einzigen, denen eine wichtige Rolle in der Behebung dieses Problems zukommt, aber aufgrund ihres Forschungs- und Lehrauftrags können sie

eine wichtige vertrauensbildende Rolle übernehmen. Universitäten können interdisziplinäre und begutachtete und somit öffentliche und zugängliche Forschung zur Attributionsproblematik betreiben und zur Erforschung von digitalen Konflikten beitragen, indem sie eigenständige interdisziplinäre Expertise und eine eigene Datenbasis aufbauen.

Ist es mit der vollständigen digitalen Vernetzung denn überhaupt noch möglich, sich als Individuum oder Unternehmen sicher im Netz zu bewegen? Oder müssen wir uns von dieser Vorstellung verabschieden?

Um diese Frage zu beantworten, muss man zuerst definieren, was sicher heisst. Im IT-Bereich wird es nie eine 100 %ige Sicherheit geben. Diese gibt es aber nirgends im Leben. Wir leben in einer Welt von Risiken, in der wir aber häufig die Wahl haben, wie wir uns verhalten. Der Mensch entscheidet, ob er mehr oder weniger Risiko eingeht und fühlt sich sicherer, wenn er glaubt, sein eigenes Risiko beeinflussen zu können. In dieser Logik sehe ich auch die Zukunft des digitalen Verhaltens: Wir entscheiden, wem wir vertrauen – sei es in Bezug auf Technologie, Daten oder deren Nutzung. Bedingung hierfür ist aber, dass wir wissen, wohin unsere Daten gehen und wie diese genutzt werden. Wenn ich weiss, wem ich vertrauen kann und wem ich welche Daten zur Verfügung stelle, fühle ich mich sicherer. Ein weiterer

Aspekt liegt in der sogenannten Resilienz: Wenn ich weiss, dass es keine absolute Sicherheit gibt, bereite ich mich auf mögliche Vorfälle vor. Als Unternehmen habe ich beispielsweise meine Notfallpläne und Vorbereitungen im Fall eines Angriffs. Dies erhöht ebenfalls die Sicherheit – zumindest in der Bewältigung von Angriffen.

Welche Massnahmen sind dazu notwendig und welchen Stellenwert nehmen dabei Technologien wie die Blockchain oder biometrische Verschlüsselungen ein?

Ein wichtiger Anspruch an Sicherheitsmassnahmen ist, dass sie nicht zu kompliziert sein dürfen. Deshalb hat sich beispielsweise die Biometrie durchgesetzt: Wenn ich nur noch meinen Finger aufs Mobiltelefon halten muss, ist das die einfachere Lösung, als wenn ich mir ein langes und kompliziertes Passwort merken muss. Gleichzeitig gilt es zu bedenken, dass Sicherheit nicht statisch ist, sondern die Angreifer immer dort ansetzen, wo wir es nicht erwarten bzw. wo es Schwachstellen gibt. Zudem suggerieren Technologien wie die Blockchain dem Menschen mehr Sicherheit, obwohl dies nicht unbedingt der Fall bzw. kontextabhängig ist. Technologien werden von den Nutzern häufig als Objekte betrachtet, wir verstehen diese aber noch zu wenig als Netzwerke zwischen Maschinen und Menschen.

Wie beurteilen Sie Artificial Intelligence und Machine Learning in Bezug auf Cyberangriffe und -abwehr?

Die Neuroforschung, die versucht, Gehirnfunktionen zu modellieren oder untersucht, wie Signale ausgetauscht werden, liefert wertvolle Erkenntnisse, die auf den Austausch zwischen Computern übertragen werden können und damit im Cyberbereich Anwendung finden. Dabei muss man aber bedenken, dass Entwicklungen wie AI, Machine Learning oder Deep Learning für Gutes oder Schlechtes genutzt werden können. Künstliche Intelligenz wird heute schon für die Erkennung von Netzwerkanomalien eingesetzt – aber auch, um schneller in ein Computernetzwerk einzudringen oder Viren zu kreieren, die sich laufend verändern können, um ihr Ziel zu erreichen. Ob nun die Abwehr oder die Angreifer davon mehr profitieren werden, ist vollständig ungewiss. Cybersicherheit ist immer schon ein Bereich von extremem «dual use» gewesen. Digitale Technologien bringen immense Vorteile – und neue, potenziell katastrophale Risiken. Das wird auch in Zukunft nicht anders sein.

Welche Akteure sind Ihrer Meinung nach denn für die Cybersicherheit verantwortlich: der Staat oder Individuen und Unternehmer in ihrer Eigenverantwortung als Nutzer?

Das ist eine zentrale Frage der Cybersicherheitspolitik. Der Staat hat die Aufgabe, das internationale Umfeld so

sicher wie möglich zu gestalten. Dies wird in supranationalen Gremien wie der UNO, NATO usw. umgesetzt. Daneben gibt es den sogenannten Intel-Bereich, sprich Nachrichtendienste. Diese Ebene ist wie bereits erwähnt in Bezug auf Cybersicherheit schwer durchschaubar und von divergierenden Interessen geprägt. Der Staat wird sicherheitspolitisch nur aktiv, wenn die Cybervorfälle eine gewisse Dringlichkeit oder Grösse erreichen und wenn es sich um eine Krise nationalen Ausmasses handelt. Dies ist jedoch recht subjektiv und kontextabhängig. Ansonsten gilt, dass jedes Unternehmen selbst dafür zuständig ist, seine Netzwerke zu sichern. Dies klingt sehr simpel, ist es aber nicht. Gerade in der Schweiz fehlen bei den für das Land zentralen KMU die Ressourcen, aber auch teilweise die Anreize dazu. Das Problem ist, dass diese Unternehmen auf unglaublich wichtigen Daten sitzen. Da fehlt bis anhin eine Lösung respektive eine Regulierung. Wir befinden uns hier in einem extremen Spannungsfeld zwischen liberaler Wirtschaft und nationaler Sicherheit.

Unser Alltag ist technologisierter denn je und dadurch ist unsere Hackbarkeit zur Normalität geworden. Braucht es im Umgang mit Sicherheit eine neue Gelassenheit, sprich: Gewöhnen wir uns daran, dass wir auf allen Ebenen angreifbar sind?

Ich denke schon. Die Tatsache, dass wir unsichere Systeme nutzen, wird je länger, je mehr zur Normalität.

Wir leben damit und gewöhnen uns daran – wie wir uns beispielsweise an die verschiedenen Risiken im Verkehr gewöhnt haben. Meiner Meinung nach ist sogar eine Gegentendenz zum Hype feststellbar, denn wir leben je länger, je besser mit der eigentlichen Banalität dieses Risikos.

Wie sieht Ihrer Meinung nach die Zukunft unserer Privatsphäre aus: Gibt es sie überhaupt noch und wenn ja, was verstehen wir in zehn Jahren darunter?

Die Privatsphäre wird es immer geben, aber wir gewöhnen uns auch hier daran, dass sich das Verständnis davon und der Umgang mit ihr verändert. Wir werden einen bewussten Umgang mit Daten, die wir auf Social Media preisgeben, etablieren, wenn wir die Kontrolle und das Vertrauen darüber haben, dass die Daten, die privat sind, auch privat bleiben. Zudem werden Daten je länger, je mehr nicht mehr gratis zur Verfügung gestellt, sondern gezielt verkauft. Insbesondere im Gesundheitsbereich wird sich diese Entwicklung festmachen.

Wir sehen Vertrauen als wichtiger werdenden Wert, sozusagen als Schmiermittel von Technologien. Denn letztlich schafft es keine Technologie, absolute Sicherheit zu garantieren. Was halten Sie von dieser These?

Das ist ein höchst faszinierendes Thema – auch, weil wir es nicht so ganz verstehen. Insbesondere das Vertrauen, das über Technologien entsteht oder auch zerstört wird, ist noch zu wenig erforscht. Vertrauen ist ein ganz zentraler Wert für die digitale Zukunft. Das Thema müsste meiner Meinung nach diskursiv viel stärker aufgegriffen werden, zum Beispiel in den erwähnten gesellschaftlichen und universitären Zusammenschlüssen oder Round Tables.

DR. MYRIAM DUNN CAVELTY ist Dozentin für Sicherheitspolitik und stellvertretende Leiterin Forschung und Lehre am Center for Security Studies der ETH Zürich. Ihre Forschungsschwerpunkte beinhalten Cybersicherheit, internationale politische Soziologie von Risiko und Sicherheitspolitik. Sie hat an der Universität Zürich Internationale Beziehungen, Geschichte und Internationales Recht studiert. Neben Ihrer Lehr-, Forschungs- und Publikationstätigkeit berät Myriam Dunn Cavelty Regierungen, internationale Institutionen und Unternehmen im Bereich Cybersicherheit, Risikoanalysen und strategische Früherkennung.

„Wenn Sie mehr für Kaffee als für IT-Sicherheit ausgeben, werden Sie gehackt. Zudem verdienen Sie es dann, gehackt zu werden.“

Richard Clarke
US-amerikanischer Terrorexperte

1
2
ABC
3
DEF
4
GHI
5
JKL
6
MNO

EIN FUSSABDRUCK FÜR DATENSAMMLER

Interview mit Cory Doctorow

Bei der Verbesserung der Cybersicherheit geht es nicht nur darum, technologische Fehler auszumerzen, die uns angreifbar machen. Wir müssen auch die Praktiken ändern, die es zulassen, dass sich solche Schwachstellen auftun. Was wir brauchen, ist eine offene, unzensierte Diskussion über die Qualität von Sicherheitssystemen, die Berechnung der tatsächlichen Kosten von Datenlecks und eine ebenso hohe Haftung für Unternehmen und Personen, denen persönliche Daten anvertraut werden. Das unsachgemässe Horten von Daten muss unattraktiv werden.

Die Debatte um die Cybersicherheit ist allgegenwärtig; Menschen und Unternehmen haben ein grösseres Bewusstsein für die Risiken des digitalen Zeitalters entwickelt. Ist das Ihrer Meinung nach eine Überreaktion auf den schnellen Wandel?

CORY DOCTOROW: Im Gegenteil, wir müssen die Cybersicherheit viel ernster nehmen und die Diskussion dazu ausweiten. Bisher lag der Fokus ausschliesslich auf den technologischen Herausforderungen. Natürlich muss die Technologie optimiert werden, um die Sicherheit zu gewährleisten. Aber um dies zu erreichen, müssen wir erst die Politik ändern. In den letzten Jahren haben Fehlentscheide im Sicherheitsbereich dazu geführt, dass Unternehmen unverantwortlich gehandelt und die Verbesserung der Sicherheitssysteme behindert haben. Ein Beispiel: Unternehmen, die polizeiliche Leis-

tungen für Städte erbringen, wie zum Beispiel automatische Kennzeichenleser oder Gesichtserkennungsprogramme, verlangen von diesen Städten die Unterzeichnung einer Geheimhaltungsvereinbarung. Wenn die Systeme also schlecht funktionieren – zum Beispiel wenn die KI-Gesichtserkennung bei einer afroamerikanischen Person eher Falschmeldungen generiert als bei einer kaukasischen –, darf die Polizei es niemandem sagen. Infolgedessen vermehren sich solche Systeme, gewinnen neue Investoren, und es wird alles getan, um die fehlerhafte Technologie zu schützen. Diese strukturellen Barrieren müssen zusammen mit den tatsächlichen Sicherheitsmängeln der Produkte angegangen werden.

Knüpfen wir an Ihr Beispiel der Gesichtserkennung an: Ist dies nicht auch das Ergebnis einer Überschätzung der Leistung von künstlicher Intelligenz?

Hier gilt es, eine wichtige Unterscheidung zu machen. Die KI ist in der Tat überbewertet. Einerseits, weil viel Lobbyarbeit und Geld für Werbung investiert werden, und viele Menschen diesen Zukunftsversprechen glauben. Andererseits ist es wie gesagt so, dass die schlechte Qualität von KI-Produkten nur selten ans Tageslicht kommt. Wenn das einzige Problem darin bestünde, dass die KI nicht richtig funktioniert, müssten wir «nur» bessere Technologien entwickeln. Aber wenn Fehlfunk-

tionen durch Vertraulichkeitsvereinbarungen geschützt werden, können diese nicht ausgemerzt werden.

Unser Leben wird immer vernetzter; wir umgeben uns mit smarten Dingen wie Autos, Häuser oder Lautsprecher auf der Strasse, im Büro und in unserem Zuhause. Wie angreifbar macht uns das?

Unsere Privatsphäre steht auf dem Spiel. Wenn wir nichts unternehmen, haben wir bald keine Kontrolle mehr darüber, was von uns und unseren Aktivitäten öffentlich wird. Bereits heute können wir theoretisch von unseren Computern, Telefonen, Fernsehern, Autos und Häusern ausspioniert werden. Dies gilt es mit allen Mitteln zu verhindern. Aber auch hier haben wir es nicht «nur» mit technischen Fehlern zu tun, die einen Angriff auf unsere Privatsphäre ermöglichen, sondern mit Systemen, die solche mangelhaften Produkte schützen. Hersteller von IoT-Geräten dürfen in ihren Produkten digitale Sperren einsetzen, die die Macht ihrer Wettbewerber und Kritiker einschränken. Nach europäischem und US-Recht ist die Veröffentlichung von Informationen, die jemandem helfen oder ihn ermutigen könnten, eine solche digitale Sperre zu umgehen, ein Verbrechen, das mit einer Freiheitsstrafe von fünf Jahren angeklagt wird. Das bedeutet, dass es unmöglich ist, eine wahrheitsgetreue Kritik an einem technologischen System zu veröffentlichen, ohne rechtlich verfolgt zu werden. Im Jahr 2017 wurde

das World Wide Web Consortium (W3C), die internationale Organisation für Standards im World Wide Web, von grossen amerikanischen Entertainment-Unternehmen wie Netflix gebeten, das DRM (Digital Rights Management) für Browser zu standardisieren – um zu verhindern, dass Menschen Videos streamen. Zusammen mit der Electronic Frontier Foundation[1] wandte ich mich an W3C und bat sie, keine Menschen zu verklagen, die wahre Kommentare über fehlerhafte Systeme abgeben. Sie haben kategorisch abgelehnt!

Führt diese Haltung auf lange Sicht nicht zu unzufriedenen Kunden und einem Rückgang des Konsums?

Vielleicht. Da immer mehr Menschen von mangelhaften Sicherheitssystemen betroffen sein werden, wird sich eines Tages eine kritische Masse von Menschen der Risiken bewusst sein, denen sie durch IoT-Geräte ausgesetzt sind. Ich nenne dies den Moment der «peak indifference»: Ein Problem, das lange Zeit auf wenig Interesse gestossen war, wird plötzlich offensichtlich, und die Zahl derer, die sich betroffen fühlen, steigt automatisch an. Allerdings ist es dann oft zu spät: Je tiefer die fehlerhaften Systeme in unser Leben integriert sind, desto schwieriger ist es, sie durch andere, bessere zu ersetzen. In der Folge könnte der Nihilismus zum dominanten Motiv in der Sicherheitsdiskussion werden. Viele werden sagen: «Es ist zu spät, wir geben auf.»

Ähnlich verhält es sich mit dem Klimawandel: Wenn die Menschen die Tragweite des Problems verstehen, wird der weltweite Anstieg der Temperatur um zwei Grad nicht mehr zu stoppen sein. Es besteht eine reale Gefahr, dass die kritische Masse an Akteuren zu spät erreicht wird, um den Grossteil der Bevölkerung davon zu überzeugen, dass dies noch einen Unterschied machen kann – in der Cybersicherheit wie dem Klimawandel.

Ein hoffnungsloses Szenario. Wie können wir verhindern, dass dies geschieht?

Wir müssen jetzt mit dem Handeln beginnen. Erstens müssen wir aufhören, die Kritik an technologischen Schwachstellen und Fehlern zu zensieren. Ein einfacher Weg, um dorthin zu gelangen, wäre eine Änderung der Haftungsfrage: Unternehmen, die Massnahmen ergreifen, um Informationen über Produktfehler zu unterdrücken, sollten mit grösseren Beträgen haften als Unternehmen, die dies unterlassen. Zweitens müssen wir Haftungsregelungen schaffen, die die vollen Kosten von Datenlecks abdecken. Heute müssen Unternehmen bei Lecks nur für die unmittelbaren Kosten aufkommen, auch wenn später schwerwiegende Folgen für die Opfer entstehen können, wie das folgende Beispiel zeigt: Vor einigen Jahren hatten sich Kriminelle in New York und London die Offenlegung persönlicher Daten infolge mehrerer grosser Datenlecks zu einem späteren Zeit-

punkt zunutze gemacht, um damit Schlüssel zu duplizieren und den Menschen genau dann ihre Häuser auszurauben, als sie abwesend waren. Ein weiteres Beispiel ist das Leck des amerikanischen Heimwaren-Unternehmen Home Depot mit über 80 Millionen gestohlenen Kreditkartendaten. Die Strafe für das Unternehmen betrug pro Kunde rund 30 Cent für den Kartenersatz plus einen Gutschein für sechs Monate Kreditkartenüberwachungsdienst. In Zukunft sollte ein Unternehmen für mindestens einen halben Prozentsatz des gesamten Werts des Eigentums aller seiner Kunden haftbar gemacht werden. Wenn die Haftung genügend hoch angesetzt wird, werden die Unternehmen bei der Datenauswahl und der Art und Weise, wie sie mit diesen umgehen, vorsichtiger. Nicht zuletzt, weil Versicherungs- und Rückversicherungsunternehmen sich weigern würden, Policen für Unternehmen aufzusetzen, die zu viele PII (personalidentifizierbare Informationen) horten.

Das Ansammeln von personenbezogenen Daten soll bestraft werden: Wie hoch ist in Zukunft der Wert von Daten noch?

Die Leute behaupten, dass Daten das neue Öl sind, aber man könnte auch sagen, Daten sind die neue Verschmutzung. Wenn Sie eine Lackfabrik sind, müssen Sie sicherstellen, dass keine giftigen Stoffe in die Wasserversorgung gelangen. Wenn Sie scheitern, werden

Sie verklagt und die Gebühren, die Sie bezahlen müssen, lassen Sie alles tun, um dies zu verhindern, wie zum Beispiel die kontinuierliche Kontrolle des Systems und des Wassers auf Lecks hin. So sollte es auch mit Unternehmen und Daten sein: Sie müssen alles in ihrer Macht Stehende tun, um Lecks zu vermeiden und sofort handeln, wenn es dennoch dazu kommt. Wenn sie dies nicht erkennen und den Menschen schaden, wird ihr Unternehmen aufgelöst und das Geld an die Betroffenen verteilt werden. Eigentlich ganz einfach.

Und wie sieht es mit der Verantwortung der Mitarbeitenden aus?

Meiner Meinung nach müssten Entscheidungsträger, die für den Datenmissbrauch verantwortlich sind, persönlich haftbar gemacht werden – auch nach der Auflösung eines Unternehmens. Die Notwendigkeit einer persönlichen Haftung wird deutlich, wenn wir uns den Fall Cloudpets ansehen, ein Unternehmen, das mit dem Netz verbundene, flauschige Tiere verkauft hatte. Die Firma ging Konkurs und kurz davor wurden persönliche Daten wie E-Mail-Adressen und Passwörter, Profilbilder und Sprachaufzeichnungen von mehr als einer halben Million Kindern und Erwachsenen, die dieses Spielzeug benutzt hatten, gestohlen. Der Hersteller wurde im Vorfeld mehrfach von Datenschutzunternehmen darüber informiert, dass seine Kundendaten online für jedermann verfügbar waren und dennoch

blieben sie fast eine Woche lang im Netz – weil das Personal zu diesem Zeitpunkt noch aus einer einzigen Person bestand, einem Buchhalter, der sich mit der Liquidation beschäftigte. So wurde weder die Firma noch die ehemalige Geschäftsleitung haftbar gemacht. Ein grosser Fehler. Meiner Meinung nach sollten Menschen, die ihnen anvertraute Daten nicht schützen, wie Menschen behandelt werden, die stehlen.

Wie wird es uns in Zukunft gelingen, den Schutz der Privatsphäre zu verbessern und dabei gleichzeitig eine datenbasierte Wirtschaft aufzubauen?

Wir brauchen neue Gesetze und Ethiken für den Umgang mit Daten. Eine Möglichkeit wäre die Bildung von sogenannten Informationstreuhändern. Eine kurze Erklärung: Das Treuhandgesetz ergibt sich aus wirtschaftlichen Beziehungen, die auf asymmetrischer Macht beruhen, wie zum Beispiel Menschen, die ihre persönlichen Informationen an qualifizierte Fachleute wie Ärzte, Anwälte oder Buchhalter weitergeben. Als Gegenleistung für dieses Vertrauen schulden die Fachleute diesen Menschen eine Loyalitäts- und Sorgfaltspflicht, was bedeutet: Sie können die Informationen ihrer Kunden nicht gegen deren Interesse verwenden und sie müssen kompetent und gewissenhaft handeln, um Datenmissbrauch zu vermeiden.[2] Nun besteht die Idee darin, dass für Online-Unternehmen, die Kundendaten

erheben und monetarisieren, die gleichen treuhänderischen Regeln gelten sollten, da ebenfalls ein einseitiges Machtverhältnis besteht: Die Firmen können die Aktivitäten ihrer Nutzer rund um die Uhr überwachen, aber die Nutzer verfügen nicht über dieselbe Macht. Neue Gesetze würden solche Unternehmen als «Informationstreuhänder» kategorisieren. Auf diese Weise wären Unternehmen und Personen, die Kundendaten sammeln und verwalten, rechtlich und ethisch verpflichtet, das Interesse der Kunden respektive der Gesellschaft über ihr eigenes Interesse zu stellen.

Was raten Sie uns allen beim Umgang mit Cyberrisiken?

Wir müssen uns der Risiken bewusster werden und aufhören, mit unserer Privatsphäre so leichtfertig umzugehen. Eltern müssen sich beim Kauf von Spielzeug wie Cloudpets allfälliger Sicherheitsrisiken bewusst sein. Viele vertrauen blindlings dem Produkt, da sie glauben, dass die Investoren ihre Sorgfaltspflicht erfüllt hätten. In einer idealen Zukunft – frei von allen strukturellen Hindernissen für eine bessere Cybersicherheit und einer Anerkennung der tatsächlichen Kosten von Datenverletzungen – könnte dies der Fall sein, und wir könnten unseren Geräten vertrauen. Bis dahin ist aber mehr Vorsicht geboten. Dies lässt sich am besten erreichen, indem man beginnt, die eigene Privatsphäre höher zu bewerten. Wir müssen unseren Kindern bei-

bringen, nicht zu viele Informationen, zum Beispiel über Social Media, weiterzugeben. Und wir müssen ihnen zeigen, wie sie sich vor Überwachung und Ausspionieren schützen. Für uns Eltern sollte die logische Konsequenz sein, dass wir unsere Kinder auch nicht ausspionieren, indem wir ihre Mediennutzung überwachen oder mit Handy-Ortung nachsehen, wo sie sich gerade befinden.

CORY DOCTOROW ist ein kanadischer Science-Fiction-Autor, Aktivist und Journalist und Mitherausgeber des bekannten Weblogs Boing Boing (boingboing.net) sowie Autor zahlreicher Bücher, zuletzt RADICALIZED und WALKAWAY, Science-Fiction-Romane für Erwachsene. In London arbeitete Cory Doctorow als Koordinator für Europa-Angelegenheiten bei der Electronic Frontier Foundation (EFF) und wurde 2007 mit dem «EFF Pioneer Award» ausgezeichnet. 2005 hat er die Open Rights Group in England mitgegründet, die sich, ähnlich wie die EFF, unter anderem für eine Liberalisierung des Urheberrechts, gegen digitale Rechteverwaltung und für den Datenschutz engagiert.

1 Die Electronic Frontier Foundation (EFF) ist eine US-amerikanische NGO, die sich für Grundrechte im Informationszeitalter einsetzt. Sie arbeitet in Gerichten und betreibt Öffentlichkeitsarbeit. Dem Direktorium der EFF gehören renommierte Informatiker und Professoren der Rechtswissenschaften an.

2 https://www.eff.org/de/deeplinks/2018/10/information-fiduciaries-must-protect-your-data-privacy

„Wer die Freiheit aufgibt, um Sicherheit zu gewinnen, wird am Ende beides verlieren.“

Benjamin Franklin
Amerikanischer Schriftsteller und einer der Gründerväter der Vereinigten Staaten

RAUS AUS DER BEQUEMLICHKEIT – ECKPFEILER FÜR EINE NACHHALTIGE CYBERSTRATEGIE

Beitrag von Raphael M. Reischuk

Um die Cybersicherheit zu verbessern, müssen wir uns der Attraktivität unserer Daten bewusst werden. Und gleichzeitig die Unattraktivität von Sicherheitsmassnahmen reduzieren. Dies gelingt uns mitunter durch die Schaffung von Anreizen für Bürger und Mitarbeiter zum Mitdenken und die Einführung von Sicherheits-Gütesiegeln für vernetzte Produkte.

Mit der fortschreitenden Digitalisierung nehmen die Berichte über Cyberangriffe auf Menschen, Systeme und Infrastrukturen stetig zu. Obwohl sich die Zahlen nur unpräzise quantifizieren lassen, werden die verursachten Kosten auf jährlich mehrere Milliarden Franken geschätzt – allein in der Schweiz. Das sind pro Einwohner grob 1000 Franken jährlich, und damit weit mehr als die derzeitigen Investitionen in den Schutz vor Cyberrisiken. Die Gründe dafür sind vielfältig, vor allem weil monetäre Mittel allein das Problem nicht lösen können. Neben sinnvollen Investitionen in Ausbildung und Infrastruktur muss der Fokus vor allem auf die Unbequemlichkeit und die Unattraktivität von IT-Sicherheit gelenkt werden. Eine auf Konnektivität ausgerichtete Gesellschaft wird sich an den Gedanken gewöhnen müssen, dass Cyberangriffe omnipräsent sind und dass folglich auch der Schutz vor eben diesen Angriffen ein Dauerthema sein wird. Was unattraktiv klingt und auf

den ersten Blick wenig Mehrwert bietet, muss den Benutzern von IT-Systemen und -Dienstleistungen daher so zugänglich und angenehm wie möglich gemacht werden. Doch wie kann dies gelingen?

ACHT PFEILER EINER NACHHALTIGEN CYBERSTRATEGIE:

1. Durch die Digitalisierung eingesparte Ressourcen für die Sicherheit einsetzen: Die zunehmende Vernetzung bringt ohne Zweifel eine Reihe von Mehrwerten und Komfort. Durch die eingesparte Zeit und den Anstieg der Produktivität bleiben Ressourcen übrig, von denen wenigstens ein Teil für die digitale Hygiene aufgebracht werden sollte. Diese insgesamt positive Bilanz sollte sich im Bewusstsein eines jeden Anwenders manifestieren. Politik und Behörden leisten hierbei bereits heute einen Beitrag, der aber in Zukunft noch attraktiver präsentiert werden muss: weniger durch Abschreckung, sondern vielmehr durch die resultierenden Vorteile einer sicheren Digitalisierung.

2. Nebst den Chancen auch die Risiken neuer Produkte berücksichtigen: Der Grundsatz aller Neu- und Weiterentwicklung von Technologie wird lauten müssen: «IT security by design and default». Was heisst

das konkret? Jedes neu zu entwickelnde Produkt und jedes frisch gestartete Projekt wird sich mit der Frage auseinandersetzen müssen, was der Hauptzweck und der Hauptschaden für das Vorhaben sind. Davon ausgehend muss ein priorisierter Vorgehensplan entwickelt werden, der sicherstellt, dass auch in unvorhergesehenen Szenarien ein sicherer Systemzustand gewährleistet ist. Vergleichbar ist dies mit den seit Jahren aus der Safety bekannten Beispielen im Personentransport mit Flugzeug und Bahn. Eine kontrollierte Abschaltung von gewissen Teilkomponenten wird zum Standard werden, anstelle von unkontrollierten und ausnutzbaren Systemzuständen.

3. Attraktivität von Sicherheitsprodukten durch Gütesiegel und Qualitätsprüfungen erhöhen: Nachhaltigkeit wird sich nicht allein durch kommerziellen Erfolg oder einen niedrigen ökologischen Fussabdruck eines Produkts definieren, sondern zusätzlich durch einen anhaltenden Beleg von Schadensfreiheit. Die Kraft der Märkte wird dabei freilich nicht reichen, um ein Umdenken hervorzubringen. Zusätzlich benötigt es Regulierung in Form von Qualitätsprüfungen und staatlichen Gütesiegeln. Die Unattraktivität von IT-Sicherheit resultiert heute unter anderem daraus, dass selbst interessierten Bürgern und Unternehmern zu wenig Informationen vorlie-

gen, um fundierte und nachhaltige Entscheidungen für den Einkauf sicherer Produkte zu treffen. Eine zentrale, möglicherweise staatlich organisierte Prüfstelle für IT-Sicherheit ist bereits heute notwendig und wird in den kommenden Jahren entstehen.

4. Die eigene Attraktivität für Angreifer erkennen und umdenken: Ein Sinneswandel wird sich in den Köpfen von Entscheidern und Privaten etablieren, von der gefühlten eigenen Unattraktivität für Angreifer (bei mir gibt es nichts zu holen; wer will schon meine Daten) hin zu der Erkenntnis, dass es nur eine Frage der Zeit ist, bis ein Angriff erfolgt. Entsprechend wird in mehr und mehr Unternehmen die Cybersicherheit als strategisches Thema in der Geschäftsleitung verankert sein. Das Bewusstsein für die Investition in Schutz- und Notfallkonzepte wird steigen. Diese werden breiter etabliert, trainiert und regelmässig angepasst werden, da Cyberangriffe schon heute ein Massenphänomen sind und in Zukunft niemand per se geschützt sein wird. Für Angreifer spielt es oft nur eine untergeordnete Rolle, wer von ihrer Ransomware erpresst wird. Das Haus mit der weit offenstehenden Haustür wird eher ausgeraubt als das gut beleuchtete und mehrfach abgeschlossene. Wem das Haus gehört, ist oft nebensächlich. In der Cybersecurity ist dies nicht anders. Folglich wird

die Messbarkeit der eigenen IT-Sicherheit immer wichtiger. Vor allem Unternehmen und Behörden werden qualifizierte Aussagen darüber treffen können, wie hoch das aktuelle Sicherheitsniveau ist und an welcher Stelle die höchste Dringlichkeit besteht. Diese Aussagen werden sich nicht auf technische Komponenten beschränken, sondern auch den heute schwer messbaren Unsicherheitsfaktor Mensch beinhalten. Bereits heute beginnen mehr als 80 % aller Angriffe mit Social Engineering, also mit Schwachstellen in der Art und Weise, wie das menschliche Gehirn funktioniert. Das Ziel dabei ist die Manipulation von Menschen, um ihr Verhalten vorherzusagen und Handlungen hervorzurufen, die sie ansonsten nicht ausführen würden. Im Fachjargon wird das KI-gestützte «Monitoring» flächendeckend brauchbare Hilfestellung leisten – nicht nur für die Evaluation des Sicherheitsniveaus von IT-Systemen, sondern auch für die Evaluation der Sicherheit der eigenen Mitarbeiter. So lassen sich wenigstens die gröbsten Löcher erkennen und stopfen.

5. Anreize schaffen für eine neue Sicherheitskultur in Unternehmen: Nebst dem Umdenken im Unternehmen wird auch der Faktor Mensch eine wichtige Rolle spielen. Die menschliche Bequemlichkeit beim Aufbau von neuen Kompetenzen und Know-how

wird durch Anreize von Arbeitgebern und Programme zum Kulturwandel minimiert werden. Cybersicherheit ist ein anhaltender Prozess innerhalb einer agilen Kultur. Und weder Prozesse noch Kultur lassen sich auslagern. So werden Umgebungen in Unternehmen und im öffentlichen Raum entstehen, in denen Mitarbeiter und Bürger Anerkennung erfahren, wenn sie auf sicherheitsrelevante Missstände hinweisen – und beispielsweise bei einer eintreffenden E-Mail einen Phishing Button in ihrer E-Mail-App drücken, um das im Hintergrund laufende KI-System mit dienlichen Hinweisen zu füttern.

6. Auf das wachsende Vertrauen in die immer besseren Sicherheitsprodukte setzen: Die Attraktivität von Sicherheitsmassnahmen wird ganz allgemein steigen, da das Vertrauen in Produkte und Dienstleistungen wachsen wird. Einen Beitrag wird die oben erwähnte Prüfstelle leisten sowie der von Unternehmen im Sinn einer guten Reputation erbrachte Beleg der anhaltenden Schadensfreiheit. Von Entwicklerseite her werden wir einen Anstieg an Transparenz in Form von Open Source erleben. Sowohl das Design als auch der Programmcode werden häufiger für Experten und interessierte Anwender einsehbar sein. Die EU-Datenschutzgrundverordnung hat bereits eine wichtige Parallele dazu vorgelebt: das

Recht eines jeden EU-Bürgers, die Hoheit über die eigenen Daten zurückzugewinnen. Internationale Konzerne wie Microsoft setzen bereits heute vermehrt auf Open Source. Dieser Trend wird sich fortsetzen und Anwendern die Möglichkeit geben, nachzuvollziehen, was Algorithmen mit den Daten tun und wie es um Hintertüren (Backdoors) in Anwendungen steht.

7. Mut zeigen und disruptive Sicherheitstechnologien adaptieren: Die menschliche Unbequemlichkeit wird unter anderem dadurch entschärft, dass Behörden und Unternehmen den Mut zeigen werden, neuartige Technologien einzusetzen, die auf den ersten Blick unbequem wirken, aber längerfristig einen nachhaltigen gesellschaftlichen Fortschritt ermöglichen. Als Beispiel sei hier eine grösstenteils in der Schweiz entwickelte neuartige sichere Internet-Architektur genannt. SCION revolutioniert das Verständnis, wie Pakete im Internet verschickt werden: Nicht länger wird an zentral kontrollierten Stellen darüber entschieden, wie Pakete weitergeleitet werden. Dieses System aus den Anfängen der 1990er-Jahre führt heute zu vielen Ausfällen, ermöglicht zahlreiche Angriffe und schafft ein hohes Mass an Intransparenz. In SCION hingegen kennt jedes Datenpaket selbst seinen Weg entlang der un-

zähligen Pfade des Internets. Über Jahre etablierte Handlungsmuster, die aufgrund veränderter Rahmenbedingungen heute nicht mehr akzeptiert werden können, werden also infrage gestellt und fundamental umgekrempelt. Verblüffend dabei: Nicht nur die Sicherheit im Cyberspace steigt, sondern auch die Geschwindigkeit und die Wartbarkeit der zugrundeliegenden Infrastruktur. Dass Sicherheit also nicht unattraktiv sein muss, zeigt dieses Beispiel auf exemplarische Weise. Wer nun glaubt, ein so fundamentaler Wandel sei nicht ohne unbequeme Unterbrüche und Ausfälle möglich, der irrt: Das Beispiel SCION zeigt dank Open Source auf transparente Weise, wie «security by design» so umgesetzt werden kann, dass die bedeutendste Infrastruktur der Welt transparenter, effizienter und sicherer wird. Nun braucht es Mut, den Umstieg zu gestalten.

8. Innovation im Bereich der Kommunikation fördern: Die vielleicht grösste Herausforderung in der IT-Sicherheit liegt schliesslich im Bereich der zwischenmenschlichen Kommunikation. Genauer gesagt in der Authentisierung von Gesprächspartnern. In Zeiten von KI-gestützten Fake News wird es bedeutend schwieriger zu entscheiden, ob ein Anruf, eine SMS oder eine E-Mail authentisch ist oder ob es sich um einen Angriff (z. B. Phishing) handelt. Um die Ge-

sellschaft nachhaltig zu schützen, werden wir hier viel Innovation erleben. Neben Biometrie und Mehrfaktorsystemen werden wir Lösungen haben, die unbemerkt viele Einflüsse evaluieren, um Menschen eine permanente Indikation zu geben, wie verlässlich und vertrauenswürdig die Interaktion ist. Zu diesen Einflussfaktoren werden Umgebungsgeräusche, Bewegungsverhalten, Stimmfrequenz, die lokale Wetterlage sowie medizinische Merkmale wie Pulsschlag, Blutdruck oder Atemfrequenz gehören. Erfolgreich wird dieser Ansatz dann sein, wenn es gelingt, Vertrauen in die datenschutzfreundliche und zugleich mehrwertbringende Nutzung der Einflussfaktoren zu gewinnen.

Auch in Zukunft wird es immer so sein, dass alle Überlegungen zur Sicherheit – egal ob physisch oder im digitalen Raum – einer Abwägung bedürfen. Sicherheit ist und bleibt ein Trade-off. Investieren wir mehr, sind wir sicherer, vielleicht sicherer als unser Nachbar oder Mitbewerber. 100 % Sicherheit werden wir dabei aber nie erreichen. Umso mehr sind wir alle gefordert, Sicherheit so attraktiv wie möglich zu gestalten. Denn eine Schwachstelle bei einem Einzelnen ist immer auch eine Schwachstelle für die Gesellschaft.

DR. RAPHAEL M. REISCHUK ist Wissenschaftler und Principal Consultant im Bereich Cyber Security, Head of Cyber Security bei Zühlke sowie Autor zahlreicher wissenschaftlicher Publikationen im Bereich der IT-Sicherheit. Er ist Mitglied mehrerer internationalen Programmkomitees und Keynote-Sprecher auf Konferenzen zu den verschiedensten Themen rund um die IT-Sicherheit. Nach seinem IT-Studium mit Fokus auf Informationssicherheit hat Raphael M. Reischuk im Bereich Web und Cloud Security am Center for IT Security, Privacy and Accountability an der Saarland- und Cornell-Universität dissertiert. Vor seiner Zeit bei Zühlke hat er zudem an der ETH Zürich an einer neuartigen Internet-Architektur und an Blockchain-Technologien geforscht und gelehrt.

„Es gibt keine Sicherheit, nur verschiedene Grade der Unsicherheit.“

Anton Neuhäusler
Deutscher Philosoph (1919–1997)

ALLREAL

Allreal kombiniert ein ertragsstabiles Immobilienportfolio mit der Tätigkeit des Generalunternehmers (Entwicklung und Realisation). Der Wert des Immobilienportfolios beläuft sich auf rund CHF 4,16 Milliarden. Im Geschäftsjahr 2018 betrug das von der Generalunternehmung abgewickelte Projektvolumen CHF 352 Millionen.
In Zürich, Bern, Cham und St. Gallen beschäftigt das Immobilienunternehmen über 230 Mitarbeitende. Allreal, mit operativem Sitz in Zürich, ist ausschliesslich in der Schweiz tätig. Die Aktien der Allreal Holding AG sind an der SIX Swiss Exchange kotiert.

www.allreal.ch

W.I.R.E.

W.I.R.E. ist ein führender interdisziplinärer Think Tank, der sich seit rund zehn Jahren mit globalen Entwicklungen in Wirtschaft, Wissenschaft und Gesellschaft beschäftigt. Im Fokus des Schweizer Denklabors stehen die frühe Erkennung neuer Trends und deren Übersetzung in strategische Landkarten und Handlungsfelder für Unternehmen und öffentliche Institutionen.

An der Schnittstelle zwischen Wissenschaft und Praxis zeichnet sich W.I.R.E. durch eine kritische Denkhaltung und politische Neutralität aus. Thematische Schwerpunkte betreffen die digitale Wirtschaft, gesellschaftliche Innovation und die Förderung der Zukunftsfähigkeit. Dabei stellt der Think Tank seine Expertise in den Dienst von Öffentlichkeit, Unternehmen und Behörden – von Life Science, Finanzdienstleistern und Medien bis hin zu Food und Industrie.

Die zwei- und dreidimensionale Wissensvermittlung von W.I.R.E. zeichnet sich durch die Verbindung von Inhalt und Form sowie einen hohen Anspruch an Ästhetik und Design aus. W.I.R.E. verfügt über ein internationales Netzwerk aus Experten, Vordenkern und Entscheidungsträgern.

www.thewire.ch

RADAR

In der von Allreal in Zusammenarbeit mit dem Think Tank W.I.R.E. herausgegebenen Publikationsreihe stehen relevante Zukunftsthemen im Mittelpunkt. Einmal jährlich fokussiert RADAR auf sich abzeichnende Entwicklungen und deren mögliche Auswirkungen auf unseren Alltag, auf die Wirtschaft und auf die Gesellschaft.

Bei den Autoren handelt es sich um Persönlichkeiten, die dank ihres Fachwissens, ihrer Tätigkeit und Erfahrung umfassend über ein Thema informieren und dieses auch einordnen können.

©2019 W.I.R.E., thewire.ch
Erstellt in Zusammenarbeit zwischen Allreal und dem Think Tank W.I.R.E.

Redaktion:	W.I.R.E., Simone Achermann, Dominique Meier
Konzept:	W.I.R.E.
Mit Beiträgen von:	Myriam Dunn Cavelty, Cory Doctorow, Raphael M. Reischuk, Stephan Sigrist
Gestaltung:	W.I.R.E., Sibylle Brodbeck
Lektorat:	Ruth Rybi
Druck:	Printlink AG, Zürich
Illustration:	©2019 Davide Bonazzi c/o theispot, Chaotic Atmospheres (Cover)