GERALD REISCHL

INTERNET OF CRIMES

WARUM WIR ALLE ANGST VOR HACKERN HABEN SOLLTEN

REDLINE | VERLAG

VORWORT

Es wird jeden treffen. Jede Familie, jedes Unternehmen, jede Organisation, jede Behörde, jede Regierung. Cyberkriminalität ist eine der größten Herausforderungen der nächsten Jahrzehnte.

Sie wird die Welt ab dem Jahr 2021 jährlich 5,5 Billionen Euro kosten – das entspricht etwas weniger als dem Finanzvermögen aller deutschen Staatsbürger, beziehungsweise etwa einem Viertel des Finanzvermögens von China; oder dem Neunfachen des Finanzvermögens von Österreich.[1] Bereits jetzt steht fest, dass dies der größte Transfer wirtschaftlichen Reichtums in der Geschichte der Menschheit sein wird.[2] Selbst wenn die Wirtschaft am Boden liegt, das Coronavirus die Börsen auf Talfahrt schickt, Wirtschaftskrisen debattiert und medial heraufbeschworen werden – es gibt einen Wirtschaftszweig, der weiter florieren wird: Cybercrime. Dieses Business trotzt jedem Konjunkturabschwung.

5,5 Billionen Euro sind eine gigantische Summe. Unvorstellbar eigentlich – nicht nur die Höhe, sondern auch die Art, wie diese Summe zustande kommt: Einerseits werden Daten zerstört oder beschädigt; Geld, Informationen und Identitäten gestohlen; Produktionen von Unternehmen lahmgelegt; Produkte verändert; Menschen, Firmen und Regierungen erpresst; illegale Waren gehandelt … Auf der anderen Seite verschlingen Maßnahmen zur Wiederbeschaffung von gelöschten oder verschlüsselten Daten, forensische Untersuchungen sowie erforderliche Imagereparaturen nach Cyberattacken enorme Mittel.

Die Anzahl der Unternehmen, die auf Cybercrimeangriffe nicht vorbereitet sind, ist hoch, weil sich niemand vorstellen kann, selbst Opfer zu wer-

den. Meist muss erst etwas passieren, ehe erkannt wird, dass man auch selbst zur Zielscheibe werden kann. Ähnlich sorglos handeln auch Privatpersonen. Viele können einfach nicht abschätzen, was passiert, wenn sie leichtfertig einen falschen Link anklicken.

Hacker verschlüsseln mit Schadprogrammen unsere Computer und erpressen uns – zahlen wir nicht, zerstören sie unsere Daten. Sie attackieren Bezahlsysteme, greifen Bankomaten an oder schleusen ihre Viren ein, um an unser Geld zu gelangen. Sie analysieren unser Verhalten in den sozialen Medien und »loggen« sich auf Basis dieses Wissens in unsere Gedankenwelt ein, geben sich als Firmenchefs aus und schöpfen so, wie die vielen Fälle von CEO-Fraud zeigen, Millionen ab. Sie stehlen Identitäten und lassen Menschen in der digitalen **und** analogen Welt verschwinden. Sie beeinflussen Wahlen und bringen Demokratien ins Wanken. Hacker attackieren Herzschrittmacher, Babymonitore oder Computersysteme in Krankenhäusern. Sie legen die Infrastruktur – ganz gleich ob Stromnetz, Verkehrsnetz oder Verkehrsmittel – lahm, manipulieren Überwachungssysteme oder Kommunikationssatelliten und beeinträchtigen die Funktionalität selbstfahrender Automobile.

Hacker verfolgen unterschiedliche Motive. Manche wollen Ruhm erlangen, indem sie Systeme und Unternehmen zerstören oder Politik und Wahlen beeinflussen, andere hacken, um an Geld zu kommen.

Cybercrime betrifft jeden, nicht nur Konzerne und Internet- und Technologie-Granden wie Facebook & Co., sondern auch Kleinunternehmer und jeden einzelnen Bürger – denn praktisch jeder ist im Internet unterwegs und nützt die Tools der digitalen Welt. Selbst in Entwicklungsländern ist die Digitalisierung auf dem Vormarsch.

Die Anfänge

Am 12. März 1989 stellte Tim Berners-Lee das World Wide Web vor und am 20. Dezember 1990 ging mit Info.cern.ch die erste Webseite online.[3, 4] Gegenwärtig gibt es etwa 1,75 Milliarden Webseiten. 4,6 Milliarden Menschen nutzen das Internet. Pro Tag werden allein auf Google etwa 10 Milliarden Suchanfragen gestellt. Aber – und das ist aufschlussreich und alarmierend

zugleich – 56 Prozent des gesamten Internetverkehrs laufen automatisch ab, dafür sorgen Bots, Hackingtools und andere automatisierte Software.[5]

Smarte Anwendungen und Künstliche Intelligenz (KI) werden künftig Unmengen an Daten generieren. Wurde im Jahr 2018 ein Volumen von 33 Zettabyte digitaler Daten global generiert, so geht man davon aus, dass die im Jahr 2025 jährlich generierte digitale Datenmenge weltweit bei 175 Zettabyte liegen wird.[6] Zur Erklärung: 1 Zettabyte sind 1 Billion Gigabyte. Diese Daten müssen einerseits erzeugt, andererseits aber auch entsprechend verarbeitet und gespeichert werden.

Attacken auf das Internet der Dinge

Im Jahr 2017 wurden 310 Millionen Wearables wie Smartwatches oder Headsets verkauft.[7] Die Analysten von Gartner gehen davon aus, dass im Jahr 2021 bereits für umgerechnet 58 Milliarden Euro Wearables gekauft werden. Die Menschheit wird immer »digitaler« und die Welt wird von einem Netzwerk »digitaler Dinge« umhüllt sein. Wir stehen erst am Anfang der digitalen Informationsgesellschaft. 99 Prozent der Welt sind laut des US-Konzerns Cisco noch nicht vernetzt. Erst ein Prozent dessen, was digitalisiert werden kann, wurde bis dato überhaupt digitalisiert.[8]

Die Digitalisierung des Menschen ist bereits in vollem Gange. In absehbarer Zeit wird ein implantierter Chip, der beispielsweise die Gesundheit überwacht oder als Haustürschlüssel genutzt wird, selbstverständlich sein. Parallel dazu werden nicht nur Tiere und Pflanzen von der Digitalisierung erfasst, sondern auch Gegenstände des Alltags wie Küchengeräte, Kleidung, Straßenlaternen, Kanaldeckel oder auch Mülltonnen. Im »Internet der Dinge«* (IoT), das schon lange zum »Internet of everything«[9] (IoE) geworden ist, wird alles – und ich meine wirklich alles – vernetzt und mit Sensoren oder Chips auf die nächste Stufe gehoben. Und diese Welt des IoE wächst in atemberaubendem Tempo. Von zwei Milliarden vernetzten Objekten im Jahr 2006 auf voraussichtlich 200 Milliarden im Jahr 2021 – das sind, rein statistisch

* Bezeichnet die Vernetzung von Gegenständen des Alltags oder von Maschinen im industriellen Umfeld per Internet.

betrachtet, etwa 26 »smarte« Objekte, die auf einen Erdenbürger kommen. Und dieses IoE ist die künftige Spielwiese der Cyberkriminellen; nicht nur, weil es Milliarden an verschiedenen Geräten geben wird, sondern auch, weil viele dieser Geräte zu wenig abgesichert und daher anfällig für Attacken sein werden. Allein im ersten Halbjahr 2019 gab es laut IT-Sicherheitsforschungsunternehmen Kaspersky 100 Millionen Cyberangriffe auf IoT-Geräte.[10]

Die positiven Auswirkungen des Internets liegen aber ebenso klar auf der Hand: Informationen, die für jedermann (mit Internet) abrufbar und frei verfügbar sind. Lexika, für die man früher viel Geld ausgeben musste, wurden durch Wikipedia obsolet, das Wissen wird dort ständig up-to-date gehalten. Ob man eine Sprache lernen, oder sich Texte übersetzen lassen will, wer ein Rezept oder Reparaturanleitungen braucht oder andere »Do-it-yourself«- Tutorials sucht – man wird auf YouTube fündig. Daneben gibt es unzählige fundierte Seiten, auf denen Fortbildungskurse angeboten werden – ob Khan Academy[11] oder Coursera[12]. Wir haben Zugriff auf praktisch alles, was jemals komponiert wurde, können uns Musikbibliotheken nach Lust und Laune zusammenstellen, Filme kurz nach dem Release auf dem Smart-TV zu Hause oder am Smartphone unterwegs sehen, und die Welt auch am (digitalen) Spieleabend zu einem Dorf machen. Zum Beispiel dann, wenn ein Deutscher bei Fifa 20 mit einem Brasilianer zockt oder sich eine Neuseeländerin mit einer Isländerin bei Mario Kart 8 Deluxe duelliert.

Ein Arzt in den USA kann das CT eines Patienten im Norden Thailands befunden, der Urlauber auf dem Kreuzfahrtschiff kann sich mit seinem Smartphone in die Überwachungskamera daheim einloggen oder die Heizung einschalten, der Landwirt von heute kann mit seinem iPad den Mais auf seinen Feldern im Auge behalten. Technologie und Innovation kann im Informationszeitalter die »Global Grand Challenges« lösen.[13]

Die Digitalisierung hat aber auch ihre Schattenseiten. Mit jedem Tag, an dem wir mehr und mehr Dinge miteinander vernetzen, steigt die Gefahr, dass dieses Netzwerk gestört wird. Haben wir einen Plan, wie wir darauf reagieren? Wie käme die Gesellschaft mit einem Ereignis zurecht, das uns wieder ins analoge Zeitalter zurückkatapultieren würde? Wir haben ein weltweites Netzwerk an Computern geschaffen, das wir kaum mehr kontrollieren können und

das die meisten auch nicht verstehen*. Cybersicherheitsexperten einschlägiger Unternehmen, von McAfee über Symantec bis hin zu Kaspersky, warnen, dass vor allem durch die 5G-Technologie und das IoT nicht nur exponentiell steigende Datenmengen anfallen, sondern auch die Attacken exponentiell steigen werden.[14, 15] Daten werden in der 5G-Ära bis zu zehnmal schneller übertragen, die Latenzzeiten werden praktisch bei null liegen. Hacker werden deshalb, unbeobachtet und anonym, in nicht ausreichend gesicherte Systeme eindringen können, weil man ihre Attacken nicht erkennen wird. Wenn man sie entdeckt, ist es bereits zu spät und die Kriminellen sind bereits wieder in die Untiefen des Internets abgetaucht. Das ist die große Herausforderung im Internet der Dinge. Denn es gilt inzwischen als Fakt, dass alles, was gehackt werden kann, gehackt werden wird. Das IoT wird die Welt verändern, aber auch die Attacken auf Systeme aller Art werden exponentiell ansteigen.

Cybersecurity ist das nächste große Ding

Cybersecurity ist ein großes Business. Die weltweiten Ausgaben für Produkte und Dienstleistungen im Bereich der Informationssicherheit lagen im Jahr 2019 bei 124 Milliarden US-Dollar.[16] Und diese Kosten werden jedes Jahr um etwa zehn Prozent steigen. Gleichzeitig steigt die Nachfrage nach Cybersecurityexperten. »IT-Sicherheitsexperte« ist jetzt schon ein gefragter Beruf, künftig werden Fachleute in dieser Sparte eine noch viel größere Rolle spielen. Bis zum Jahr 2021 wird es laut Palo Alto Networks Research Center weltweit 3,5 Millionen unbesetzte Cybersicherheitsstellen geben.[17] Wobei sich die Frage stellt, ob künftig nicht ohnehin jede IT-Position in einem Unternehmen gleichzeitig auch eine Cybersicherheitsposition ist, da sich jeder IT-Mitarbeiter mit dem Schutz der Tech-Infrastruktur und den dazugehörigen Menschen befassen werden muss. Ohne diese allumfassende Herangehensweise kann der Kampf gegen die Cyberkriminalität nicht gewonnen werden. Bisher beschäftigen viele Unternehmen nur einen CIO, einen Chief Information Officer, der für die gesamte IT-Infrastruktur verantwortlich ist. An-

* Deshalb verstehen wir übrigens auch die Updates nicht, die wir installieren müssen, damit unsere Geräte in diesem System weiterhin funktionieren können.

gesichts der steigenden Zahl von Attacken wird in vielen Firmen nun auch ein CISO installiert, ein Chief Information Security Officer. Doch im Grunde sollte jeder CIO auch ein CISO sein. Denn sie werden sich künftig vor Arbeit kaum mehr retten können.

»Cybersecurity ist die Grundlage für eine erfolgreiche und nachhaltige Digitalisierung«, sagt Andreas Tomek, Partner bei KPMG-Österreich und dort für den Bereich Cybersecurity verantwortlich. Tomek ist darüber hinaus Initiator und Organisator des europäischen Sicherheits-Start-up-Wettbewerbs Security Rockstars. »Unternehmen müssen sich so aufstellen, dass Cybersicherheit und Digitalisierungsinitiativen stets miteinander gedacht werden – nur so kann ein stabiles Wachstum gelingen.« Das scheint derzeit nicht wirklich der Fall zu sein, wie die Cyber Security Studie 2020 ergeben hat, bei der mehr als 600 Unternehmen teilgenommen haben.

Auf der einen Seite hat Cybersicherheit nach wie vor für ein Drittel der befragten Firmen noch nicht den Stellenwert, den das Thema haben sollte – es fehlt hier an dedizierten und gut ausgebildeten Experten. Das Unternehmen vor Angriffen zu schützen, spielt – Ransomware hin und Phishing-Kampagne her – für sie noch nicht wirklich eine Rolle; mit Phishing werden Unternehmen übrigens am häufigsten konfrontiert.

Auf der anderen Seite hat ein Drittel der Unternehmen mittlerweile aber erkannt, welche langfristigen finanziellen Folgen Cyberattacken haben können. »Dieses Drittel hat entweder eine Cyberversicherung abgeschlossen oder spezifische Rückstellungen gebildet«, bestätigt Tomek. Denn, und das zeigt auf, wie dramatisch Hackerattacken gesehen werden – jeder dritte Unternehmer glaubt, dass es mehr als einen Monat dauern kann, um einen Angreifer aus dem System zu werfen und die Probleme, die die Cyberattacke verursacht hat, zu lösen. Als »besonders interessant« bezeichnet Tomek die Tatsache, dass drei von vier Unternehmen sich mehr Unterstützung vom Staat wünschen würden. Trotz NIS-Gesetz (Netz- und Informationssystemsicherheitsgesetz) und Datenschutzgrundverordnung fehlt es hier vor allem an praktischer Unterstützung, Förderung europäischer Technologien und Wissensvermittlung seitens des Staates.

Denn die Waffen der Cyberkriminellen werden nicht nur raffinierter und heimtückischer, sondern auch immer zugänglicher. Cyberwaffen kann man

in Darknet-Shops fast so einfach kaufen wie ein Tetrapak Milch im Supermarkt. Das Darknet ist ein Umschlagplatz für Drogen, Falschgeld, Waffen und all diejenigen Tools und Programme, die Hacker dafür nutzen, um in unsere Computer, Smartphones oder auch in Systeme von Regierungen einzudringen. Das wurde sowohl bei den Hackerangriffen auf den Deutschen Bundestag 2015[18] als auch auf das österreichische Außenministerium Anfang 2020[19] offensichtlich. Sind die Zugänge und Passwörter erst einmal geknackt, können Unternehmen und andere Internet-User – Stichwort »Ransomware«[20] – damit erpresst werden

Derzeit heftig diskutierte Technologien, wie 5G, Artificial Intelligence (AI), Big Data, Blockchain und Kryptowährungen, wie beispielsweise Bitcoin oder Monero, eröffnen nicht nur Menschen mit guten Absichten neue Chancen und Möglichkeiten. Sie beflügeln ebenso die Kreativität »der Bösen«, die immer neue Methoden und Tricks entwickeln, um den Ermittlungsbehörden stets einen Schritt voraus zu sein.

Cybercrime ist die am schnellsten wachsende Kriminalitätssparte.[21] Anders als bei analogen Verbrechen müssen Kriminelle nicht »vor Ort« sein. Eine Attacke kann von überall aus gestartet werden – ein Internetanschluss reicht aus. Gegenwärtig sind 4,6 Milliarden Menschen im Web, 2022 werden 6 Milliarden Menschen das Web nutzen, 2030 sollen es bereits 7,5 Milliarden sein.[22, 23] Es gibt heute also bereits 4,6 Milliarden Ziele – sowie dementsprechend 4,6 Milliarden potenzielle Täter.

PROLOG

CYBERCRIME IM SCHATTEN VON COVID-19

Wer war »Patient Zero«, also der erste dokumentierte Träger des Sars-CoV-2-Erregers, der als Covid-19 in die Geschichte eingehen wird?[1] War es jener 55-jährige Bewohner der chinesischen Provinz Hubei, bei dem am 17. November 2019 eine Infektion diagnostiziert wurde, aus der Monate später eine Pandemie entstand, die den gesamten Globus in ein gesellschaftliches und wirtschaftliches Chaos stürzte?

Wurde das »Coronavirus« in einem Labor gezüchtet, um andere Länder damit zu attackieren – Stichwort »Biowaffe«? Oder ist es einem Labor einfach »entwischt«? Wurde es von einem Tier auf den Menschen übertragen? Weil der Sars-CoV-2-Erreger einem Virus sehr ähnlich ist, den Fledermäuse und Schuppentiere in sich tragen?[2] Oder wurde das Virus aus einem anderen Land nach China eingeschleppt?

Im Internetzeitalter gibt es oft unzählige Erklärungen für ein und dasselbe Ereignis. Und für jede dieser Erklärungen werden »plausible« Argumente und logische »Beweise« geliefert. Woher Covid-19 tatsächlich stammt? – Das wird wohl für immer Spekulation bleiben. Selbst bei der im November des Jahres 2002 aufgetretenen Infektionskrankheit SARS sind sich die Wissenschaftler bis heute nicht hundertprozentig sicher: »Anhand der Gensequenzen wird vermutet, dass ein bekanntes Coronavirus entweder mutiert oder dass eine Virusart, die bisher nur Tiere befallen hat, auf den Menschen ›übergesprungen‹ ist.«[3] Doch bleiben wir bei Covid-19. Chinesische Wissenschaftler sollen, so

berichtete die South China Morning Post am 13. März 2020,[4] im Januar dieses Jahrs exakt 266 Menschen ausfindig gemacht haben, die bereits im Jahr 2019 an Covid-19 erkrankt gewesen sein sollen. Die Experten hätten damals auch den »Patient Zero« gefunden, hieß es. Die Fallzahlen wären damals zwar gering gewesen, seien aber ab 17. November 2019 stetig gestiegen, bis dann bereits einen Monat später, am 15. Dezember 2019, 27 Fälle der neuartigen Krankheit dokumentiert werden konnten. Ab diesem Zeitpunkt dürfte sich die Zahl der Neuinfektionen praktisch täglich verdoppelt haben. Dass es sich bei diesem Virus um eine neuartige Infektionskrankheit handelte, soll den chinesischen Behörden erst Ende Dezember des Jahres 2019 bewusst geworden sein. Am 31. Dezember meldeten Chinas Behörden den ersten bestätigten Coronavirus-Fall an die Weltgesundheitsorganisation, die noch am selben Tag mit einer Aussendung an die Öffentlichkeit ging: »Pneumonia of unknown cause reported to WHO China Office«.[5]

»Made in China« oder »Made in the USA«?

Die Welt streitet über den Ursprung der neuartigen Infektionskrankheit: Ist die Wurzel allen Übels tatsächlich auf einem Markt in der 11-Millionen-Stadt Wuhan zu suchen? Nicht nur in den sozialen Medien wird heftig darüber diskutiert. Selbst renommierte Wissenschaftler und Experten sind sich uneinig und fallen sogar – teilweise abstrusen – Verschwörungstheorien zum Opfer. Eine Sammlung solcher Theorien hat der junge Telepolis-Journalist Bulgan Molor-Erdene in seinem Artikel »Coronavirus: ›Made in China‹ oder ›Made in the USA‹?« zusammengestellt.[6]

Die USA unterstellen China, den Ausbruch des Virus vertuscht zu haben. Sie bezeichnen Covid-19 auch als »Wuhan-Virus« oder »chinesisches Coronavirus«, und verpassen ihm damit ein »Made-in-China«-Label. In sämtlichen Medien wird behauptet, das Virus habe sich von einem Seafood-Market in Wuhan aus verbreitet, weil sich die Essgewohnheiten der Chinesen so grundsätzlich von denen der westlichen Welt unterscheiden würden. Videos, unter anderem auf YouTube, sollen beweisen, was alles an (teilweise noch lebenden) Tieren verzehrt würde und dass Covid-19 nur die logische Folge solcher

Ernährungsgewohnheiten sein könne. China wiederum versucht argumentativ entgegenzuhalten. Anfang März des Jahres 2020 behauptete der Sprecher des chinesischen Außenministeriums, Zhao Lijian, dass Covid-19 zwar zuerst in China entdeckt worden wäre, es aber nicht erwiesen sei, dass das Virus tatsächlich aus China stamme.[7]

Auf jedes chinesische Argument folgt ein amerikanischer Konter. Der republikanische US-Senator Tom Cotton (Arkansas) behauptete in einem Interview mit Fox News Mitte Februar[8], das Coronavirus sei in einem »Superlabor der Biosicherheitsstufe 4« entwickelt worden, das sich in der Nähe des Seafood-Markets von Wuhan befinden würde.

Obwohl zahlreiche Wissenschaftler diese Entstehungsgeschichte ins Reich der Märchen verwiesen haben, bleiben solche Verschwörungstheorien lebendig. Sie werden mitunter sogar von angesehenen, verdienstvollen Medizinern, wie dem österreichischen Virologen Wolfgang Graninger, weiterverbreitet. Der Infektiologe lehrte an der Medizinischen Universität Wien, war der Leiter der klinischen Abteilung für Infektionen und Tropenmedizin am Wiener Allgemeinen Krankenhaus und gilt bis heute als anerkannter Experte. Staatsoberhäupter aus der ganzen Welt ließen Graninger einfliegen, um sich von ihm behandeln zu lassen. Ab 1996 war er der behandelnde Arzt des damaligen österreichischen Bundespräsidenten Thomas Klestil, der an einer Autoimmunerkrankung litt und im Jahr 2004 verstarb. Doch mit einem Interview vom 15. März 2020 im *Kurier* sorgte Graninger für Aufsehen. Auf die Frage, wer das Virus seiner Ansicht nach »erfunden« habe, meinte er: »Die Chinesen (…) Es war nicht für China gedacht, sondern es sollte in den USA ausgesetzt werden, damit dort die Bevölkerung hysterisch wird und die Wirtschaft ordentlich kracht (…) das ist die Rache der Chinesen an den Amerikanern.« Auf Nachfrage, wie es angesichts dieser Theorie zu erklären sei, dass auch Chinesen infiziert wurden und starben, argumentierte Graninger: »Das war ein Unfall. Das Virus ist ihnen entwischt. Es hat ja das Militär sofort reagiert, indem es die Region abgeriegelt und Spitäler errichtet hat.«

Wenn selbst angesehene Mediziner derartige Theorien vertreten und unbelegte Behauptungen aufstellen, so ist es nicht verwunderlich, dass sich diese ebenfalls in den sozialen Medien rasch verbreiten. Am 12. März 2020 empfahl der bereits oben erwähnte Sprecher des chinesischen Außenministeriums,

Zhao Lijian, seinen Twitter-Followern einen Artikel des auf Verschwörungstheorien spezialisierten kanadischen Webportals GlobalResearch mit dem Titel »Covid-19: Evidence that Virus originated in the USA«.[9] Darin hieß es: Japanische und taiwanesische Epidemiologen und Pharmakologen hätten festgestellt, dass das neue Coronavirus in den USA entstanden sein könnte, weil in den USA alle fünf Coronavirus-Typen aufzufinden seien, in China jedoch nur einer. In den USA habe es bereits 2019 zahlreiche Fälle von Lungenentzündungen gegeben, die man dort auf Vaping zurückgeführt habe[10]. Der taiwanesische Mediziner unter den Experten habe laut GlobalResearch die USA darauf aufmerksam gemacht, dass er davon überzeugt sei, dass diese Todesfälle auf das Coronavirus zurückzuführen seien. Seine Warnungen seien jedoch ignoriert worden.

Im Juli des Jahres 2019 verfügte die Aufsichtsbehörde C.D.C. (Centers for Disease Control and Prevention) eine Teilschließung des wichtigsten Biolabors des US-Militärs in Fort Detrick, Maryland, USAMRIID (U.S. Army Medical Research Institute of Infectious Diseases). Als Begründung für die Einstellung wesentlicher Forschungsprojekte auf unbestimmte Zeit wurden mangelhafte Sicherheitsvorkehrungen gegen die Verbreitung von Krankheitserregern angeführt.[11] Im USAMRIID werden zum einen Abwehrmaßnahmen gegen biologische Kriegsführung entwickelt. Andererseits werden aber auch Impfstoffe gegen sowie Behandlungs- und Diagnosemöglichkeiten für die gefährlichsten Krankheitserreger der Welt erforscht. Eines der aktuellsten Projekte des USAMRIID ist ein Medikament gegen Ebola. In dem bereits erwähnten GlobalResearch-Artikel wird die Behauptung aufgestellt, das Virus habe sich aus dem Labor heraus »verselbstständigt«, und die Behörden hätten die daraus resultierenden tödlichen Lungeninfektionen mit dem Vaping der E-Zigaretten gerechtfertigt, obwohl die Symptome angeblich nie zu Vaping gepasst hätten. Im September 2019 wurde bekannt, dass Hunderte US-Bürger von einer (angeblich durch Vaping verursachten) Lungenkrankheit betroffen waren und 39 daran gestorben sind.[12]

Wie aber wäre das Virus dann nach China gelangt? Auch dafür liefert die Verschwörungstheorie die passende Erklärung: Im Oktober 2019 fanden im chinesischen Wuhan die Military Games statt, an denen auch die US-Army mit 300 Soldaten teilnahm. Die Spiele begannen am 19. Oktober und dauer-

ten bis 27. Oktober. Drei Wochen später gab es in China unbestätigterweise »Patient Zero«. Die Theorie hinkt. Da die Inkubationszeit maximal 14 Tage beträgt, hätte es vor der Entdeckung dieses Patienten Null eigentlich einen oder viele andere geben müssen, die infiziert worden wären und andere angesteckt hätten. Doch darauf geht GlobalResearch nicht ein. Telepolis bringt die Absurdität dieser Theorie sehr treffend auf den Punkt: »Für Larry Romanoff von GlobalResearch[13] heißt das: Es könnte sein, dass sich einige Mitglieder des US-Teams durch einen zufälligen Ausbruch in Fort Detrick mit dem Virus infiziert haben, ihre Symptome aber bei einer langen anfänglichen Inkubationszeit unmerklich waren und dass diese Personen während ihres Aufenthalts bei den Militärspielen in Wuhan möglicherweise Tausende von Anwohnern an verschiedenen Orten infiziert haben, von denen viele später auf den Seafood-Markt gingen. Von dort aus hat sich das Virus dann wie ein Lauffeuer ausgebreitet.«[14]

Ob in einem Labor in Fort Detrick oder in einem Labor in Wuhan: Dass das Virus »gezüchtet« worden sei, daran glauben ernstzunehmende Wissenschaftler nicht. Man könne mit hoher Wahrscheinlichkeit bestätigen, dass das Virus kein Produkt der Gentechnik sei,[15] wird sowohl auf dem populären Diskussionsforum virological.org als auch auf der britischen Plattform fullfact.org betont, auf der Informationen auf ihren Wahrheitsgehalt hin geprüft werden.[16]

Fake News und Verschwörungstheorien zu Covid-19

Vor diesem Hintergrund ist es beinahe logisch, dass sich in den Medien Verschwörungstheorien, Fake News und unbelegbare Behauptungen verbreiten. Covid-19 beweist auf anschauliche Weise, wie rund um ein Ereignis Falschmeldungen entstehen, sich weiterentwickeln und immer weiterverbreiten. In einer Zeit, in der selbst Staatspräsidenten die Klimaerwärmung leugnen[17], in der es Zehntausende Menschen gibt, die daran glauben, dass die Erde flach ist*, darf man sich nicht wundern, wenn selbst die absurdesten Theorien plötzlich als »wahr« beurteilt und verbreitet werden.

* Einer von sechs Amerikanern ist sich nicht sicher, ob die Erde eine Kugel ist.

KAPITEL 1

FAKEWORLD

»Es gibt Deepfakes von dir«,

stand in der Betreffzeile. Die Nachricht hätte auch ein Spam sein können, aber instinktiv googelte Noelle Martin nach dem Wort »Deepfake«, als sie 2019 das kryptische Mail von einem ihr unbekannten Absender erhielt. Ihr stockte der Atem, als sie las: »Deepfake ist die Verschmelzung der beiden Begriffe ›Deep Learning‹ und ›Fake‹. Ein Deepfake ist ein Video, bei dem das Gesicht eines Menschen auf das Original montiert wird. Die Technologie basiert auf künstlicher Intelligenz, die die Eigenheiten und Gesten eines bestimmten Gesichts lernt und sie daher überzeugend nachbilden kann, um jede Bewegung auszuführen.« [1, 2, 3]

Die junge australische Frauenrechtsaktivistin, die mittlerweile weit über die Grenzen Australiens hinaus bekannt ist, googelte weiter. Sie klickte auf das Symbol »Videos« – und sofort poppte eine Trefferliste von offensichtlich gefälschten Videos auf. Sie zeigten Politiker, TV-Moderatoren oder Schauspieler, in teils sehr diffamierenden Posen. So beispielsweise in Pornovideos – in den Hauptrollen bekannte Schauspielerinnen wie Megan Fox oder Scarlett Johansson. Es war zwar erkennbar, dass es sich um Fälschungen handelte, aber diese waren teilweise erschreckend gut gefakt.

Noelle Martin spürte, wie sich allmählich Panik in ihr breit machte. Sie antwortete auf die E-Mail: »*Kannst du sie mir senden*?« Es kam eine Antwort, die nichts weiter als einen Link zu einer Pornoseite enthielt. Martin klickte auf den Link und es startete ein elf Sekunden langer Clip, der eine Frau zeigte, die mit einem Mann Sex hatte.[4] Die Frau war in Ganzkörper-Nahaufnahme zu sehen, ihre Augen blickten direkt in die Kamera, in die Augen des Betrachters. Und die Betrachterin war in diesem Moment Noelle Martin selbst. Sie sah nicht in das Gesicht einer Fremden, sondern in ihr eigenes. Sie war die Hauptdarstellerin des Pornoclips. Noelle Martin wurde Opfer von »Face Swapping«, dem digitalen Gesichtstausch.

Betitelt wurde der Clip mit »Noelle Martin«. Das Video war mit den Hashtags #NoelleMartin, #Feminist, #Amateur, #BigTits, #Indisch versehen worden. In der Beschreibung wurde erläutert, dass es sich um ein echtes Video von Noelle Martin handeln würde. Und es war nicht das Einzige, wie sich später herausstellen sollte. Es gab ein weiteres Video, das sie über die Suchleiste

fand, ebenfalls betitelt mit ihrem Vor- und Nachnamen. Diesmal war es ein Oralsex-Video. Überzeugend gut gefälscht. Noelle Martin geriet in Panik – warum sollten Menschen, die sie kennen, die Echtheit dieser täuschend real aussehenden Fälschungen anzweifeln? Wie konnte sie klarstellen, dass sie nicht die Person war, die in diesen Videos zu sehen ist? Sie klappte ihren Laptop zu und war verzweifelt. Noch verzweifelter als sieben Jahre zuvor. Denn es gab eine Vorgeschichte.

Bereits im Jahr 2012 erlebte Noelle Martin einen einschneidenden Moment, der ihr Leben völlig veränderte.[5] Zwar verdankte sie diesem Erlebnis auch ihre gegenwärtige Karriere als Frauenrechtsaktivistin und Kämpferin für den Schutz vor Missbrauch im Netz. Doch den Weg zu internationaler Bekanntheit hätte die junge Frau gerne mit weniger Hürden gemeistert.

Diese Erfahrung war auch der Grund dafür, dass Martin bei Erhalt der Deepfake-Mail des Fremden sofort in Panik geriet: Bei einer sogenannten Umkehrbildsuche im Web – man kann anhand eines Beispielbildes ähnliche oder gleiche Fotos finden – wollte die damals 18-jährige Rechtsstudentin herausfinden, ob jemand im Netz Fotos von ihr veröffentlicht habe. Für die Suche nutzte sie ein Foto, das sie irgendwann auf Facebook gepostet hatte – ein einfacher Schnappschuss, der sie in einem schwarzen Kleid zeigt, lächelnd, auf einer Party mit Freunden. Das Ergebnis ließ sie erstarren: Dutzende pornografische Bilder poppten auf, alle zeigten, vermeintlich, Noelle Martin bei verschiedensten Sexualpraktiken. Alle waren gefälscht. Um einige der Fotos »noch echter« aussehen zu lassen, hatten die Cyberkriminellen per Photoshop nachträglich Spermaspuren auf ihrem Gesicht platziert.

Im ersten Moment hoffte sie noch, dass die Frau auf den Fotos ihr nur zufällig ähnlich sah. Aber je genauer sie die Bilder betrachtete, desto deutlicher wurde es, dass sie zwar den Körper einer anderen sah, jedoch sehr wohl ihr eigenes Gesicht – extrahiert aus unterschiedlichen Aufnahmen, die sie selbst oder Freunde von ihr auf Social Media teilweise bereits vor Jahren teilten. Manche der bearbeiteten Fotos wurden nicht nur kommentiert, sie enthielten ausführliche und detaillierte Beschreibungen darüber, wer ihre Freunde seien oder was sie studiert habe. Selbst ihre Wohnadresse war auf diesen Seiten zu finden. Noelle Martin glaubte, ihr würde der Boden unter den Füßen weggezogen.

Zu dem Schock kam auch noch Kritik aus ihrem Umfeld sowie wenig hilfreiche Ratschläge von der Polizei, an die sie sich gewandt hatte: Hätte sie ihre Social-Media-Aktivitäten auf »privat« gestellt, wäre ihr das nicht passiert, bekam sie zu hören. Doch die Vorwürfe gingen ins Leere. Der Privatmodus war »an« gewesen, aber der oder die Angreifer hatten sich anhand von Fake-Profilen mit Facebook-Freunden von Noelle Martin angefreundet und konnten dadurch ebenfalls ihre Fotos sehen. Darüber hinaus verfolgten sie die junge Frau in öffentlich zugänglichen Bildergalerien, die oft nach Events erstellt werden.

Noelle Martin stellte sich immer wieder die Frage nach dem Warum. *Warum sie*? Und warum wird eine Frau, die keine Feinde hat und sich nie hat etwas zuschulden kommen lassen, Opfer eines derartigen Rufmords? Weil man sich in der Öffentlichkeit zeigt, mitunter auch Fotos davon postet oder auch die Art der Kleidung, die man trägt – das alles könne doch nicht als Einladung gewertet werden, jemanden auf so heimtückische Weise zu attackieren! Es müsse Tausende Frauen da draußen geben, die auf die gleiche Art verunglimpft würden, nur nichts davon wüssten. Davon war Noelle Martin nun überzeugt.

SOCIAL MEDIA LIEFERT DAS FUTTER

Social Media hat die Kommunikation revolutioniert. Menschen können sich vernetzen, über nationale und internationale Grenzen hinweg miteinander in Kontakt treten, Gemeinschaften bilden und Inhalte teilen. Allein auf Facebook, mit seinen etwa 2,5 Milliarden Nutzern eine der größten Plattformen im Web, werden pro Sekunde 4000 Fotos hochgeladen.[6] Das sind 350 Millionen Fotos pro Tag: Urlaubsbilder, Tierfotos, Schnappschüsse, Food-Porn, Selbstporträts mit Duckface oder ohne, aber auch sehr, sehr viele Kinderfotos.

Dazu muss man wissen: Fotos, die auf Social-Media-Plattformen gepostet werden, können für kriminelle Zwecke missbraucht werden, und das werden sie auch! Es beginnt beim kleinen Copyright-Verstoß – das Motiv wird geklaut und ohne Zustimmung des Fotografen weiterverwendet – und geht bis zu Identitätsdiebstahl.