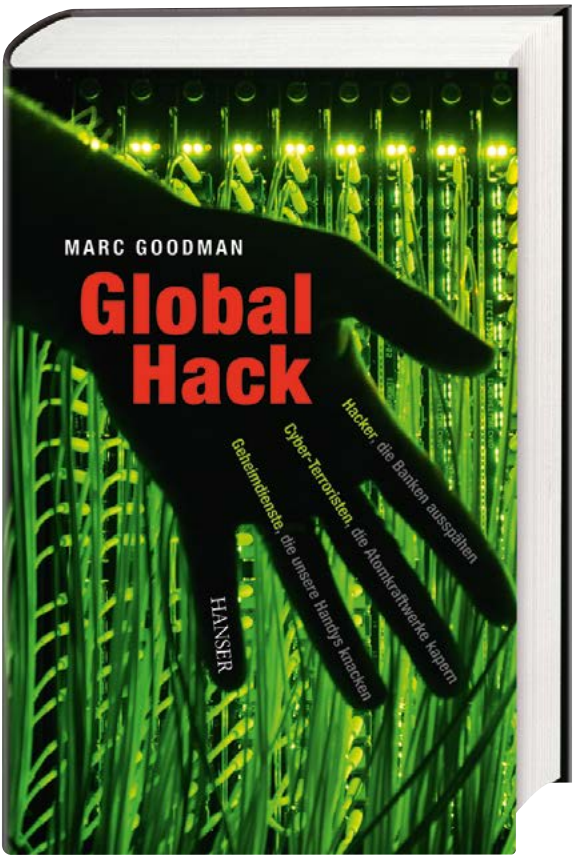
Leseprobe aus:

Marc Goodman
Global Hack



Mehr Informationen zum Buch finden Sie auf
www.hanser-literaturverlage.de

HANSER

Marc Goodman

GLOBAL HACK

Marc Goodman

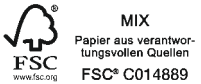
GLOBAL HACK

Hacker, die Banken ausspähen.
Cyber-Terroristen, die Atomkraftwerke kapern.
Geheimdienste, die unsere Handys knacken.

Aus dem Englischen von Henning Dedekind,
Kathleen Mallett und Karin Miedler

HANSER

Titel der Originalausgabe:
Future Crimes: Everything is Connected, Everyone is Vulnerable and What We Can Do About It.
United States: Doubleday, a division of Random House LLC, New York, 2015.
Canada: Random House of Canada Limited, Toronto, Penguin Random House companies, 2015.



Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

1 2 3 4 5 19 18 17 16 15

www.hanser-literaturverlage.de
Herstellung: Denise Jäkel
Umschlaggestaltung: Birgit Schweitzer, München, unter Verwendung eines Fotos von
© Daniel Reinhardt/picture alliance/dpa
Satz: Kösel Media GmbH, Krugzell
Druck und Bindung: Friedrich Pustet, Regensburg
Printed in Germany
ISBN 978-3-446-44463-8
E-Book-ISBN 978-3-446-44464-5

All meinen Lehrern, die mir so viel beigebracht haben.

Inhalt

Teil III: Den Fortschritt überleben

KAPITEL 17

KAPITEL 18

VORWORT

Der irrationale Optimist: Wie ich wurde, was ich bin

Mein Einstieg in die Welt des Hightech-Verbrechens war recht unspektakulär. Im Jahre 1995 arbeitete ich als Ermittler im berühmten Parker Center, dem damaligen Hauptquartier der Polizei von Los Angeles. Ich war 28 und bekleidete den Rang eines Sergeants. Eines Tages bellte mein Vorgesetzter meinen Namen quer durch das volle und geschäftige Dezernat: »Gooooodmaaaaan, bewegen Sie ihren Arsch hierher!« Ich glaubte, ich würde Schwierigkeiten bekommen, doch stattdessen stellte mir der Lieutenant jene Frage, die mein Leben verändern sollte: »Wissen Sie, wie man in WordPerfect die Rechtschreibprüfung aktiviert?«

»Klar, Chef, drücken Sie einfach Strg + F2«, entgegnete ich.

Er grinste und sagte: »Ich wusste doch, dass Sie der richtige Mann für diesen Fall sind.« So begann also meine Karriere als Hightech-Ermittler mit meinem ersten eigenen Fall im Bereich der Computerkriminalität. Durch mein Wissen, wie man in WordPerfect die Rechtschreibprüfung aktiviert, zählte ich Anfang der Neunziger zur polizeilichen Technik-Elite. Seit jenem Fall interessiere ich mich nicht nur brennend für die Technik an sich, sondern vor allem auch für ihre illegalen Anwendungen. Obwohl ich erkenne, welcher Schaden durch rechtswidrig eingesetzte Technologien entsteht, finde ich es trotzdem faszinierend, wie clever und innovativ Kriminelle zur Erreichung ihrer Ziele vorgehen.

Um die allerneuesten Technologien in ihre modi operandi aufzunehmen, bringen sich Verbrecher regelmäßig auf den neuesten Stand. Die Zeiten, da sie die Ersten waren, die einen Pager mit sich herumtrugen und kiloschwere Mobiltelefone verwendeten, um sich gegenseitig verschlüsselte Botschaften zu schicken, sind längst vorbei. Kriminelle Vereinigungen wie die mexikanischen Drogenkartelle verfügen heute über eigene, landesweite Telekommunikationssysteme.[1]

Man stelle sich nur einmal vor, welcher Raffinesse es bedarf, ein landesweit voll funktionsfähiges, verschlüsseltes Telekommunikationsnetzwerk zu errichten – das ist umso erstaunlicher, wenn man bedenkt, dass viele Amerikaner immer noch keinen brauchbaren Handy-Empfang haben.

Organisierte Banden machen sich neue Technologien in der Regel früh zu eigen. Lange, bevor es der Polizei überhaupt in den Sinn kam, entdeckten sie das Internet für sich. Seitdem sind sie den Behörden immer eine Nasenlänge voraus. Die Schlagzeilen sind voll von Geschichten über 100 Millionen gehackter Internetkonten hier und 50 online gestohlenen Millionen dort. Die Entwicklung dieser Verbrechen ist frappierend und schreitet leider immer schneller voran.

Gegenstand dieses Buches ist nicht einfach, was sich gestern ereignet hat oder heute ereignet. Im Fokus steht auch nicht die Frage, wie lang ein Passwort sein sollte. Vielmehr geht es darum, wohin wir morgen gehen werden. Im Zuge meiner Nachforschungen und Ermittlungen, zunächst als Angehöriger des Los Angeles Police Department, später in Zusammenarbeit mit bundesweiten und internationalen Organisationen zur Verbrechensbekämpfung, hatte ich mit Kriminellen zu tun, die weit über die heutige Cyberkriminaliät hinaus in neue Bereiche wie Robotik, virtuelle Realität, künstliche Intelligenz, 3-D-Druck und synthetische Biologie vorgedrungen waren. In den meisten Fällen sind sich meine Kollegen von Polizei und Regierung, mit denen ich mich auf der ganzen Welt getroffen habe, dieser bedrohlichen technologischen Entwicklungen nicht bewusst, geschweige denn ihrer zunehmenden Anwendung durch das organisierte Verbrechen und den Terrorismus. Da ich jemand bin, der sein Leben in den Dienst der öffentlichen Sicherheit gestellt hat, bereiten mir die Trends, die ich allerorten beobachte, große Sorgen.

Manch einer mag mich als Panikmacher oder übertriebenen Pessimisten verteufeln, doch ich bin keines von beiden. Angesichts dessen, was ich über unsere Zukunft erfahren habe, bin ich vielmehr optimistisch – vielleicht »irrational optimistisch«. Um es ganz klar zu sagen: Ich bin kein Technikfeind. Ich bin auch nicht so töricht, anzunehmen, die Technik wäre der Quell allen Übels auf der Welt. Ganz im Gegenteil: Ich glaube an die ungeheure Kraft der Technik als treibende Kraft des Guten. Man sollte auch nicht vergessen, dass sie vielgestaltige Möglichkeiten zum Schutz des Einzelnen und der Gesellschaft bietet. Allerdings war die Technik schon immer ein zweischneidiges Schwert. Meine Erfahrungen mit echten Kriminellen und Terroristen auf sechs Kontinenten haben mir eindeutig gezeigt, dass die Mächte des Bösen niemals zögern, aufkommende Technologien zu nutzen und sie zum Schaden der breiten Masse ein-

zusetzen. Die Tatsachenlage und mein Bauchgefühl sagen mir zwar, dass wir noch beachtliche Hürden vor uns haben (denen Regierung und Industrie leider nicht genug entgegensetzen), doch möchte ich an die Technik-Utopie glauben, die uns Silicon Valley einst versprochen hat.

Dieses Buch ist die Geschichte der Gesellschaft, die wir mit unseren technologischen Mitteln aufbauen, und wie eben diese Errungenschaften gegen uns gerichtet werden können. Je mehr wir unsere Geräte und unser Leben mit der globalen Informationsstruktur vernetzen – sei es via Mobilfunk, soziale Netzwerke, Fahrstühle oder selbstfahrende Autos – desto verwundbarer werden wir für jene, die wissen, wie die zugrundeliegenden Technologien funktionieren, und sie zu ihrem Vorteil und zum Schaden des kleinen Mannes nutzen. Kurz: Wenn alles vernetzt ist, ist alles angreifbar. Die Technik, die wir gewohnheitsmäßig in unserem Leben akzeptieren, ohne uns große Gedanken darüber zu machen, kann uns eines Tages leicht zur Stolperfalle werden.

Indem ich die neuesten kriminellen und terroristischen Methoden beleuchte, hoffe ich, bei meinen Freunden in der Politik und in Sicherheitskreisen eine angeregte und längst überfällige Diskussion anzustoßen. Die meisten sind mit herkömmlichen Verbrechen zwar bereits überlastet, doch müssen sie sich früher oder später mit der rasanten Entwicklung von Technologien auseinandersetzen, die unsere globale Sicherheit wie ein Tsunami des Bösen destabilisieren könnte.

Mehr noch: Ich habe vor langer Zeit geschworen, andere »zu schützen und ihnen zu dienen«; daher will ich dafür sorgen, dass der breiten Öffentlichkeit die erforderlichen Fakten an die Hand gegeben werden, damit Bürger sich selbst, ihre Familien, ihre Unternehmen und ihre Gemeinden gegen eine wachsende Bedrohung verteidigen können, mit denen sie viel früher als erwartet konfrontiert werden. Dieses Wissen »Insidern« vorzubehalten, die bei der Regierung, der Polizei und im Silicon Valley arbeiten, reicht schlicht nicht aus.

Während meiner Zeit im öffentlichen Dienst war ich unter anderem für Organisationen wie das LAPD, das FBI, den U. S. Secret Service und Interpol tätig. Dabei wurde mir zunehmend klar, dass Kriminelle und Terroristen weltweit wesentlich innovativer waren als die Behörden, und die »Guten« immer weiter ins Hintertreffen gerieten. Auf der Suche nach effektiveren Methoden zur Bekämpfung der wachsenden Verbrecherlegionen, die neueste Technologien missbrauchten, quittierte ich meinen Dienst und zog ins Silicon Valley, um mehr darüber zu erfahren, was als Nächstes geschehen würde.

In Kalifornien tauchte ich in eine Gemeinde technischer Innovatoren ein, um herauszufinden, wie sich ihre neuesten wissenschaftlichen Entdeckungen auf

den Normalbürger auswirken würden. Ich besuchte die Sprösslinge des Silicon Valley und freundete mich mit einigen hochbegabten Mitgliedern der Start-up-Community San Franciscos an. Ich wurde an die Fakultät der Singularity University berufen, eine erstaunliche Institution auf dem Gelände des Ames Research Center der NASA, wo ich mit einer Reihe hervorragender Astronauten, Robotiker, Daten- und Computerwissenschaftler und synthetischer Biologen zusammenarbeitete. Diese Männer und Frauen leisten Pionierarbeit. Sie besitzen die Fähigkeit, über den Tellerrand der heutigen Welt zu blicken und das gewaltige Potenzial einer Technik freizusetzen, die eine Antwort auf die drängendsten Fragen der Menschheit liefern kann.

Viele Unternehmer, die in Silicon Valley mit Hochdruck an unserer technologischen Zukunft arbeiten, machen sich jedoch gefährlich wenig Gedanken um politische, rechtliche oder ethische Aspekte und übersehen die Sicherheitsrisiken, die ihre Schöpfungen für den Rest der Gesellschaft darstellen. Da ich selbst schon Kriminellen Handschellen angelegt und mit Polizeikräften in über 70 Ländern zusammengearbeitet habe, betrachte ich die potenziellen Risiken neuer Technologien aus einem ganz anderen Blickwinkel als die arglosen Menschen, die solche Neuerungen meist unkritisch in ihren Alltag einbinden.

Aus diesem Grund habe ich das Future Crimes Institute gegründet. Ziel war es, meine eigenen Erfahrungen als Straßenpolizist, Ermittler, internationaler Antiterror-Analyst und – seit Kurzem – Silicon-Valley-Insider zu nutzen und eine Gemeinschaft gleichgesinnter Experten zusammenzubringen, die sowohl den negativen als auch den positiven Auswirkungen rasanter technologischer Entwicklungen begegnen kann.

Mit Blick auf die Zukunft bereiten mir insbesondere die Omnipräsenz der Computertechnologie in unserem Leben und die damit verbundene Abhängigkeit Sorgen. Dadurch werden wir zunehmend angreifbar, und zwar in einer Art und Weise, die die meisten von uns nicht einmal ansatzweise verstehen. Die gegenwärtige Komplexität von Systemen und deren Interdependenzen nehmen stetig zu. Dennoch gibt es Einzelne und Gruppen, die sie zum Schaden aller rasch durchschauen und in Echtzeit weiterentwickeln.

Dies ist ihre Geschichte – die Geschichte organisierter Verbrecher, Hacker, skrupelloser Regierungen, regionaler Akteure und Terroristen, die miteinander darum wetteifern, sich die neuesten Technologien zunutze zu machen.

Die vom Silicon Valley verheißene Technik-Utopie mag möglich sein, doch wird sie nicht wie durch Zauberhand von selbst erscheinen. Damit sie erblühen kann, müssen Bürger, Regierungen, Konzerne und Nichtregierungsorganisationen enorme und konzentrierte Anstrengungen unternehmen. Zwischen jenen,

welche die Technik zugunsten der gesamten Menschheit vorantreiben, und denjenigen, die sie stattdessen rücksichtslos zu ihrem eigenen Vorteil nutzen wollen, ist ein neuer Kampf entbrannt. Es ist die Schlacht um die Seele der Technik und um ihre Zukunft. Sie wird im Hintergrund und zum Großteil im Verborgenen geschlagen und ist damit den Blicken des Durchschnittsbürgers entzogen.

Statt lediglich die neuesten kriminellen Innovationen und technischen Schwachstellen zu katalogisieren, zeigt dieses Buch einen Weg auf, wie wir den vielfältigen Bedrohungen, die uns erwarten, entgegentreten können. Vorausschauend halte ich es für möglich, schon heute die Verbrechen von morgen vorherzusehen und zu verhindern – bevor wir einen Punkt erreichen, an dem es kein Zurück mehr gibt. Künftige Generationen werden zurückblicken und ein Urteil über unsere Bemühungen fällen, dieser Sicherheitsbedrohungen Herr zu werden und die Seele der Technik so zu verteidigen, dass sie ausschließlich zum Wohle der Menschheit eingesetzt wird.

Eine gutgemeinte Warnung: Wenn Sie weiterlesen, werden Sie Ihr Auto, Ihr Smartphone oder Ihren Staubsauger künftig mit ganz anderen Augen sehen.

TEIL I:
EIN STURM ZIEHT HERAUF

KAPITEL 1

Vernetzt, abhängig, angreifbar

Mat Honans Leben sah auf dem Bildschirm ziemlich gut aus: In einem Fenster seines Browsers waren Bilder seiner neugeborenen Tochter zu sehen; in einem anderen strömten die Tweets seiner tausenden Twitter-Follower. Als Reporter der Zeitschrift *Wired* in San Francisco lebte er ein urbanes und vernetztes Leben und war in Sachen Technik immer auf dem allerneuesten Stand. Trotzdem konnte er sich nicht vorstellen, dass seine digitale Welt mit ein paar Klicks ausgelöscht werden könnte. An einem Tag im August geschah es. Seine Fotos, E-Mails und vieles mehr fielen einem Hacker in die Hände. Gestohlen in wenigen Minuten von einem Teenager auf der anderen Seite des Erdballs. Honan war ein leichtes Ziel. Wie wir alle.

Honan erinnert sich an den Nachmittag, als alles zusammenbrach. Er spielte gerade auf dem Fußboden mit seiner kleinen Tochter, als plötzlich sein iPhone ausging. Vielleicht war der Akku leer. Er erwartete einen wichtigen Anruf, also steckte er das iPhone in die Station und fuhr es erneut hoch. Statt des üblichen Bildschirms mit seinen Apps erblickte er ein großes weißes Apple-Logo und eine mehrsprachige Anzeige, die ihn willkommen hieß und einlud, sein neues iPhone in Betrieb zu nehmen. Wie seltsam.

Honan war unbesorgt: Er machte allabendlich ein Backup seines iPhones. Sein nächster Schritt war daher logisch – sich in die iCloud einloggen und das iPhone mitsamt den Daten neu laden. Beim Einloggen in seinen Apple-Account teilte man ihm jedoch mit, dass sein Passwort, das er ganz sicher richtig eingegeben hatte, von den iCloud-Göttern für falsch befunden worden sei.

Honan, ein cleverer Journalist der wichtigsten Technologie-Zeitschrift der Welt, hatte freilich noch einen anderen Trick auf Lager. Er würde das iPhone einfach mit seinem Laptop verbinden und die Daten von der Festplatte seines Computers laden. Was als nächstes geschah, ließ ihm das Herz sinken.

Als Honan seinen Mac hochfuhr, wurde er von einer Nachricht des Apple-Kalenderprogramms begrüßt, die ihn darüber in Kenntnis setzte, dass sein Gmail-Passwort inkorrekt sei. Sofort danach wurde der Bildschirm seines Laptops – sein hübsch gestalteter Desktop – aschgrau und verschwand, als wäre er gestorben. Das Einzige, was auf dem Bildschirm noch zu sehen war, war eine Aufforderung: Bitte geben Sie Ihr vierstelliges Passwort ein. Honan war sicher, dass er nie ein Passwort gesetzt hatte.

Schließlich erfuhr er, dass sich ein Hacker Zugang zu seinem iCloud-Account verschafft und dann die praktische Apple-Funktion »Mein iPhone suchen« benutzt hatte, um sämtliche elektronischen Geräte in Honans Welt zu lokalisieren. Eines nach dem Anderen wurde unter Beschuss genommen. Mit der »Remote-Wipe-Funktion« löschte der Hacker sämtliche Daten, die Honan in seinem Leben angesammelt hatte. Erstes Opfer war das iPhone, dann das iPad. Last, aber ganz bestimmt nicht least, war das MacBook an der Reihe. In einem einzigen Augenblick waren sämtliche Daten gelöscht, darunter alle Babyfotos, die Honan im ersten Lebensjahr seiner Tochter gemacht hatte. Ebenfalls verloren waren die unersetzlichen fotografischen Erinnerungen an längst verstorbene Verwandte, verpufft im Äther durch die Hand eines unbekannten Dritten.

Nächstes Angriffsziel war Honans Google-Account. Mit einem Wimpernschlag waren die acht Jahre sorgsam gepflegter E-Mails verloren. Berufliche Korrespondenzen, Notizen und Erinnerungen wurden mit einem einzigen Mausklick gelöscht. Schließlich wandte der Hacker seine Aufmerksamkeit seinem ultimativen Ziel zu: Honans Twitter-Account, @Mat. Dieser wurde nicht nur geknackt, sondern von dem Hacker dazu missbraucht, in Honans Namen rassistische und homophobe Beschimpfungen an seine tausenden Follower zu verschicken.

Nach diesem Online-Anschlag nutzte Honan seine Fähigkeiten als investigativer Journalist, um herauszufinden, was sich ereignet hatte. Er wollte versuchen, seinen iCloud-Account zu retten, und rief beim technischen Support von Apple an. Nach einem über 90-minütigen Gespräch erfuhr er, dass »er« gerade 30 Minuten zuvor angerufen und verlangt habe, dass man sein Passwort zurücksetze. Wie sich herausstellte, wurden zum Ändern von Honans Passwort lediglich seine Rechnungsadresse und die letzten vier Ziffern seiner Kreditkartennummer abgefragt. Honans Adresse war über den Abfragedienst Whois frei zugänglich, da er sie beim Einrichten seiner privaten Website eingegeben hatte. Selbst, wenn das fehlgeschlagen wäre, hätte man sie sich über Dutzende anderer Online-Dienste wie etwa WhitePages oder Spokeo leicht besorgen können.

Beim Erschleichen der letzten vier Ziffern von Honans Kreditkartennummer

ging der Hacker davon aus, dass Honan (wie die meisten von uns) über ein Amazon-Konto verfügte. Er hatte recht. Ausgestattet mit Honans echtem Namen, seiner E-Mail- und Rechnungsadresse, setzte sich der Übeltäter mit Amazon in Verbindung, täuschte erfolgreich einen Kundendienstmitarbeiter und erhielt schließlich Zugang zu den erforderlichen letzten vier Stellen der Kreditkartennummer. Diese einfachen Schritte und nichts weiter stellten Honans gesamtes Leben auf den Kopf. Wenngleich es in diesem Fall nicht geschah, hätte der Hacker mit denselben Informationen ebenso leicht auch Honans Bank- und Wertpapierkonten knacken und plündern können.

Der Teenager, der sich schließlich mit dem Angriff brüstete – Phobia, wie er in Hackerkreisen genannte wurde –, behauptete, es sei ihm darum gegangen, die gewaltigen Sicherheitslücken der Internetdienste aufzuzeigen, die wir täglich bedenkenlos nutzten. Das war ihm gelungen. Honan eröffnete einen neuen Twitter-Account, um mit seinem Feind zu kommunizieren. Phobia, der dazu den Account @Mat benutzte, willigte ein, Honans neuem Account zu folgen, so dass die beiden sich nun gegenseitig Botschaften schicken konnten. Honan stellte Phobia die Frage, die ihm auf der Seele brannte: Warum? Warum hast du mir das angetan? Wie sich herausstellte, waren die in fast zehnjähriger Kleinarbeit gesammelten Daten lediglich ein Kollateralschaden.

Phobias Antwort war schaurig: »Ehrlich, ich habe nichts gegen Dich persönlich … Mir gefiel einfach Dein [Twitter-] Nutzername.« Das war es also. Das war der ganze Grund – ein begehrter Twitter-Name mit drei Zeichen. Ein tausende Kilometer entfernter Hacker fand ihn gut und wollte ihn schlicht für sich selbst haben.

Der Gedanke, dass jemand, der »nichts gegen einen hat«, mit wenigen Klicks ein ganzes digitales Dasein auslöscht, ist absurd. Als Honans Geschichte im Dezember 2012 als Titelstory in *Wired* erschien, sorgte sie für einiges Aufsehen … eine oder zwei Minuten lang. Eine Debatte darüber, wie sich unsere Alltagstechnologien sicherer machen ließen, folgte zwar, verebbte aber bald wieder. Seit Honans Irrungen und Wirrungen hat sich herzlich wenig getan. Wir sind immer noch genauso angreifbar, wie es Honan damals war – und sogar noch mehr, weil wir inzwischen auch von mobilen und Cloud-basierten Anwendungen abhängig sind.

Wie bei den meisten von uns, waren auch Honans zahlreiche Accounts in einem selbstreferenziellen Netz falschen digitalen Vertrauens miteinander verbunden: dieselbe Kreditkartennummer im Apple-Profil und im Amazon-Konto; eine iCloud-Mailadresse, die auf Gmail verwies. Alle hatten bestimmte Informationen gemein, darunter Login-Daten, Kreditkartennummern und Passworte.

Sämtliche Daten waren mit ein und derselben Person verbunden. Honans Sicherheitsmaßnahmen waren insgesamt nicht mehr als eine digitale Maginot-Linie – ein instabiles Kartenhaus, das beim leichtesten Stoß in sich zusammenfiel. Alle oder zumindest die meisten Informationen, die es bedurfte, um sein (oder unser) digitales Leben zu vernichten, sind für jedermann, der auch nur ein klein wenig geschickt oder kreativ ist, online offen zugänglich.[1]

Fortschritt und Risiken in einer vernetzten Welt

Vor wenigen Jahren noch war Google für uns lediglich eine Suchmaschine, von der wir uns inzwischen aber Hals über Kopf abhängig gemacht haben, ohne lange darüber nachzudenken. Heute nutzen wir Google für Karten, Kalender, Adressen, Videos, Unterhaltung, Voicemail und Telefonate. Eine Milliarde Menschen hat ihre intimsten Details auf Facebook ausgebreitet und willig das Surfverhalten ihrer Freunde, Verwandten und Kollegen in sozialen Netzwerken offengelegt. Wir haben Milliarden von Apps heruntergeladen und nutzen sie für Geldgeschäfte, beim Kochen oder zum Archivieren von Babybildern. Über unsere Laptops, Handys, iPads, TiVos, Kabelanschlüsse, PS3s, Blu-Rays, Nintendos, HDTVs, Rokus, Xboxen und Apple-TVs verbinden wir uns mit dem Internet.

Die positiven Aspekte der technologischen Evolution sind offenkundig. Während der vergangenen 100 Jahre bewirkte ein rasanter medizinischer Fortschritt, dass sich die durchschnittliche Lebenserwartung eines Menschen mehr als verdoppelte und die Kindersterblichkeit um einen Faktor zehn zurückging.[2] Das durchschnittliche, inflationsbereinigte Pro-Kopf-Einkommen hat sich weltweit verdreifacht. Der Zugang zu qualitativ hochwertiger Bildung, für viele lange ein Traum, ist dank Webseiten wie der Khan Academy heute kostenlos. Das Mobiltelefon schließlich bescherte Nationen rund um den Erdball einen milliardenschweren wirtschaftlichen Aufschwung.[3]

Die grundlegende Architektur des Internets bietet die Möglichkeit einer globalen Vernetzung, durch welche unterschiedlichste Völker auf der ganzen Welt wie nie zuvor miteinander in Kontakt treten können. Eine Frau in Chicago kann mit einem völlig Fremden in den Niederlanden »Words with Friends« spielen. Ein Arzt im indischen Bangalore kann die Röntgenbilder eines Patienten in Boca Raton, Florida, studieren und interpretieren. Ein Bauer in Südafrika hat über sein Handy Zugang zu denselben landwirtschaftlichen Daten wie ein Doktorand am MIT. Diese Vernetzung ist eine der größten Stärken des Internets,

das mit zunehmender Größe auch immer mächtiger und nützlicher wird. In unserer modernen, technisierten Welt gibt es viel zu feiern.

Während die Vorzüge der Online-Welt von den Vertretern der Technologiebranche bestens dokumentiert und regelmäßig gepriesen werden, gibt es freilich auch eine Kehrseite dieser weltweiten Vernetzung.

Unsere Stromnetze, Luftverkehrskontrollnetze, Feuerwehrleitsysteme und selbst unsere Fahrstühle werden allesamt von Computern gesteuert. Das allein ist kritisch. Obendrein machen wir unser Leben Tag für Tag abhängiger vom globalen Informationsnetz, ohne lange zu überlegen, welche Folgen das für uns haben könnte. Was aber würde geschehen, wenn die technischen Errungenschaften, denen wir uns auf Gedeih und Verderb verschrieben haben, die Grundfesten unserer modernen Gesellschaft, plötzlich verschwänden? Wie sieht der Notfallplan der Menschheit aus? Die Wahrheit ist: Es gibt keinen.

Die Erde ist flach (und steht allen offen)

Jahrhundertelang war das westfälische System souveräner Nationalstaaten weltweit vorherrschend.[4] Es bedeutete, dass Länder auf ihrem Territorium die Hoheitsrechte ausübten und sich äußere Kräfte nicht in die inneren Angelegenheiten einer Nation einzumischen hatten. Die westfälische Struktur wurde durch ein System aus Grenzen, Armeen, Wächtern, Toren und Schusswaffen gesichert. Sowohl die Immigration von Fremden als auch die Emigration von Menschen aus dem Gebiet eines Nationalstaates wurde scharf kontrolliert. Daneben errichtete man Zoll- und Kontrollstrukturen, um den Güterstrom über die nationalen Grenzen zu steuern und zu begrenzen. Doch so weitsichtig die Unterzeichneten des Westfälischen Friedens im Jahre 1648 auch waren, so sah doch keiner von ihnen Snapchat voraus.

Physische Grenzen spielen zwar immer noch eine Rolle, doch in einer Online-Welt verschwimmen solche Trennlinien. Bits und Bytes fließen ungehindert von einem Land zum anderen, ohne dass Grenzkontrollen, Einwanderungsgesetze oder Zollbehörden ihren Transit behindern. Die traditionellen transnationalen Verbrechensbarrieren, mit denen sich frühere Generationen von Dieben, Ganoven und Zuchthäuslern konfrontiert sahen, sind in der Online-Welt niedergerissen worden, sodass zwielichtige Elemente jeden virtuellen Ort nach Belieben aufsuchen und verlassen können.

Man muss sich einmal vergegenwärtigen, welche Auswirkungen das auf unsere Sicherheit hat. Wenn Kriminelle früher eine Bank am New Yorker Times

Square auszurauben versuchten, galten bestimmte Dinge dabei als unumstößlich. Zunächst einmal war klar, dass die Verbrecher einen physischen Ort im Midtown South Precinct, also innerhalb des Zuständigkeitsbereiches der New Yorker Polizei aufgesucht hatten. Der Bankraub stellte eine Verletzung sowohl von US-Bundesrecht als auch der Gesetze des Staates New York dar, also mussten das NYPD und das FBI auf Grundlage bestehender Gesetze gemeinsam in dem Fall ermitteln. Das Opfer (in diesem Falle die Bank) war ebenfalls im Zuständigkeitsbereich beider Strafverfolgungsbehörden ansässig, was deren Ermittlungsarbeit stark vereinfachte. Bei der Falllösung hätte man sich auf physische Beweise gestützt, die der Bankräuber vermutlich am Schauplatz des Verbrechens hinterlassen hätte, etwa Fingerabdrücke auf einem Zettel für den Kassierer oder die DNA auf einer Theke, über die er gesprungen wäre. Vielleicht hätte das Kamera-Überwachungssystem der Bank sogar Aufnahmen seines Gesichts geliefert. Zudem unterlag auch der Kriminelle selbst gewissen physischen Beschränkungen. Die entwendeten Dollarnoten besaßen ein bestimmtes Gewicht, also konnte man nur eine begrenzte Menge davon aus der Bank schaffen. Vielleicht wäre in den Geldbündeln auch ein explodierender Farbbeutel versteckt gewesen, der den Verdächtigen für die Polizei kenntlich gemacht hätte. Althergebrachte, bewährte Grundpfeiler der Ermittlungsarbeit wie etwa eine gemeinsame Zuständigkeit oder das physische Beweismittel – für die Behörden unverzichtbare Werkzeuge bei der Verbrechensbekämpfung – gibt es in der heutigen Welt jedoch häufig nicht mehr.

Vergleichen wir obiges Times-Square-Szenario mit dem berüchtigten Internet-Raub von 1994, den der Russe Wladimir Levin von seiner Wohnung in St. Petersburg aus verübte. Levin, ein Computerprogrammierer, wurde beschuldigt, die Accounts mehrerer großer Unternehmenskunden der Citibank gehackt und dabei 10,7 Millionen Dollar erbeutet zu haben.[5] Zusammen mit Komplizen auf der ganzen Welt hatte Levin große Summen auf Konten in Finnland, den Vereinigten Staaten, den Niederlanden, Deutschland und Israel transferiert.

Wer war in diesem Fall zuständig? War es die Polizei der Vereinigten Staaten, wo das Opfer (die Citibank) ansässig war? Waren es die Behörden in St. Petersburg, wo der Beschuldigte das ihm zur Last gelegte Verbrechen begangen hatte? Oder lag die Zuständigkeit vielleicht bei Israel oder Finnland, wohin die riesigen Summen auf betrügerische Konten elektronisch überwiesen wurden? Um das Verbrechen zu begehen, hatte Levin die Vereinigten Staaten physisch nie betreten. Er hinterließ keine Fingerabdrücke oder DNA und wurde nie durch einen explodierenden Farbbeutel markiert. Er musste auch keine tausende Kilo schweren Geldscheinbündel aus der Bank schleppen; für das Ganze brauchte er

lediglich eine Maus und eine Tastatur. Eine Maske oder eine abgesägte Schrotflinte waren ebenfalls unnötig; Levin versteckte sich einfach hinter seinem Computerbildschirm und schlug auf der Flucht virtuelle Haken, um seine digitalen Spuren zu verwischen.

Das Wesen des Internets bringt es mit sich, dass wir in einer zunehmend grenzenlosen Welt leben. Heute kann jeder, ob in guter oder schlechter Absicht, mit Lichtgeschwindigkeit virtuell um den halben Planeten rasen. Für Kriminelle ist diese Technologie ein wahrer Segen, da sie sich nun von einem Land zum anderen ihren virtuellen Weg um den Globus hacken, sehr zur Frustration der Polizei. Außerdem haben die Kriminellen gelernt, sich selbst vor Verfolgung im Internet zu schützen. Ein geschickter Hacker würde niemals von seiner Privatwohnung in Frankreich aus eine Bank in Brasilien angreifen. Stattdessen würde er seine Cyberattacke über mehrere infizierte Netzwerke führen, etwa von Frankreich über die Türkei und Saudi-Arabien, und dann erst sein eigentliches Ziel in Brasilien ins Visier nehmen. Diese Möglichkeit, Ländergrenzen zu überspringen, eine der größten Stärken des Internets, bereitet der Polizei ungeheure Zuständigkeits- und Verwaltungsprobleme und ist einer der Hauptgründe dafür, dass die Verfolgung von Cyberkriminalität so schwierig und bisweilen so fruchtlos ist. Ein Polizist in Paris hat keinerlei Befugnis, eine Verhaftung in São Paulo vorzunehmen.

Die guten alten Zeiten der Cyberkriminalität

Das Wesen der Cyberbedrohung hat sich im Laufe der letzten 25 Jahre dramatisch gewandelt. In den Anfangstagen des PCs war Schadenfreude die Hauptmotivation der Hacker. Sie hackten Computersysteme, um ganz einfach zu zeigen, dass sie dazu in der Lage waren, oder um auf etwas Bestimmtes hinzuweisen. Eines der allerersten Computerviren, die IBM-PCs befielen, war das Brain-Virus, 1986 programmiert von den damals 24- und 17-jährigen Brüdern Amjad und Basit Faruk Alvi aus Lahore in Pakistan.[6] Ihr Virus sollte harmlos sein und lediglich andere davon abhalten, die Software zu kopieren, welche die beiden Brüder in jahrelanger Arbeit entwickelt hatten. Brain infizierte den Boot-Sektor einer Floppy Disk, um so deren illegales Kopieren zu verhindern, und erlaubte den Brüdern, illegale Kopien ihrer Software nachzuverfolgen. Aufgebracht darüber, dass andere ihre Software kopierten, ohne dafür zu bezahlen, bauten die Brüder noch eine ominöse Warnung ein, die auf den Bildschirmen infizierter Computer erschien:

Willkommen im Verlies © 1986 Brain & Amjads (pvt).
BRAIN COMPUTER SERVICES 730 NIZAM BLOCK ALLAMA IQBAL
TOWN LAHORE-PAKISTAN PHONE: 430791,443248,280530.
Vorsicht vor diesem VIRUS … Kontaktieren Sie uns wegen einer Impfung …

Diese Botschaft ist in mehrerlei Hinsicht bemerkenswert. Zunächst behaupteten die Brüder, ihren Virus urheberrechtlich geschützt zu haben – ein ziemlich kühner Schachzug. Noch seltsamer war, dass sie ihre Adresse und Telefonnummer angaben, damit sich Nutzer wegen einer »Impfung« oder der Beseitigung des Virus an dessen Schöpfer wenden konnten. Für Basit und Amjad war es eine folgerichtige Entscheidung, einen Virus in die Welt zu setzen, doch was sie dabei nicht bedacht hatten, war, dass ihre Schöpfung die Fähigkeit besaß, sich zu replizieren und zu verbreiten – was sie dann auf ganz altmodische Weise auch tat, nämlich durch Menschen, die Disketten von einem Computer zum anderen trugen. So reiste Brain schließlich um den gesamten Erdball und machte Basit und Amjad dem Rest der Welt bekannt.[7]

Mit der Zeit wurden die Hacker ehrgeiziger – oder boshafter, wie man es nimmt. Unsere Vernetzung untereinander über E-Mail-Dienste brachte es mit sich, dass digitale Viren nicht länger über ein sogenanntes »Sneakernet« – also von Menschenhand per Diskette – verbreitet werden mussten, sondern sich dank früher Dienste wie CompuServe, Prodigy, EarthLink und AOL via Modem über das Telefonnetz ausbreiten konnten. Neuere Viren und Trojaner wie Melissa (1999), ILOVEYOU (2000), Code Red (2001), Slammer (2003) und Sasser (2004) konnten nun problemlos weltweit das Betriebssystem Microsoft Windows infizieren und zerstörten dabei Studienarbeiten, Rezepte, Liebesbriefe und Unternehmenskalkulationen, die auf den jeweiligen Festplatten gespeichert waren. Plötzlich waren wir alle Teil dieses Spiels.

»Malware« (Schadsoftware), ein Begriff, der die Worte »mali-cious« (bösartig) und »Software« miteinander kombiniert, hat heutzutage vielgestaltige Erscheinungsformen, doch ist das Ziel stets, zu zerstören, zu verwirren und zu stehlen – oder einem Datensystem oder einem Netzwerk eine illegale oder nicht autorisierte Funktion unterzuschieben:

- Computerviren verbreiten sich, indem sie ein anderes Programm mit einer Kopie von sich selbst infizieren, also auf dieselbe Weise, wie ein echtes Virus einen biologischen Wirt befallen würde.
- Computerwürmer richten ebenfalls Schaden an, tun dies jedoch als eigenständige Software und benötigen kein fremdes Programm, um sich zu verbreiten.

- Trojaner, benannt nach dem Holzpferd, mit welchem die Griechen der Sage nach in Troja eindrangen, tarnen sich oft als legitime Software und werden aktiviert, wenn ein Nutzer sich dazu verleiten lässt, die Programmdateien auf ein Zielsystem zu laden und dort auszuführen. Trojaner erzeugen regelmäßig »Hintertüren«, die Hackern den dauerhaften Zugriff auf ein infiziertes System erlauben. Trojaner reproduzieren sich nicht dadurch, dass sie andere Programme infizieren, sondern verbreiten sich erst dann, wenn Nutzer eine Datei anklicken oder einen infizierten E-Mail-Anhang öffnen.

Virusautoren wissen heute, dass die Öffentlichkeit allmählich (ganz allmählich) begreift, dass man von Fremden geschickte Dateien besser nicht anklicken sollte. Folglich haben Kriminelle ihre Taktiken erneuert und sogenannte Drive-by-Downloads entwickelt, die Malware verwenden, um sich Schwächen in Computerskripten wie Java oder ActiveX zunutze machen, gängige Programmiersprachen in Internet-Browsern.

Die Welt ist online gegangen, und Tools wie Internet Explorer, Firefox und Safari zu hacken, lohnt sich für Kriminelle. Der neue modus operandi kommt die arglosen Nutzer teuer zu stehen. Forscher von Palo Alto Networks stellten fest, dass bis zu 90 Prozent aller modernen Schadsoftware über zuvor gehackte beliebte Websites verbreitet wird, welche die Infektion in dem Augenblick weitergeben, in dem ein argloser Nutzer die betreffende Seite besucht.[8] Die Websites vieler großer Unternehmen, darunter auch von Yahoo!, einem der weltweit führenden Webportale, wurden von Kriminellen gekapert, sodass die Anbieter ihre eigenen Kunden vergifteten, wenn diese gutgläubig vorbeischauten, um sich über Sportergebnisse oder die neuesten Börsennachrichten zu informieren.[9]

Die Malware-Explosion

Inzwischen geht es im Hackergeschäft nicht mehr nur um Schadenfreude, sondern längst um Geld, Informationen und Macht. Anfang des 21. Jahrhunderts ersannen Kriminelle Mittel und Wege, ihre bösartige Software zu Geld zu machen, etwa durch Identitätsdiebstahl und andere Methoden. Immer neue Viren tauchten auf. Im Jahre 2015 ist deren Anzahl beängstigend. Das Deutsche Forschungsinstitut AV-Test schätzte 2010, dass an die 49 Millionen Malware-Programme im Umlauf seien.[10] Im Jahr darauf berichtete das Antivirus-Unternehmen McAfee, es entdecke Monat für Monat zwei Millionen neuer Malware-Files.

Im Sommer 2013 gab die Cybersicherheitsfirma Kaspersky bekannt, dass sie jeden Tag fast 200 000 neue Malware-Programme identifiziere und isoliere.[11]

Betrachtet man diese Statistiken mit einem gewissen Zynismus und geht davon aus, dass die Antivirus-Unternehmen das Problem, dessen Bekämpfung ihr Geschäft ist, naturgemäß vielleicht ein wenig übertreiben, ist man versucht, diese Zahlen dramatisch herunterzurechnen – sagen wir, um 50 oder sogar 75 Prozent. Das würde trotzdem noch bedeuten, dass täglich 50 000 neue Viren in Umlauf kommen. Man stelle sich nur vor, welch gewaltigen Forschungs- und Entwicklungsaufwand es auf globaler Ebene erfordert, diese Masse eigens programmierter Schadsoftware zu schaffen. Wie jeder Geschäftsmann weiß, sind Forschung und Entwicklung eine kostspielige Angelegenheit. Daher müssen die Erträge, die das internationale organisierte Verbrechen aus seiner Investition in illegale Software zieht, gewaltig sein. Eine unabhängige Studie der zuverlässigen Consumers Union, die auch die Zeitschrift *Consumer Reports* herausgibt, scheint die wachsende Bedrohung durch Computer-Malware zu bestätigen. Eine Erhebung unter den Mitgliedern ergab, dass ein Drittel aller Haushalte in den Vereinigten Staaten im vergangenen Jahr Probleme mit einer Schadsoftwareinfektion gehabt hatte. Die Verbraucher kostet die Angelegenheit schwindelerregende 2,3 Milliarden Dollar pro Jahr.[12] Wohlgemerkt: Das bezieht sich nur auf diejenigen, die einen Cyberangriff überhaupt entdecken.

Die Illusion von Sicherheit

Jedes Jahr setzen Verbraucher und Geschäftsleute auf der ganzen Welt ihr Vertrauen in die Softwareindustrie, die sie vor der wachsenden Bedrohung durch Schadsoftware schützen soll. Einer Studie der Gartner-Gruppe zufolge beliefen sich die weltweiten Ausgaben für Sicherheitssoftware im Jahre 2012 insgesamt auf fast 20 Milliarden Dollar.[13] Bis 2017 wird eine Erhöhung dieser jährlich aufgewendeten Summe auf 94 Milliarden prognostiziert.

Wenn man Menschen nach Computerviren fragt, lautet die Antwort meist, dass sie ein Antivirus-Produkt aus dem Hause Symantec, McAfee oder Trend Micro verwenden. Es ist die instinktive Antwort einer gut geschulten Öffentlichkeit. Zwar mögen sich solche Werkzeuge in der Vergangenheit als durchaus hilfreich erwiesen haben, doch werden sie zunehmend ineffizienter. Die Statistiken hierzu sprechen eine klare Sprache. Im Dezember 2012 beschlossen Wissenschaftler von Imperva, einem im kalifornischen Redwood Shores ansässigen Unternehmen aus dem Bereich der Data-Center-Security, und Studenten

des Technion – Israel Institute of Technology, die verbreiteten Antivirus-Programme unter die Lupe zu nehmen. Sie sammelten 82 Computerviren und testeten die Schadsoftware gegen die Abwehrprogramme von über 40 der weltgrößten Antivirus-Anbieter, darunter Microsoft, Symantec, McAfee und Kaspersky Lab. Das Ergebnis: Die Erkennungsrate lag bei gerade einmal fünf Prozent, was bedeutete, dass 95 Prozent aller Schadsoftware vollkommen unentdeckt geblieben war.[14] Es bedeutet auch, dass die Antivirus-Software, die Sie auf ihrem Computer installiert haben, nur fünf Prozent aller Bedrohungen erkennt, die gegen Ihr Gerät gerichtet sind. Wenn das Immunsystem Ihres Körpers eine ähnliche Erfolgsquote hätte, wären Sie innerhalb weniger Stunden tot.

Monate später aktualisieren die Giganten der Sicherheits-Softwarebranche schließlich ihre Programme, doch ist es dann häufig schon zu spät. Die Wahrheit ist, dass Kriminelle und Virusautoren der einst zu unserem Schutz errichteten Antivirus-Industrie um Längen voraus sind. Schlimmer noch ist, dass die Zeit immer länger wird, die es braucht, bis eine neu in Umlauf gebrachte Schadsoftware erstmals erkannt wird. So entdeckten Forscher des Kaspersky Lab in Moskau 2012 eine hochkomplexe, bis dato unbekannte Schadsoftware namens Flame, die bereits seit über fünf Jahren weltweit Daten aus Informationssystemen gestohlen hatte. Mikko Hypponen, der hochangesehene Forschungsleiter der IT-Sicherheitsfirma F-Secure, bezeichnete Flame als Versagen der Antivirus-Industrie und stellte fest, dass ihm und seinen Kollegen möglicherweise »unser eigenes Spiel eine Nummer zu groß« geworden sei. Obwohl sich auf der ganzen Welt Millionen auf diese Tools verlassen, ist doch ziemlich eindeutig, dass die Antivirus-Ära vorbei ist.[15]

Einer der Gründe, warum es sich als immer schwieriger erweist, der großen Bandbreite technologischer Bedrohungen in unserem heutigen Leben zu begegnen, ist, dass die Anzahl sogenannter Zero-Day-Attacken eklatant zugenommen hat. Eine Zero-Day-Attacke, auch Exploit genannt, nutzt eine bis dato unbekannte Schwachstelle in einer Computeranwendung, die Entwickler und Sicherheitsleute noch nicht beseitigt haben. Statt proaktiv selbst nach solchen Schwachstellen zu suchen, berücksichtigen Antivirus-Softwarefirmen in der Regel nur bekannte Datenpunkte. Sie blockieren einen bösartigen Code dann, wenn er ebenso aussieht wie die anderen bösartigen Codes, die sie bereits kennen. Das ist ungefähr so, als hängte man ein Suchplakat von Bonnie und Clyde auf, weil man weiß, dass die beiden schon Banken ausgeraubt haben. Die Bankangestellten wären somit gewarnt, dass sie vor den beiden auf der Hut sein müssten, doch solange niemand auftauchte, auf den diese Beschreibung zuträfe, wären sie möglicherweise nicht so wachsam – bis ein anders aussehender

Bankräuber zuschlüge. Zero-Day-Attacken werden zunehmend für die große Bandbreite von Technologieprodukten entwickelt, die wir tagtäglich nutzen. Betroffen ist alles von Microsoft Windows über Linksys-Router bis hin zum omnipräsenten PDF Reader oder Flash Player von Adobe.

Die Hacker kamen schließlich darauf, dass, je mehr Lärm sie dabei veranstalteten, in unsere Computersysteme einzudringen, wir umso schneller dass Problem behoben und sie wieder hinauswarfen. Schlau, wie sie sind, arbeiten sie heute daher im Geheimen, als hätte man eine Schläferzelle in seinem Computer. Man könnte nun denken, die Virus-Erkennungsquote von mageren fünf Prozent gälte nur für den Durchschnittsbürger, der zu Hause ein PC-Sicherheitsprogramm installiert hat. Unternehmen mit riesigen Budgets für Informationstechnologie und deren Sicherheit sind gegen Hacker bestimmt wesentlich besser gerüstet! Nicht wirklich. Zehntausende erfolgreicher Angriffe auf Konzerne, große Nichtregierungsorganisationen und Regierungen auf der ganzen Welt zeigen, dass selbst hohe Aufwendungen für den Schutz wertvoller Informationen nur eine relativ geringe Wirkung zeigen.

Aus dem *Data Breach Investigations Report* von Verizon aus dem Jahre 2013 geht hervor, dass die meisten Unternehmen schlicht nicht in der Lage waren, einen illegalen Zugriff auf ihre Informationssysteme festzustellen. Die wegweisende Studie, die Verizon in Zusammenarbeit mit dem US-Geheimdienst, der Polizei der Niederlande und der Spezialeinheit für sogenannte E-Crimes der britischen Polizei erstellt hatte, besagte, dass es in durchschnittlich 62 Prozent aller Angriffe auf Unternehmen mindestens zwei Monate dauere, bis diese bemerkt würden.[16] Eine vergleichbare Studie von Trustwave Holdings offenbarte, dass zwischen dem Eindringen in ein Unternehmensnetzwerk und dessen Entdeckung im Schnitt 210 Tage vergingen.[17] Damit bleiben dem Angreifer – ob er nun dem organisierten Verbrechen, der Konkurrenz oder einer fremden Regierung angehört – fast sieben Monate Zeit, in denen er ungehindert sein Unwesen in diesem Netzwerk treiben kann; Zeit, um Geheimnisse und wettbewerbsrelevantes Unternehmenswissen zu stehlen, Finanzsysteme zu knacken und sich persönliche Kundendaten anzueignen, etwa Kreditkartennummern.

Wenn ein Unternehmen dann irgendwann doch erkennt, dass es eine digitale Laus in seinem Pelz hat und wichtige Daten gestohlen wurden, sind es zu 92 Prozent leider nicht die Chef-Sicherheitsbeauftragten, das Sicherheitsteam oder der Systemadministrator, die den Fremdzugriff feststellen.[18] Vielmehr setzen die Polizei, ein erboster Kunde oder ein Vertragspartner das Opfer über das Problem in Kenntnis. Wenn die größten Unternehmen der Welt – Firmen, die zusammen Millionen für ihre Cyberabwehr ausgeben und ganze Abteilungen

unterhalten, in denen Profis rund um die Uhr ausschließlich mit dem Schutz ihrer Netzwerke beschäftigt sind – derart leicht von Hackern angegriffen werden können, dann sind die Aussichten für den Schutz privater Daten am heimischen PC in der Tat düster.

Wie schwer ist es, sich in ein durchschnittliches Computersystem einzuhacken? Lächerlich einfach. Der Verizon-Studie zufolge lassen sich sämtliche Sicherheitsschranken innerhalb weniger Minuten überwinden, wenn ein Hacker ein Netzwerk erst einmal aufs Korn genommen hat. Dieselbe Studie kommt zu dem Schluss, dass es nur in 15 Prozent aller Fälle länger als ein paar Stunden dauert, um ein System zu knacken. Diese Erkenntnisse lassen einen beängstigenden Rückschluss zu: Von dem Zeitpunkt an, in dem sich ein Hacker Ihre Welt als Angriffsziel wählt, ist das Spiel in 75 Prozent aller Fälle innerhalb weniger Minuten vorbei.[19] Man erhält einen Schlag, wird k. o. geschlagen und geht zu Boden, bevor man noch weiß, was einen da getroffen hat. In der heutigen Welt bewegen sich Hacker monatelang unbeirrt in fremden Datensystemen, beobachten, warten, lauern und plündern alles von Passwörtern über Arbeitsprojekte bis hin zu alten Selfies. Sie und ich sind ein leichtes Ziel. Seltsam, dass wir das als Gesellschaft so einfach hinnehmen. Wenn wir einen Einbrecher im Haus bemerken würden, der uns beim Schlafen beobachtete oder beim Duschen filmte, würden wir sofort die Polizei rufen (oder schreien und zur Schusswaffe greifen). Im Cyberspace ist das an der Tagesordnung, doch die meisten Menschen regen sich nicht auf, sind sich der Bedrohung oft sogar nicht einmal bewusst – trotz aller Risiken und der Tatsache, dass uns die Bösewichte im Schlaf belauern.

Die Kosten für unsere Cybersicherheit schießen weiter in die Höhe. Für Sicherheitsmaßnahmen in Hard- und Software werden Unternehmen weltweit bis 2017 zwar voraussichtlich 100 Milliarden Dollar ausgeben, doch ist diese Summe kaum mehr als ein Anfang, wenn man sich das volle ökonomische Risiko der technologischen Angreifbarkeit vergegenwärtigt. Nehmen wir zum Beispiel den 2007 festgestellten Cyberangriff auf TJX, das Mutterunternehmen der Einzelhandelsketten T. J. Maxx und Marshalls in den Vereinigten Staaten und T. K. Maxx in Europa.[20]

In diesem Fall eigneten sich Hacker die Kreditkartendaten von über 45 Millionen Kunden an, damals der bis dato größte Cyberraubzug gegen ein Einzelhandelsunternehmen.[21] Vor Gericht stellte sich später heraus, dass sogar fast 94 Millionen Opfer betroffen waren.[22] TJX erreichte zwar einen Vergleich mit Visa, MasterCard und seinen Kunden in Höhe von 256 Millionen Dollar, doch glauben viele Analysten, dass die tatsächlichen Kosten leicht die Milliarden-

grenze erreicht haben könnten. Eine der zuverlässigsten Quellen, wenn es um die Kosten von Datenklau geht, ist das Ponemon Institute, das unabhängige Studien zu Datenschutz und Informations-Sicherheitspolitik durchführt.[23] Bei der Berechnung von Verletzungen der Cybersicherheit, so das Institut, sei es wichtig, die Verlustanalyse weit über die direkten Diebstähle bei den Kunden hinaus auszuweiten.

Wenn ein Unternehmen wie TJX Opfer eines Angriffs wird, muss es eine ganze Menge Geld ausgeben, um die Sicherheitslücke festzustellen, die Angreifer in Schach zu halten, den Fall zu untersuchen, die Eindringlinge zu identifizieren und schließlich das Computernetzwerk zu reparieren und auszubessern. Darüber hinaus entstehen häufig große Verkaufsrückgänge, wenn eine misstrauische Öffentlichkeit davor zurückschreckt, die Dienste eines als unsicher gebrandmarkten Unternehmens weiter in Anspruch zu nehmen. Dazu kommen noch die Kosten für Kreditkarten-Ersatzgebühren (die in den USA momentan bei etwas über fünf Dollar pro Karte liegen), eine neue Überwachung des Zahlungsverkehrs, die das Opfer einrichten lassen muss, um weiteren Kreditkartenbetrug zum Schaden seiner Kundschaft zu verhindern, sowie erhöhte Versicherungsprämien – man sieht, wie schnell in einem solchen Fall die Kosten eskalieren können.[24] Kein Wunder also, dass die meisten Unternehmen nur äußerst ungern zugeben, gehackt worden zu sein, und viele versuchen, eine solche Angelegenheit möglichst lange zu leugnen.

Wir geben große Summen für weitgehend ineffektive Vorbeugungsmaßnahmen aus und reagieren in der Regel erst, wenn es bereits zu spät ist (und die Hacker sich unserer Systeme bemächtigt haben). Als Gesellschaft zahlen wir einen hohen Preis für unsere mangelnde technologische Sicherheit. Unsere wachsende Vernetzung und die damit einhergehende Abhängigkeit von vollkommen ungeschützten Technologien kann sich auf eine Art und Weise rächen, die weit mehr als nur unseren Geldbeutel betrifft.

Das Internet hat seine Unschuld verloren. Unsere klein gewordene Welt der Datenautobahnen wird zu einem immer gefährlicheren Ort, und je mehr wir angreifbare Technologien in unserem Alltag verwenden, desto verwundbarer werden wir. Die nächste industrielle Revolution, die Informationsrevolution, ist bereits im Gange – mit Auswirkungen für unsere persönliche und globale Sicherheit in noch ungeahntem Ausmaß. Der Einzelne, Organisationen und selbst unsere wichtigsten Infrastrukturen scheinen gegen diese Bedrohung machtlos; und doch verlässt der sprichwörtliche Zug der Technik den Bahnhof und gewinnt laufend an Fahrt. Anzeichen dafür gibt es überall, wenn man weiß, wo man suchen muss.

Gleich hinterm Horizont warten neue Technologien wie die Robotik, künstliche Intelligenz, Gentechnik, synthetische Biologie, Nanotechnologie, 3-D-Produktion, Kognitions- und Neurowissenschaften und virtuelle Realität, die unsere Welt verändern werden und eine ganze Palette an Sicherheitsrisiken bergen, neben denen die heutige Cyberkriminalität wie ein Kinderspiel aussehen wird. Diese Innovationen werden in nur wenigen Jahren eine bedeutende Rolle in unserem Alltag spielen, und doch gibt es noch keine vollständige, umfassende Studie dazu, wie wir mit den damit einhergehenden Risiken umgehen sollen.

Das Ausmaß dieses tiefgreifenden Wandels und seiner Begleitrisiken ist den meisten Menschen bislang verborgen geblieben, doch ehe wir's uns versehen, wird unsere globale Gesellschaft eine Billion neue Endgeräte mit dem Internet verbunden haben – Geräte, die jeden Aspekt unseres Lebens durchdringen werden. Diese dauerhaften Verbindungen werden, zum Guten wie zum Schlechten, weltweit eine beiderseitige Abhängigkeit von Mensch und Maschine schaffen und ein fester Bestandteil unserer Alltagserfahrung werden.

Als Folge davon wird es bei der Technologie nicht mehr allein um Maschinen gehen; sie wird zum Lebensstrang unseres Daseins selbst werden. Diejenigen, die wissen, wie die allem zugrundeliegenden Technologien funktionieren, werden sie immer geschickter zu nutzen verstehen – zu ihrem Vorteil und, wie bereits zu sehen war, zum Nachteil des kleinen Mannes. Das Füllhorn der Technologie, dem wir mehr oder weniger sorg- und kritiklos Einlass in unser Leben gewährt haben, könnte zur Stolperfalle für uns werden. Dieses Risiko macht die neue Normalität aus – eine Zukunft, auf die wir völlig unvorbereitet zusteuern. Dies ist ein Buch über Mensch und Maschine und darüber, wie der Sklave zum Herrn werden könnte.