DIGITAL KRIMINELL MENSCHLICH

EINE CYBER-STAATSANWÄLTIN ERMITTELT

JANA RINGWALD

MURMANN

DIGITAL
KRIMINELL
MENSCHLICH

JANA
RINGWALD

DIGITAL KRIMINELL MENSCHLICH

EINE CYBERSTAATSANWÄLTIN ERMITTELT

MURMANN

INHALT

VORAB

Mein Name ist Jana Ringwald.
Ich bin Cyberstaatsanwältin.

Mein Beruf spielt sich im Verborgenen ab. Die Staatsanwaltschaft ist eine Behörde, die sich mit der kriminellen Welt anlegt.

Es ist meine persönliche Entscheidung, über meinen Beruf zu sprechen. Ich achte und respektiere, dass andere dies nicht tun.

Dieses Buch ist meinem Leben als Cyberstaatsanwältin entlehnt. Es gibt meine Erfahrungen wieder, meine Ansichten und meinen Blick auf die Geschehnisse, die weit über den einzelnen Fall hinausreichen.

Eine Staatsanwältin ist zur Verschwiegenheit verpflichtet. Sie darf in der Öffentlichkeit nur über Angelegenheiten ihrer beruflichen Tätigkeit sprechen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Aus diesem Grund werde ich keine Namen nennen und Erlebtes, das außerhalb der Presseberichterstattung oder der öffentlichen Hauptverhandlung stattfand, in einer Weise erzählen, die den tatsächlichen Geschehnissen gerecht wird, ohne sie im Detail preiszugeben.

Was kann man dann noch erzählen?
Eine ganze Menge.
Denn dieses Buch enthüllt nicht meinen Beruf.
Es erzählt meinen Weg.

PROLOG

Es gibt eine Veränderung, die jeder von uns täglich zu leisten hat. Es ist die eigene Anpassung an eine sich immer schneller drehende Welt. Ein Schwungrad voller Risiken, Chancen, Optionen, Probleme und Konflikte. Mit neuen Sichtachsen, Perspektiven und Lösungen. Viele Menschen fühlen sich überfordert. Vielerorts herrschen Unordnung, Unübersichtlichkeit und Unschärfe. Hinzu kommt: Unser Leben ist den Zentrifugalkräften des hochdynamischen Wandels ausgesetzt. Eine der stärksten unter ihnen ist die fortschreitende Digitalisierung.

Mit dem täglich ansteigenden Wissen steigt der Datenverkehr, steigt das Datenaufkommen in dieser Welt, und nahezu alle von uns tragen hierzu bei. Es ist eine unumkehrbare Entwicklung und undenkbar, dass es an einem Tag in der Zukunft einmal weniger Datenverkehr geben wird als noch tags zuvor.

Unser Leben ist digital, und die Abgrenzung zum Analogen fällt uns zunehmend schwerer. Oftmals gelingt sie kaum noch. Was wir einmal eine digitale Parallelwelt nannten – das Internet –, ist integraler Bestandteil unseres Alltags, unseres Berufs, unseres Privatlebens, unserer gesamten Lebenswirklichkeit geworden. Es macht an keiner Stelle Halt, reicht bis in die entlegensten Gebiete dieser Welt. Es ist unser selbst erschaffenes und selbst erwähltes Neuland. Es vereinfacht, ermöglicht und skaliert.

Wir alle zahlen einen Preis, wenn wir dieses Neuland betreten. Wir zahlen ihn auf der Suche nach mehr Orientierung, Sicherheit und nach einem verlässlichen Werteverständnis. Das Internet

begeistert uns und macht uns Angst. Denn wir können nicht mehr kontrollieren, was es an neuen Kräften freisetzt, die unsere Verlässlichkeiten infrage stellen wie kaum etwas zuvor.

Das ist unser Neuland. Es macht Angst und ist gleichzeitig ein riesiger Chancen- und Optionenraum, der uns großartige Anpassungsmöglichkeiten gibt. Dieses Buch ist eine Offerte, diesen unaufhaltbaren Prozess mitzugestalten, es ist ein Plädoyer gegen die Angst vor ihm.

Im großen Neuland gibt es eine besondere Welt, die unser Leben begleitet. Sie folgt allem nach, was unser Fortschritt mit sich bringt, und spiegelt unser Tun, ohne dass es unserer Zustimmung bedarf. Es ist die Welt des Kriminellen, der illegalen Machenschaften. Sie ist kein eigener Kosmos, sondern dockt an unsere Bequemlichkeiten, Bedürfnisse, Unsicherheiten und Verletzlichkeiten an.

Missbräuchliches Verhalten ist ein sozialer Umstand. Nicht immer wird die Grenze zum Unerträglichen überschritten. Doch wenn dies geschieht, dann nennen wir es eine Straftat. Eine Handlung, die nicht mehr akzeptiert und auch nicht lediglich sanktioniert werden kann.

Seine Straftat macht einen Menschen zu einem Straftäter. Sie setzt ein eigenes Regime staatlichen Handelns frei, erzeugt nicht selten eine Öffentlichkeitswirkung und ruft immer wieder alte Kategorien in uns wach, die älter sind, als wir zurückdenken können. Wer hat das Recht zu handeln und wer hat das Recht zu urteilen? Wer zählt zu den Guten und wer zu den Bösen? Was ist richtig und was ist falsch?

Wie ein wenig funktionaler Wurmfortsatz hängt Kriminalität als nicht wegzudenkender Umstand an unserem menschlichen und gesellschaftlichen Miteinander und passt sich chamäleonartig an alles Neue an. In der Weise, dass Betrug über das Internet sehr viel mehr Menschen erreichen kann als eine persönliche Ansprache, aber

auch in jener, dass ein Banküberfall heute nicht mehr allzu viel Sinn ergibt und es neuer Brachialmethoden bedarf. Kriminalität transformiert sich mit uns.

Aber transformieren wir uns auch mit ihr?

Es gibt eine Unbekannte, und sie bleibt den meisten von uns verborgen. Die dunkle Seite des Internets ist mein Ermittlungsumfeld. Ich bin Cyberstaatsanwältin. Mein Job dreht sich um Daten, Kryptowährungen, Darknet und Cyberattacken. Eine analytische, chaotische, eine kaum greifbare Welt.

In den zurückliegenden Jahren durfte ich an einigen der spektakulärsten Ermittlungserfolge der internationalen Cybercrime-Bekämpfung mitwirken. An der Abschaltung multimillionenschwerer Darknet-Marktplätze und Schadsoftware-Botnetze, am Takedown weltführender illegaler Krypto-Mixing-Dienste und der Sicherstellung inkriminierter Kryptowährungen in dreistelliger Millionenhöhe.

Diese Schläge gegen die Cyberkriminalität wecken Interesse und eine große Erwartung: Der Staat hat es im Griff. Mein Beruf birgt den Auftrag, die Deutungshoheit im digitalen Raum zu erringen und zu verteidigen. Doch diese Deutungshoheit ist stark infrage gestellt. Die Strafprozessordnung wurde nicht für den selbstverständlichen Umgang mit Daten und die nassforsche Dynamik der digitalen Welt konzipiert. Der Cyberraum lässt Regierungen nicht genügend Zeit, um sich angemessen an die Entwicklungen im Bereich der Cyberkriminalität oder an technische Durchbrüche des Ermittelns anzupassen.

So kämpft der Staat einen Kampf, der ihn selbst meint. Er ist längst selbst Opfer von Cybercrime geworden. Und Opfer der Daten. Das Internet zwingt einen allzeit gültigen Übermachtanspruch in die Knie. Und es ist meine Aufgabe, die Eindämmung und Überführung von Straftaten an einem Ort zu bewältigen, den wir immer nur ungefähr kennen: im digitalen Neuland.

So wie eine Ärztin den Fernzugriff auf ihre Patienten erwägen und die Macht von Maschinen beurteilen können muss, so muss ich immer wieder neu lernen, wie das, was meine Aufgabe ist – Straftaten zu verfolgen – im digitalen Zeitalter gelingen kann. Der Schritt in die Cybercrime-Bekämpfung war meine Entscheidung gegen die Komfortzone. Ich musste von vorne anfangen, neues lernen, mich hinten anstellen und darauf vertrauen, dass ich trotz alledem einen Mehrwert schaffen könnte. Ohne ein Informatikstudium und ohne zu wissen, was digitale Währungen einmal mit uns anstellen würden. Es war der Aufbruch ins Neuland, jedoch nicht ohne Gepäck.

Als Staatsanwältin vertrete ich den Staat gegen das Kriminelle. Als Cyberstaatsanwältin habe ich diese Aufgabe im digitalen Raum.

Recht und Gerechtigkeit sollen einen universellen Geltungsanspruch haben, damals wie heute, analog wie digital. Doch was bedeutet das konkret? Welche Anpassungsleistung haben wir dort zu erbringen? Welchen Teil unseres Werteverständnisses verändert das Internet und welchen lässt es unberührt?

Mein Berufsstand schaut wie durch ein Brennglas auf den gesellschaftlichen Wandel. Ich ermittle im Verborgenen und finde dort die Auswirkungen unseres gesellschaftlichen Werdens. Was ich aber ebenfalls finde, das sind alte Fragen im neuen Gewand. Die digitale Transformation entlässt uns nicht, sie stellt Fragen nach Recht und Gerechtigkeit bloß anders. Sie eskaliert unsere stereotypen Vorstellungen von Gut und Böse und gibt uns wenig Zeit für eine wohlüberlegte Neuorientierung.

Die Forderung digitaler Lösungen ist laut. Doch die wichtigen Fragen nach der Schuld und dem Ermessen, nach Läuterung und dem Umgang mit Fehlern richten sich nicht an die digitale Welt. Sie richten sich an uns Menschen. Der Mensch steht weiterhin im Mittelpunkt, selbst wenn er meint, den Anschluss an den digita-

len Wandel verpasst zu haben. Auf diese Weise stellt die digitale Transformation unsere Bereitschaft, unser Handeln und unseren Fortschritt konsequent und ehrlich zu Ende zu denken, auf den Prüfstand.

Das Spiel von Räuber und Gendarm ist nur eines, das immer wieder neue Regeln bekommt. Es transformiert sich unaufhörlich mit allen anderen gesellschaftlichen Formen und Phänomenen.

Wie man durch unvorhersehbares Gelände kommt, lässt sich aus vielen Perspektiven beschreiben. Denn auf eine Weise ermitteln wir alle täglich im Neuland.

Ich tue es als Cyberstaatsanwältin.
Und ich lade Sie ein, Sie dorthin mitzunehmen.

KAPITEL 1

EIN SCHUFT IST EIN SCHUFT IST EIN SCHUFT

CYBERCRIME ist die qualitativ beste Fortbildung für Ermittler und Strafverfolger. Die Cybertäter arbeiten gründlicher und konsequenter als alle anderen. Jede Eventualität muss mitgedacht werden. Von Anfang an. Wir lernen dadurch täglich, unsere Cyberresilienz zu stärken, indem wir den Worst Case mitdenken und uns das Schlimmste vorstellen. Der berühmte SolarWinds-Hack hielt uns lange in Atem. Perfide gut geplant und durchgeführt. Cyberkriminelle sind den Ermittlern oft einen Schritt voraus. In der Aufklärung schließen wir die Lücke. Was die modernen Schufte wieder antreibt, noch besser zu werden. Das ist digitaler Fortschritt auf höchstem Level. Wir sollten Cybercrime als Lernkultur begreifen.

Dezember 2020, wenige Tage vor Heiligabend

Das Erste, was ich abends von den Ermittlern erhielt, war ein Link. Er führte zu einer Publikation der Firma FireEye, einem US-amerikanischen Unternehmen, das Software zur Erkennung von Cyberangriffen entwickelt hatte.

»We have detected a global intrusion campaign«, waren die einleitenden Worte des Berichts. Unbekannten Tätern war es gelungen, eine sogenannte »Supply-Chain-Attacke« in einer Software der Firma SolarWinds durchzuführen.

Unternehmen nicht direkt, sondern über ihre digitale Lieferkette anzugreifen, ist ein Mittel, um mit nur einer Infiltration eine große Anzahl Betroffener zu erreichen. Ich hatte zuvor von dieser Art der Cyberattacke gelesen, einen Fall dazu jedoch noch nicht auf dem Tisch gehabt. Ein erschreckend schlichter, fast schon naheliegender Ansatz, um mit relativ wenig Aufwand großen Schaden anzurichten.

Der Arbeitstag war lange vorbei. Ich ließ mich in Sportklamotten auf die Couch fallen und las weiter.

Die unbekannten Täter hatten lange Zeit unerkannt in den sogenannten Build-Prozess einer Software eingegriffen, die Firmen und Behörden weltweit nutzen, um ihre Netzwerkperformance zu überwachen, ihre IP-Adressen zu managen und die firmeneigenen Lagersysteme zu monitoren. Sie bauten eine Art Hintertür in die Software ein, um einen empfohlenen Standardprozess auszunutzen. Entsprechend der Herstellerempfehlung nahmen Tausende Kunden von SolarWinds regelmäßige Updates der Software vor. Dank der eingebauten Hintertür erhielten die Täter mit jedem dieser Updates

Zugriff auf die IT-Systeme der Nutzer der Software. Weltweit waren das rund 18 000.

Die Liste der prominenten Opfer des wohl spektakulärsten Hackingangriffs des Jahres 2020 war lang. Erst drehte sich vieles um das IT-Sicherheitsunternehmen FireEye, das über eines der kompromittierten Updates der SolarWinds-Software Orion selbst zum Opfer des Angriffs geworden war. Doch dann wurde publik, dass sich neben weiteren US-Behörden auch das US-amerikanische Finanzministerium und Teile des Pentagons die raffinierte Spionagesoftware eingefangen hatten. Selbst das US-Energieministerium mitsamt seiner untergeordneten National Nuclear Security Administration (NNSA) wurde als betroffen gemeldet. Die NNSA verwaltet das Atomwaffenarsenal der USA.

Kurz nach der Übersendung des Links baten mich die Ermittler um ein Gespräch per Videoschalte. Meine Ankündigung, so auszusehen wie eine, die gerade vom Joggen nach Hause kam, wurde gekontert mit der Bemerkung: »Wir haben uns auch nicht für dich schick gemacht, Jana.« Wenn Weihnachten auf dem Spiel steht, hilft vertrauter Galgenhumor. Zwei ebenso vertraute Gesichter erschienen auf dem Bildschirm, um mit Frau Staatsanwältin zu sprechen.

»Hast du den Bericht von FireEye gelesen?«

»Ja.«

»Gut. Hast du Fragen?«

Gute Cyberermittler preschen nicht vor, sondern achten darauf, dass die Juristin an Bord auch mitkommt auf der digitalen Nachtfahrt. An dieser Stelle hatte ich erst einmal keine Fragen.

»Nein.«

»Gut. Wir müssen davon ausgehen, dass auch jede Menge deutsche Kunden von SolarWinds die verseuchte Software nutzen und sich den Mist über das letzte Update eingefangen haben. Es könnten ein paar Hundert sein. Kann alles dabei sein. Firmen, Behörden, Institute. Orion nutzen echt viele.«

Orion?

So hieß die betroffene Software des Unternehmens SolarWinds, die weltweit von schätzungsweise 18 000 Abnehmern genutzt wurde, darunter Firmen und Institutionen aus der privaten Wirtschaft sowie Behörden. Die Schadsoftware, die die Täter gegen sie einsetzten, stellte sich der Weltöffentlichkeit mit dem Namen »Sunburst« vor.

Krieg der Sterne. Kosmisch digital.

»Wir wissen von konkreten deutschen Betroffenen. Aber wovon wir ausgehen müssen: Die meisten Firmen werden von ihrem Glück noch gar nichts wissen.«

Das Management von FireEye, das die eigene Betroffenheit zum Anlass nahm, die Welt über den SolarWinds-Hack zu informieren, hatte sich nicht nur dazu bekannt, selbst Opfer des Angriffs geworden zu sein. Die Unternehmensspitze hatte auch sinngemäß in Videostatements erklärt, dass sie den Angriff nur deswegen erkannt hätten, weil sie selbst in der Detektion von Cyberangriffen hoch spezialisiert waren.

Es war ein Cyberangriff, den man als Betroffener nur mitbekam, wenn man selbst zu den Experten gehörte. Denn der blinde Passagier mit dem Namen »Sunburst« gab sich erst einmal nicht zu erkennen.

Ich scrollte den Artikel hinunter und beantwortete die ersten Fragen, die sich in einer solchen Situation immer wieder stellen: Sachverhalt verstanden. Zuständigkeit geklärt. Zusage für die Einleitung eines staatsanwaltlichen Ermittlungsverfahrens erteilt.

»Braucht ihr aktuell etwas von mir?«

Kopfschütteln auf dem Bildschirm.

»Wie es aussieht, heute nicht, aber wir müssen schauen, wie wir an die Geschädigten herankommen. Wenn wir die Betroffenheit in Deutschland geklärt haben, dürfte ein bisschen was auf dich zukommen, denn von denen allen brauchen wir Daten.«

Cybercrime-Fälle beginnen ganz unterschiedlich, aber bei allen erklingt ein äquivalenter Startschuss: die Suche nach Daten. Denn mit Erklärungen, menschlichen Erinnerungen und Papier können wir nicht allzu viel anfangen.

Die Strafprozessordnung sieht in § 94 vor, dass »Gegenstände, die als Beweismittel für die Untersuchung von Bedeutung sein können, in Verwahrung zu nehmen oder in anderer Weise sicherzustellen sind«. Und dazu gehören auch Daten. Nicht nur Tatmesser, Steuerunterlagen und Videoaufzeichnungen von Tankstellen.

Aber nur, weil die Durchsuchung von Firmenräumen richterlich angeordnet wurde, heißt das noch lange nicht, dass wir finden, wonach wir suchen.

Am Empfangstresen einer Firma mit einem Durchsuchungsbeschluss zu stehen, kann ein Triumphzug, aber auch der Beginn einer langen und unangenehmen, schlimmstenfalls erfolglosen Suche sein. Denn Daten werden nicht sortiert wie Aktenordner. Ein Durchsuchungsbeschluss ist nur ein stumpfes Schwert, wenn wir an der falschen Stelle selbst suchen müssen. Recht haben und Recht bekommen sind auch für uns Strafverfolger zwei unterschiedliche Paar Schuhe.

Wo genau welche Unternehmensdaten gespeichert sind, wissen in Unternehmen nur sehr wenige. Und genau diese Personen sind solche, mit denen wir am liebsten sofort sprechen. Wenn möglich, auch ohne Durchsuchungsbeschluss, sondern mit einem Besteck, das unser Gegenüber in die Lage versetzt, uns zu geben, was wir brauchen, ohne dass Dienstausweise gezückt werden müssten. Es ist die staatsanwaltliche Herausgabeanordnung nach § 95 der Strafprozessordnung: »Wer einen Gegenstand der vorbezeichneten Art in seinem Gewahrsam hat, ist verpflichtet, ihn auf Erfordern vorzulegen und auszuliefern.«

Wer diese Aufforderung von der Staatsanwaltschaft erhält, muss keine wartenden Polizeibeamten betreuen, sondern kann uns die

Daten selbst heraussuchen und übermitteln. Und die deutschen Betroffenen der SolarWinds-Attacke wurden immer mehr.

Das Klischee, dass Polizeieinsätze kurz vor dem Wochenende starten oder sich Hackingangriffe zu Beginn der Ferien häufen, mag ein persönlicher Eindruck überarbeiteter Ermittlerinnen und Ermittler sein. Eine sachliche Erklärung dafür besteht gleichwohl. Kurz vor den freien Tagen erlahmen Prozesse, sind Entscheider nicht mehr so gut erreichbar wie an einem Dienstagmorgen im November. Solche Schwächen nehmen Täter gerne mit.

»Das war es dann erst mal, Jana. Wir schicken dir die Anregung zur Verfahrenseinleitung spätestens morgen zu und hoffen, dass wir alle Weihnachten feiern können.«

Ich winkte zwei vertrauten Gesichtern zu. Sie winkten zurück. Der Bildschirm verdunkelte sich.

Der Angriff auf die Orion-Software von SolarWinds funktionierte, weil Unternehmen genau das taten, was ihnen empfohlen worden war: regelmäßige Updates der erworbenen Software vorzunehmen. Unbeschadet von der Attacke blieben alle SolarWinds-Kunden, die das entweder vergessen oder für nicht so wichtig befunden hatten.

Dabei lautet die gebetsmühlenartige Empfehlung an alle Internetnutzer dieser Welt: Updates zur Sicherheit des eigenen Systems vornehmen. Rechtzeitig und regelmäßig.

Dieses Mantra hatten die Sunburst-Täter in zynischer Weise persifliert und gezeigt, dass kein Verhalten einen hundertprozentigen Schutz vor einem Hackingangriff etablieren kann.

Im Zuge von Cyberermittlungen bei einem Unternehmen, dessen Gebäudeleitsystem nach einem Hackingangriff nicht mehr funktionierte, durften wir in einem anderen Fall einmal erleben, dass größerer Schaden nur durch den Umstand verhindert werden konnte, dass die betroffene Institution ein so altes Computersystem betrieb, dass die Schadsoftware sich nicht zurechtfand und kein wirkliches Unheil