INHALT

Geräte richtig nutzen

Souverän online unterwegs

PROLOG

Es war 10 Uhr morgens, ich befand mich auf dem Weg zu einer Konferenz, als meine Assistentin einen Anruf weiterleitete. Eva, eine junge Frau aus Köln, stand unter Schock: Soeben hatte ihr Exfreund einen digitalen Anschlag auf sie verübt. Am Abend zuvor hatte er sie gefragt, ob sie zu ihm zurückkehren wolle, doch Eva wollte nicht. In einem friedlichen, aber entschlossenen Ton hatte sie ihm das gesagt und ihn gebeten, sie nicht mehr zu kontaktieren. Eva wollte endlich Abstand gewinnen und glaubte, auch für ihn wäre dies das Beste, denn so würden beide ein neues Kapitel im Buch des Lebens aufschlagen können. Sie hätte sich nie träumen lassen, dass ihr Ex zu einer solchen Tat im Stande wäre. Er hatte den Anschlag offenbar über Wochen vorbereitet, im Grunde hatte alles schon zwei Jahre zuvor angefangen: Er hatte damals ab und zu eine versteckte Kamera mitlaufen lassen, als die beiden sich noch sehr nahe waren. Es war unfassbar: Seit heute Morgen befanden sich Videos ihrer intimsten Momente auf verschiedenen einschlägigen Webseiten im Internet. Dazu berichtete ein Nachbar ihrer Eltern, eine

DVD mit eben diesen Videos per Post erhalten zu haben. Der Exfreund hatte, so fanden wir später heraus, Dutzende dieser DVDs an Menschen aus Ihrem Umfeld, rund um Köln und anderswo, privat wie beruflich, versandt.

Sebastian war seit zwei Monaten Direktor eines 5-Sterne-Hotels in Los Angeles, nach fünfundzwanzig Jahren harter Arbeit. Ein Mitarbeiter im Service trug ein religiöses Symbol aus Asche auf der Stirn, das in der Mittagssonne langsam zerlief – ein wenig appetitlicher Anblick. Sebastian hatte den Mitarbeiter zuvor schon zweimal aufgefordert, das Zeichen zu entfernen, doch der Mitarbeiter tat nichts. In der Küche passierte es dann: Sebastian verlor die Geduld und warf dem Mitarbeiter die Worte »Wipe that f****** thing off your face« an den Kopf. Natürlich hätte er nicht die Fassung verlieren dürfen, doch die Folgen dieses einen unkontrollierten Moments in seinem langen Berufsleben waren dramatisch: Die Gewerkschaft schlachtete den Vorfall als offensichtlichen Akt der Diskriminierung aus, Zeitungen und Fernsehen berichteten darüber. Suchte man nach Sebastian im Internet, fand man seitenweise Referenzen zu diesem einen schwachen Moment in seinem Leben. Sebastian verlor seinen Job, einen neuen konnte er nicht finden, drei lange Jahre lang. Am Ende nahm er eine Stelle in einem Kasinohotel im asiatischen Macau an, während seine Frau und Kinder in Los Angeles blieben. Er sah sie zweimal im Jahr – ein hoher Preis für einen unbedachten Augenblick.

Pfarrer Bernhard traute seinen Augen nicht: Polizisten durchsuchten sein Haus und beschlagnahmten sämtliche Computer, denn sie hatten einen anonymen Hinweis erhalten. Und in der Tat fanden sie auf einer Festplatte kinderpornographische Bilder. Pfarrer Bernhard konnte sich das nicht erklären. Wenn nicht wenig später eine Zeugenaussage zutage gebracht hätte,

was wirklich geschehen war, wäre sein Leben ruiniert gewesen: Seine Familie, alles, wofür er gearbeitet hatte, hätte er verlieren können. Ein krimineller Hacker aus der rechtsradikalen Szene hatte die Fotos auf seinem Laptop platziert. Man wollte sich auf diese Weise an Pfarrer Bernhard rächen, hatte der doch mit großem persönlichen Einsatz und einigem Erfolg gegen den Extremismus in seiner Gemeinde gekämpft. Dank seiner Bemühungen wurden etwa die Drahtzieher eines Anschlags auf einen Dönerstand neben der Kirche ausfindig gemacht. Nun war Pfarrer Bernhard beinahe selbst Opfer eines Anschlags geworden – eines digitalen Anschlags.

Diese drei Geschichten haben sich nicht genau so ereignet. Sie beruhen auf Erlebnissen aus meinem Umfeld und auf Begebenheiten, von denen ich im Rahmen meiner Tätigkeit für den Virtual Bodyguard erfahren habe.[1] Eine wachsende Zahl von uns kennt ähnliche Ereignisse. Nicht immer sind die Geschehnisse derart dramatisch, aber doch haben sie häufig tiefgreifende Folgen für die Privatsphäre von Menschen, die das nicht verdient haben. In der digitalen Welt lauern viele Gefahren: Der sogenannte Black-Hat-Hacker,[2] der aus der Ferne unsere Webcam im Laptop kapert und unbemerkt Bilder von uns macht. Arbeitgeber, die den privaten E-Mail-Verkehr ihrer Mitarbeiter überwachen. Mobbing unter Teenagern, Berufskollegen, ehemaligen Freunden.

---

1 Virtual Bodyguard, 2014, www.vbodyguard.com.

2 Die Hacker-Szene teilt sich in sogenannte »White-Hat-Hacker« und »Black-Hat-Hacker«. Während Erstere sich als die Guten im Spiel betrachten (und es in der Regel sind, indem sie beispielsweise helfen, Sicherheitslücken aufzudecken und damit deren Eliminierung zu veranlassen), sind Letztere die, die uns zu schaffen machen. Wir haben es in diesem Buch also in der Regel mit den sogenannten »Black-Hat-Hackern« zu tun.

Dem einen oder anderen mag bei diesen Geschichten die Freude am sogenannten digitalen Zeitalter vergehen. Das wäre schade, denn die Welt ist durch die Existenz des Internets eine transparentere, sozialere und demokratischere geworden. Unterdrückte Menschen organisieren sich über soziale Netzwerke, um ihre Rechte wahrzunehmen. Mittellose Studenten können im Internet Kurse amerikanischer Eliteuniversitäten besuchen, ohne einen Cent dafür bezahlen oder einen Fuß auf den Campus setzen zu müssen. Online-Enzyklopädien wie *Wikipedia* machen Wissen heute zugänglich für jedermann und ersetzen statische Standardwerke wie den *Brockhaus*, der ohnehin nur für Wohlhabende erschwinglich war.

Auch im normalen Alltag verbessern die Neuerungen der digitalen Welt unsere Lebensqualität. Smartphone und Laptop erlauben es uns, auch unterwegs produktiv zu sein. Dieses Buch ist so zum Beispiel nicht nur am Schreibtisch, sondern auch im Zug sowie bei Rotwein und Pasta in der Tessiner Wintersonne entstanden. Dabei hatte ich nahezu jederzeit online Zugang zu wertvollen Informationen. Ich konnte Gedanken niederschreiben, während sie mir kamen, egal, wo ich mich in dem Moment gerade befand.

Die digitale Welt hat unser Leben deutlich verändert – und das ist gut so. Zugleich müssen wir lernen, bewusst mit all diesen Neuerungen umzugehen, um daraus möglichst keine Beeinträchtigungen zu erfahren. Das ist ein ganz normaler Prozess. Auch der Straßenverkehr war zunächst etwas Neues, Unorganisiertes. Angeblich dachte man in seinen Anfängen sogar einmal darüber nach, vor jedem Auto ein Pferd laufen zu lassen, weil alles, was schneller als ein Pferd war, gefährlich sein könnte. Heute kennen wir klare Regeln: Wir lernen diese, üben fahren und machen einen Führerschein. Der Straßenverkehr ist recht

sicher geworden. Dabei bleibt allerdings ein Restrisiko bestehen, denn gefahrlose Mobilität gibt es nicht. Es geht darum, dieses Risiko zu minimieren.

Genauso ist es auch mit der digitalen Welt: Wir stecken hier noch in den Anfängen, aber vieles ist heute schon möglich. Wir rasen mit 300 Tausend Kilometern pro Sekunde über die Datenautobahnen (bildlich gesprochen, denn in Tat und Wahrheit umrunden unsere Daten in Sekundenbruchteilen den Globus), wissen aber noch viel zu wenig darüber, wie wir uns ausreichend vor Unfällen schützen. Auch der Gesetzgeber ist überfordert und lässt private Unternehmen wie Google, Facebook, Apple und viele andere weniger große, aber dennoch schlagkräftige Mitbewerber nahezu frei schalten und walten. Staaten

hinken bei der Aufgabe, die notwendigen juristischen Rahmenbedingungen für ein sicheres digitales Leben zu schaffen, heillos hinterher.

Die Enthüllungen von Edward Snowden über das Ausmaß der weltweiten Überwachungs- und Spionagepraktiken von Geheimdiensten haben zu Recht eine wichtige Diskussion über Privatsphäre und persönliche Sicherheit im digitalen Zeitalter ausgelöst. Doch irgendein ferner amerikanischer Geheimdienst ist kaum unsere unmittelbarste Gefahr. Sicherlich müssen wir Behörden und Regierungen auf die Finger schauen, damit auch sie nicht Dinge tun, die dem Datenschutzgedanken widersprechen. Hier werden die Mühlen allerdings langsam mahlen, der politische Willensbildungsprozess steckt erst in seinen Anfängen.

Schon heute aber ist unsere Privatsphäre in Gefahr. Dabei stammen, so zeigt meine Erfahrung, typische Bedrohungen in den meisten Fällen aus unserem direkten Umfeld – von Menschen, die wir einmal Freunde nannten oder gar liebten, von Widersachern im privaten und beruflichen Umfeld, von Unternehmen, deren Dienstleistungen und Produkte wir nutzen wollen. Dazu kommen uns zumeist unbekannte Black-Hat-Hacker, die mit uns spielen wollen wie die Katze mit der Maus.

Die Verantwortung, uns und unsere Liebsten gegen digitale Angriffe zu schützen, liegt heute und vermutlich auch in Zukunft primär bei uns selbst. Wir müssen uns Verhaltensweisen zum Schutz der Privatsphäre aneignen. Wir müssen aufmerksam sein, ein Gefühl für Gefahren entwickeln, sie möglichst bannen und bei einem Vorfall wenigstens den Schaden gering halten. Der größte Feind: Ignoranz. Bis tatsächlich etwas passiert, halten wir uns häufig für unverwundbar. Auch das ist genauso wie im Straßenverkehr.

Der *Safe Surfer* wird Ihnen mit 52 verständlichen und praktikablen Tipps helfen, Ihre Privatsphäre zu schützen. Zum einen soll dieses Buch durch anschauliche Beispiele für Gefahren sensibilisieren und es Ihnen leichter machen, solche frühzeitig zu erkennen. Zum anderen soll es Ihnen helfen, sich effektive Denk- und Handlungsweisen zum Schutz der Privatsphäre anzueignen. Sie können den *Safe Surfer* als Arbeitsbuch nutzen, Tipps nach dem Lesen sofort umsetzen und persönliche Notizen dazu vornehmen, damit Sie später nachvollziehen können, was Sie getan haben. Bitte denken Sie dabei daran: Ihre persönlichen Notizen sollten entweder so verfasst sein, dass kein Dritter mit ihnen etwas anfangen kann, oder Sie bewahren sie an einem sicheren Ort auf, zusammen mit sonstigen vertraulichen Dokumenten und Informationen wie Zugangscodes oder Passwörter (mehr dazu in Kapitel 11).

Es wird an manchen Stellen dieses Buchs vorkommen, dass ich auf konkrete Anwendungen und Produkte hinweise, aber das wird die Ausnahme bleiben. Zum einen gibt es häufig mehrere Möglichkeiten, zwischen denen Sie frei wählen können. Zum anderen würde es den Rahmen dieses Buchs sprengen, für jedes Gerät, jedes Betriebssystem und jede Anwendung eine separate Betriebsanleitung zu schreiben. Allerdings möchte ich Ihnen dennoch eine möglichst gute Hilfestellung anbieten. Ich unterhalte aus diesem Grunde begleitend zum Buch eine Webseite, auf der Sie zu den Tipps, wo es sinnvoll ist, weiterführende Informationen finden. Besuchen Sie also parallel zur Lektüre und Umsetzung der Tipps www.safe-surfer.com/buch.

Selbst wenn www.safe-surfer.com/buch nützliche Hinweise für Sie bereithält, möchte ich Sie zugleich ermutigen, Fragen eigenständig zu klären. Das ist oft gar nicht so schwer, und Sie trainieren so Ihre Fähigkeit, sich neuen Herausforderungen der

digitalen Welt zeitnah und effektiv zu stellen. Für die Fälle, in denen Sie allein nicht weiterkommen, empfehle ich Ihnen, Kontakt zu einem technischen Experten in Ihrer Nähe aufzubauen. Wichtig ist, dass dies eine Person ist, der Sie vertrauen können (siehe auch Kapitel 6).

Ein Wort noch zu den Geschichten und Beispielen in diesem Buch: Wenn es sich nicht um eine in diversen Medien publizierte Story über in der Öffentlichkeit stehende Personen handelt, habe ich Situationen anonymisiert und verfremdet; manchmal packte ich auch mehrere Erlebnisse zusammen. Die Geschichten sind also fiktiv, als Basis für diese Geschichten dienten allerdings reale Begebenheiten.

Ich wünsche Ihnen viel Spaß beim Lesen und viel Erfolg bei der Umsetzung der Tipps!