Kapitel 1
Basiswissen und Softskills

Die Digitalisierung ist aus kaum einem Leben mehr wegzudenken. Der Blick auf das Smartphone direkt nach dem Aufstehen ist für viele Menschen alltäglich geworden. Und bereits vor dem Frühstück haben wir vielfältige Möglichkeiten, mit unserem Smartphone Informationen aufzunehmen, zu kommunizieren und Inhalte zu erstellen.

Digitale Technologie ist überall um uns herum, und damit diese intelligent wird, muss sie vernetzt werden. Diesen technologischen Fortschritt verdanken wir dem Internet. Es gibt jedoch wie so oft zwei Seiten der Medaille und neben den beeindruckenden Chancen eben auch ernstzunehmende Risiken bei der Nutzung des Internets.

Digitale Sicherheit bei digitalen Gefahren

Neue Geräte, neue Apps, neue Software, neue Möglichkeiten – mit der Nutzung nehmen auch die Risiken im Umgang mit modernen Technologien zu, da wir vermehrt Wertvolles im Internet hinterlassen: von unseren Urlaubsfotos bis hin zu getätigten Online-Zahlungen und anderen Bankdaten.

Die Gefahrenlage hat sich im Vergleich zu früher verändert. Menschen werden heute Opfer von realem Betrug im Internet. Gefälschte E-Mails, das Vortäuschen falscher Identitäten oder schlichtweg Schadsoftware können der Grund dafür sein. Cyber-Kriminelle versuchen, persönliche Daten wie Kreditkarteninformationen oder Passwörter zu ergaunern.

Die gute Nachricht ist: Wer verhindern will, zum Opfer einer der vielen Betrugsmaschen zu werden, der hat viele Möglichkeiten, diese Gefahr zu reduzieren. Dafür muss jedoch jeder selbst tätig werden.

Das beruhigende Gefühl, etwas für den Schutz der eigenen digitalen Daten getan zu haben, kann einen abends besser einschlafen lassen. Denn wer sich vorher Gedanken darüber macht, wie wichtig einem die Daten sein können, kann diese besser schützen. Fotos von der Hochzeit, einmaligen Momenten Ihrer Kinder oder anderen einzigartigen Erlebnissen lassen sich schließlich nicht einfach noch einmal machen.

Dabei gibt es Parallelen zwischen der digitalen Sicherheit und der Sicherheit eines Gebäudes: Ihr Haus soll kein Gefängnis sein – es sollen jedoch nur berechtigte Personen zu den verschiedenen Zimmern Zugang bekommen. Angreifer werden immer versuchen, unberechtigt Zutritt zu erhalten. Sie sollten auf diese Einbruchsversuche eingestellt sein. Wer versucht, in ein Haus einzubrechen, der sollte es schwerer haben, als nur die Klinke der Tür herunterzudrücken – unerlaubtes Eindringen muss im realen wie im digitalen Leben so schwer wie möglich gemacht werden.

In keinem Bereich des echten Lebens gibt es eine 100%-ige Sicherheit. So ist es auch im digitalen Leben. Aber wie hoch sollte der Schutz sein? Diese Frage muss jeder für sich selbst beantworten – wir geben Ihnen jedenfalls in diesem Buch Möglichkeiten an die Hand, ein sehr hohes Schutzniveau zu erreichen.

Gehen Sie nach dem Pareto-Prinzip vor. 20 % des Aufwands bringt Ihnen 80 % des Erfolgs. Sie müssen nicht jede Maßnahme bis ins letzte Detail umsetzen, um es Kriminellen in der digitalen Welt schwer zu machen!

Die Verhältnismäßigkeit spielt bei IT-Sicherheitsmaßnahmen eine große Rolle. So sind Sie im privaten Umfeld einem relativ geringen Risiko ausgesetzt, das Opfer einer staatlich beauftragten Hackergruppe zu werden. An dieser Stelle stünden Sie ganz klar jenseits vom Pareto-Prinzip: Sie müssten einen erheblichen Mehraufwand in Kauf nehmen für nur etwas mehr Schutz. Eine deutlich realistischere Gefahr, von der bereits Millionen Menschen betroffen sind, ist dagegen der Diebstahl von Accounts und damit letztlich auch von Identitäten. In diesem Buch widmen wir uns der Vermeidung von realistischen Gefahren.

Ihre E-Mail-Adresse ist der Sicherheitsanker Ihrer digitalen Identität. Alle Möglichkeiten zum Schutz Ihrer E-Mail-Adresse sollten Sie ergreifen. Wer Ihre E-Mail-Adresse hackt, der kann Passwörter zurücksetzen und so auch Zugriff auf andere Dienste, Webseiten und Anwendungen bekommen.

Eine gesunde Portion Vorbereitung, ein bisschen Misstrauen, der richtige und bewusste Umgang mit ungewöhnlichen Situationen sowie eine gute Account-Hygiene tragen einen großen Teil zu Ihrem Schutz bei.

Schaffen Sie Risikobewusstsein

Waren Sie schon einmal in den Umkleideräumen eines Fitnessstudios, in dem die Mitglieder die Schlösser für ihre Spinde selbst mitbringen müssen? Es gibt dort die unterschiedlichsten Formen, Farben und Stärken zu sehen – vom Zahlenschloss

mit drei Stellen bis hin zum Panzerschloss. Oder mit anderen Worten: Das Sicherheitsbedürfnis der Menschen ist unterschiedlich hoch und Menschen sind auch unterschiedlich stark dazu bereit, Investitionen in ihre Sicherheit zu tätigen.

Natürlich kommt es auch auf die inneren Werte an: Wer nur seine Mütze und Ersatzsocken wegschließt, für den reicht das Zahlenschloss. Oder stecken Sie Ihr Smartphone, Ihre Rolex und den Autoschlüssel Ihres Luxussportwagens in den Spind? Dann ist das Panzerschloss die richtige Wahl. Im digitalen Raum ist es ähnlich – der zu schützende Inhalt sind Daten und Informationen. Schutzmechanismen sind beispielsweise Passwörter, die unterschiedlich stark sein können.

Im Internet existieren wie im echten Leben auch Personen mit extremen Einstellungen. Auf der einen Seite gibt es immer wieder die Personen, die behaupten, sie hätten sowieso nichts zu verstecken. Diese zeichnen sich häufig durch große Arglosigkeit und Fahrlässigkeit aus und vernachlässigen ihre eigene Sicherheit im Internet oft sträflich. Auf der anderen Seite stehen Personen, die scheinbar kein Teil der Digitalisierung sind. Sie halten sich komplett heraus und haben weder ein Smartphone noch Accounts in sozialen oder beruflichen Netzwerken.

In diesem Buch geben wir Ihnen Hilfsmittel an die Hand, mit denen Sie risikobewusste Entscheidungen treffen können. Sie sollen die Chancen des digitalen Raumes ausschöpfen können: von der Digitalisierung profitieren, aber sicher!

Es gibt keine unwichtigen Daten im Internet – ausnahmslos. Auch scheinbar komplett belanglose Daten können von Hackern in den richtigen Kontext gebracht werden und zum Schlüssel für ihren kriminellen Erfolg sein.

Der souveräne Umgang mit Geräten, Apps und Cloud

Alles, was mit Technik zu tun hat, entwickelt sich rasend schnell weiter. Wir haben inzwischen die Möglichkeit, in eine virtuelle Realität (Virtual Reality) abzutauchen und können sogar die reale mit der virtuellen Welt verbinden (Augmented Reality). Wer ein neueres Auto fährt, für den ist die enge Verbindung mit dem Smartphone selbstverständlich. Die Sprachsteuerung zu Hause unterscheidet die Stimmen der Mitbewohner und fährt auf Wunsch die Jalousien hoch und die Heizung herunter, wenn das Fenster offen ist.

Man muss nicht jeden Trend mitmachen. Doch für jeden Einzelnen gibt es Funktionen, die das Leben nicht nur bequemer machen (darum geht es häufig), sondern auch sicherer, andere reduzieren die Einsamkeit oder können in Notfällen

Bescheid geben. So kann ein Sprachassistent auch dann Menschen helfen, wenn der Notknopf nicht getragen wird oder in Reichweite ist. Dieser Assistent benötigt einen Zugang zur Cloud.

Der Begriff *Cloud* fällt sehr häufig im Zusammenhang mit der Digitalisierung. Dabei ist die Cloud eigentlich nur der Computer von jemand anderem. Häufig steht dieser Computer mit vielen anderen leistungsstarken Systemen in einer Serverfarm von Amazon, Google, Microsoft, Alibaba oder anderen Unternehmen. Das bringt viele Vor-, aber auch Nachteile mit sich.

Im November 2020 sind Teile der Server von Amazon ausgefallen. Daraufhin haben viele Staubsaugerroboter nicht mehr funktioniert. Auch wenn der Zusammenhang nicht direkt klar ist: Die Saugroboter kommunizieren über die (ausgefallenen) Server. Die zahlreichen Serverfarmen können getrost als das Rückgrat des Internets bezeichnet werden.

Die Nutzung der Cloud ist auf den ersten Blick oft preiswert. Eine geringe monatliche Gebühr wird fällig, um die Rechenleistung anderer Computer nutzen zu können.

Google Stadia, GeForce Now oder Amazon Luna sind Beispiele für Cloud-Dienste. Anspruchsvolle Videospiele können von jedem Computer aus gespielt werden. Sie brauchen nur einen Browser und eine Internetverbindung. Eine anspruchsvolle Grafikkarte oder Spielekonsole benötigen Sie nicht mehr, denn Sie bekommen die Rechenleistung von den Servern des jeweiligen Unternehmens und zahlen dafür eine monatliche Gebühr.

Die Nutzung von Cloud-Diensten führt aber auch zu neuen Gefahren, denn

- ✔ der Übertragungsweg vom Rechner zum Cloud-System muss gesichert sein,
- ✔ Sie können den Cloud-Anbieter nicht überprüfen und müssen ihm vertrauen,
- ✔ der Wechsel eines Cloud-Anbieters ist oft nicht leicht und wird absichtlich schwer gemacht,
- ✔ neue Lizenzvereinbarungen oder Änderungen am Datenschutz kommen regelmäßig und dann sind Sie gefordert, sich über die Konsequenzen zu informieren.

Neben Google, Amazon und Apple gibt es zahlreiche kleinere Anbieter von vernetzten Produkten. Sollten diese Unternehmen irgendwann nicht mehr existieren, so können Sie auch mit den Geräten nichts mehr anfangen, da die Software keine Updates mehr erhält und Sie keine Unterstützung mehr bei Problemen bekommen.