Cybersicherheit

für Dummies

» Hier geht's direkt zum Buch

DAS VORWORT

Einleitung

Im Laufe einer einzigen Generation hat unsere Welt enorme Veränderungen durchgemacht. Die Verfügbarkeit des Internets sowohl für Verbraucher als auch für Unternehmen gekoppelt mit der Erfindung mobiler Endgeräte und kabelloser Netzwerke hat eine Informationsrevolution eingeleitet, die sich auf jeden einzelnen Aspekt unseres Lebens auswirkt.

Die Abhängigkeit von Technologien hat uns gleichzeitig gigantische Gefahren beschert. Kaum ein Tag geht vorbei, an dem wir nicht irgendeine Nachrichtenmeldung über einen Datenskandal, einen Cyberangriff oder eine Sicherheitslücke hören oder lesen. Da wir Menschen von Tag zu Tag abhängiger von Technologien werden, sind auch die möglichen negativen Konsequenzen von Cyberangriffen exponentiell gewachsen. Mittlerweile haben wir den Punkt erreicht, an dem Menschen ihr Vermögen, ihren Ruf, ihre Gesundheit, ja sogar ihr Leben aufgrund von Cyberangriffen verlieren.

Wir, die wir in einer modernen Welt leben, sind uns mehr und mehr darüber im Klaren, warum wir uns vor Cyberbedrohungen schützen müssen. Dieses Buch zeigt Ihnen, wie das gelingen kann.

Über dieses Buch

In den letzten Jahrzehnten sind zwar zahlreiche Bücher zu Cybersicherheitsthemen erschienen, die meisten von ihnen geben allerdings der breiten Bevölkerung nicht die Informationen, die sie benötigen, um sich selbst angemessen gegen Gefahren zu verteidigen.

Viele Cybersicherheitsratgeber richten sich an eine technisch sehr versierte Zielgruppe und erdrücken technische Laien mit für sie irrelevanten Informationen. Sie erschweren es den Lesern daher, das erworbene Wissen praktisch umzusetzen. Darüber hinaus gibt es noch diverse Bücher, die im Self-Publishing erschienen sind und eine Einführung in das Thema Cybersicherheit geben sollen, dabei allerdings an allerlei Dingen kranken. In einigen Fällen wurden sie sogar von technischen Laien verfasst und enthalten Fehlinformationen. Abgesehen davon kursieren viele Sicherheitschecklisten, die Klischees wiederholen und veraltete Ratschläge geben. Das kann dazu führen, dass die Nutzer durch Befolgen der Tipps ihre Cybersicherheit eher verschlechtern, statt sie zu verbessern. Leider hat auch die ständige Wiederholung von Cybersicherheitsempfehlungen durch Medienschaffende nach Berichten über Sicherheitslecks (»Ändern Sie alle Ihre Passwörter!«) verbunden mit dem Ausbleiben irgendwelcher Konsequenzen, wenn die Nutzer diesen Anweisungen nicht gefolgt sind, zu einer Cybersicherheitsmüdigkeit geführt. Das heißt, dass viele bei Vorfällen schlichtweg überhaupt nicht mehr reagieren, weil einmal zu oft »Feuer!« gerufen wurde.

Ich habe *Cybersicherheit für Dummies* geschrieben, damit alle, die keine Experten auf dem Gebiet sind, ein Buch mit den Grundlagen zur Hand haben. Darin erfahren sie, was beim Thema Cybersicherheit relevant ist, und auch, warum es das ist. Das Buch bietet Ihnen praktische und klar formulierte Ratschläge, die Sie leicht umsetzen können und mit denen

Sie sich, Ihre Kinder, Ihre Eltern und womöglich sogar Ihr kleines Unternehmen im Cyberraum schützen.

Eine kleine Warnung vorweg: Wenn Sie alle Informationen in diesem Buch verinnerlichen und sie in die Praxis umsetzen, werden Sie zwar Ihre eigene Cybersicherheit erheblich verbessern, doch alleine das Lesen dieses Buches macht Sie genauso wenig zu einem Cybersicherheits-Profi, wie Sie das Lesen eines Buchs über die Funktionsweise des menschlichen Herzens zu einem kompetenten Kardiologen macht.

Cybersicherheit ist ein komplexes Gebiet, das sich rasend schnell verändert. Fachleute arbeiten Jahre, wenn nicht sogar Jahrzehnte daran, ihre Fähigkeiten und ihr Fachwissen zu erhalten, weiterzuentwickeln und zu verfeinern. Bitte betrachten Sie dieses Buch daher nicht als Ersatz für die Beauftragung eines Profis, wenn Ihre Situation den Letztgenannten erforderlich macht.

In der neuen Auflage dieses Buchs sind wichtige neue Entwicklungen berücksichtigt worden: vor allem die weitgehende Verbreitung von Arbeiten im Homeoffice (hier hat die COVID-19-Pandemie die Entwicklung beschleunigt) in Kapitel 6 und die überwältigend schnelle Weiterentwicklung von künstlicher Intelligenz (KI) in den letzten Jahren (Kapitel 20), vor allem von sogenannter generativer KI, also ChatGPT und Konsorten.

Und diese schnelle Entwicklung geht natürlich auch nach Drucklegung dieses Buches weiter: Denken Sie daher bitte immer daran, dass sich technische Produkte ständig im Fluss befinden und schnell verändern. Screenshots, die Sie in diesem Buch finden, sind womöglich nicht identisch mit dem, was Sie auf Ihrem Bildschirm sehen, wenn Sie den Anweisungen aus diesem Buch folgen. Vergessen Sie nicht: Die Gefahren für die Cybersicherheit entwickeln sich laufend weiter. Dasselbe gilt auch für die Technologien und Methoden, die dazu eingesetzt werden, sie zu bekämpfen.

Wie dieses Buch aufgebaut ist

Cybersicherheit für Dummies besteht aus sechs Teilen.

Die Teile I, II und III bieten Ihnen einen Überblick über Cybersicherheit, mögliche Gefahren und versorgen Sie mit allerlei Tipps, wie Sie sich selbst und Ihre Familie gegen externe Bedrohungen verteidigen und verhindern können, dass Sie gefährliche (und potenziell verheerende) Fehler begehen. Sie erfahren mehr darüber, wie Sie Ihre Online-Konten sichern und wie Sie Passwörter auswählen und schützen. Selbstständige und Freiberufler erhalten ein paar zusätzliche Tipps, wie sie ihre berufliche Tätigkeit im Cyberraum sichern können. Außerdem wagen wir einen Blick in die Zukunft.

Teil IV beschäftigt sich damit, wie Sie einen Sicherheitsvorfall erkennen und wie Sie anschließend damit umgehen.

Teil V deckt den Themenbereich rund um Sicherheitskopien und Backups ab. Das ist etwas, das Sie regelmäßig tun sollten, bevor Sie gezwungen sind, Daten aus Backups wiederherzustellen oder Ihre Geräte zurückzusetzen. Letzteres ist ein Thema, das Sie ebenfalls in diesem Teil finden.

Teil VI ist der Teil mit kurzen und knackigen Informationen, die Ihnen helfen sollen, Ihre Cybersicherheit mit nur wenigen Schritten zu verbessern. Hier lohnt es sich, ein Lesezeichen hineinzulegen.

Törichte Annahmen über die Leser

Wenn Sie dieses Buch lesen, gehe ich davon aus, dass Sie folgende Erfahrungen mit Computertechnologie haben:

- ✔ Sie wissen, wie man eine Tastatur und eine Maus benutzt – entweder auf einem Mac oder einem Windows-PC – und haben Zugriff auf eines dieser Geräte.
- ✔ Sie wissen, wie man ein sogenanntes Smartphone benutzt – ob nun mit einem Apple- oder Android-Betriebssystem – und haben Zugriff auf ein solches.
- ✔ Sie wissen, wie man einen Internetbrowser wie Firefox, Chrome, Microsoft Edge, Opera oder Safari benutzt.
- ✔ Sie wissen, wie Sie Programme und Apps auf Ihrem Computer und Ihrem Smartphone installieren.
- ✔ Sie wissen, wie Sie etwas über eine Suchmaschine, zum Beispiel Google, suchen können.

Konventionen in diesem Buch

Ich möchte Ihnen an dieser Stelle ein paar der Konventionen erläutern, die Sie in diesem Buch entdecken werden:

- ✔ Begriffe, die anschließend näher definiert werden, oder Hervorhebungen sind *kursiv* gedruckt.
- ✔ Codes und Internetadressen erscheinen in der sogenannten `Listingschrift`.
- ✔ Bezeichnungen von Optionen und Befehlen, auf die Sie in einer Benutzeroberfläche stoßen, sind als KAPITÄLCHEN formatiert.

Symbole, die in diesem Buch verwendet werden

Die folgenden Symbole finden Sie links neben dem Text. Sie heben wichtige Informationen für Sie hervor.

Die Glühbirne finden Sie dort, wo ich Ihnen weiterführende Tricks verrate, die das Thema interessanter machen oder es verdeutlichen sollen. In den Tipps finden Sie ein paar praktische Abkürzungen, von denen Sie bisher vielleicht noch nichts wussten.

Das Erinnerungssymbol hebt Informationen hervor, die Sie sich merken sollten.

Hier heißt es: Aufgepasst! Das Warndreieck soll Sie davor bewahren, häufige Fehler zu begehen, und gibt Ihnen manchmal sogar Tipps, um begangene Fehler wieder rückgängig zu machen.

Wie es weitergeht

Cybersicherheit für Dummies ist so verfasst, dass Sie das Buch nicht von vorne bis hinten durchlesen müssen. Sie müssen nicht einmal das gesamte Buch lesen.

Wenn Sie das Buch gekauft haben, weil Sie einen wie auch immer gearteten Cybersicherheitsvorfall erlitten haben, können Sie direkt zu Teil IV springen, ohne alles davor lesen zu müssen. (Es ist aber durchaus ratsam, den Rest hinterher zu lesen, da Sie mithilfe der Lektüre verhindern können, erneut Opfer eines Cyberangriffs zu werden.)