VORWORT

Cyber-(Online-, Internet-, Netz-)Kriminalität ist auch im deutschsprachigen Raum an der Tagesordnung: 2019 wurden in Österreich laut neuester polizeilicher Kriminalstatistik 28.439 Kriminalfälle im Internet angezeigt (2018 waren es 19.600 – das bedeutet eine Steigerung um 48 Prozent!). In Deutschland wurden 2019 bundesweit 294.665 Straftaten mit „Tatmittel Internet" erfasst, das sind 8,4 Prozent mehr als im Vorjahr.

Das sind die höchsten Werte der letzten Jahre, auch ohne Berücksichtigung der Dunkelziffer. Zumeist als Angriff auf Unternehmen, jedoch immer häufiger auch mit der Zielrichtung Privatpersonen und Angestellte. Gerade in Zeiten des Homeoffice und Homelearning steigt die Gefahr für Privatpersonen massiv an. Und gerade diese kennen sich mit Sicherheit im Netz noch nicht ausreichend aus, kennen nur einige Geschichten aus der Tagespresse.

Von Kriminalität im Netz kann jeder betroffen sein, da die Hacker und Betrüger ihre potenziellen Opfer nicht immer nach dem finanziellen Vermögen, sondern oft nach dem leichtesten Zugriff aussuchen. Oder einfach mit Massenmails wie einem großen Netz arbeiten und schauen, was sich in den Maschen der Aussendungen verfängt.

Hilfreich ist es daher, wenn man die gängigen Angriffsmethoden kennt und sie so einfach(er) identifizieren kann. Und noch besser ist es, wenn man weiß, mit welchen Tools und Methoden man sich gegen Angriffe schützen kann. Oft sogar im Vorhinein, sodass die Angriffe von Beginn an ins Leere laufen.

Mit diesem Ratgeber möchten wir in einfacher und verständlicher Sprache aufzeigen, mit welchen Fallen und Tricks Hacker und Betrüger arbeiten. Dies geschieht zuerst einmal mit Hilfe plastischer Beispiele aus dem realen Leben. Diese Geschichten ergänzen wir um Erklärungen, wie diese Fallen funktionieren, wie die Hacker Sie und Ihren Computer beeinflussen wollen. Und natürlich zeigen wir Ihnen hierbei auch, wie Sie diese Fallen erkennen und sich vor ihnen schützen können. Damit Sie bei einem Angriff zwar eine schöne Geschichte für die Runde unter Freunden, jedoch keinen Schaden haben.

Sie möchten kompakte und konkrete Empfehlungen erhalten, wie Sie sich im Vorhinein möglichst umfassend schützen können? In unserem Kapitel „Empfehlungen und Tipps für Nutzer“ zeigen wir Ihnen auf, wie Sie Computer und Smartphone mit einfachen Mitteln sichern. Damit Ihnen nichts passieren kann, wenn Hacker und Betrüger mit einer neuen Masche, einer neuen Geschichte einen Angriff starten.

Sie haben Kinder? Dann sollten Sie nicht nur an Ihre Sicherheit denken, sondern sich auch über die besonderen Gefahren für Heranwachsende Gedanken machen. Unerwünschte Inhalte, Mobbing im Internet, Hassprediger und Spielesucht muss man nicht tatenlos hinnehmen, sondern kann seine Kinder hiervor schützen. Wir zeigen Ihnen, was Sie tun können.

Mögen Sie Anglizismen, d.h. englische Fachausdrücke im (auch) deutschen, österreichischen oder Schweizer Sprachgebrauch? Wir nicht! In der Regel erklären wir Ihnen Sachverhalte in verständlicher deutscher Sprache und setzen die englischen Fachausdrücke nur in Klammer als Ergänzung dazu. Oder wir verwenden die englischen Fachbegriffe mit direkter Übersetzung ins Deutsche. So können Sie sich voll auf das Verstehen und Vermeiden der Fallen konzentrieren.

Oft lassen sich Fallen mit einfachen Maßnahmen im Vorhinein vermeiden. Diese Maßnahmen haben wir in Checklisten zusammengefasst, um Ihnen einen noch besseren Überblick zu ermöglichen.

Das Wissen in diesem Buch und die verwendeten Beispiele gelten international und sind nicht an politische oder geografische Grenzen gebunden. Betrüger und Hacker sind überall dort aktiv, wo sie sich Profit versprechen. Die Hilfen und Unterstützungsangebote für Sie sind jedoch national. Da sich das Buch an deutschsprachige Leserinnen und Leser richtet, verweisen wir unter „Adressen und Links“ im Serviceteil dieses Buches auf Angebote aus Deutschland, Österreich und der Schweiz.

Wien, im Juli 2020 *Manfred Lappe, Walter J. Unger*