Antivirenprogramme: Ein falsches Gefühl der Sicherheit

Viele Menschen vertrauen kostenpflichtigen Sicherheitsprogrammen, damit die Computernutzung und die Smartphone Nutzung abgesichert werden. Das Vertrauen in diese Programme ist dann so groß (“Ich habe dafür ja Geld bezahlt, dann bin ich bestimmt gut geschützt!”), dass die eigenen Handlungen häufig gar nicht mehr ordentlich hinterfragt werden. Man wird unvorsichtig. Dabei gibt es zwei relativ simple Regeln, mit denen man die eigenen digitalen Handlungen bestens kontrollieren kann, um sich abzusichern. Oft sind es keine fiesen Programmierer, die das Betriebssystem auf der Ebene des Programmiercodes austricksen, sondern es sind Betrugsmaschen, die den Menschen in die Irre führen, sodass das Opfer selbst die Tür zum digitalen Betrug öffnet.

Keine Fremdbestimmung

Wenn eine E-Mail, eine SMS oder eine Meldung bereits mit den Worten “Sofort” beginnt, ist Vorsicht geboten. Alle Formulierungen, die bei Ihnen als Leser eine große Dringlichkeit und Eile bewirken sollen, sind mit sehr hoher Wahrscheinlichkeit unseriös. Nicht nur die Fremdbestimmung, man solle und müsse sofort mit einer Handlung beginnen, sondern auch sehr exakte Handlungsanweisungen, was zu tun sei, sind mit Vorsicht zu genießen. Wenn Sie sich dies merken und sich niemals adhoc in der digitalen Welt zu **schnellen Aktionen** oder zu **exakt beschriebenen Handlungen** hinreißen lassen, dann ist der Gewinn an Sicherheit größer als durch den besten Virenscanner.
Der Hintergrund zu diesen beiden Hinweisen ist der folgende: Bei digitalen Problemen kann man das betroffene Gerät immer ausschalten, vom Netz/Strom trennen, und schon ist die Gefahr gebannt. Viren, Trojaner und andere Schadprogramme können keine weiteren Schäden anrichten, wenn der Computer/das Smartphone ausgeschaltet wurden. Und somit ist jede Begründung einer “Eile” ungerechtfertigt. Im ausgeschalteten Zustand kann man sich in aller Ruhe, mit klarem Kopf und mit Hilfe von erfahrenen Ansprechpartnern um das Problem kümmern und eine angebrachte Herangehensweise erarbeiten. Es können Stunden, Tage oder gar Wochen verstreichen, bevor das Problem schlussendlich in aller Ruhe gelöst werden kann. Denn anders als der Virus im menschlichen Körper, “vermehren” sich die digitalen Viren und anderen Schadprogramme **nicht mehr**, wenn der befallene “Wirt” inaktiv ist. Wenn das Gerät ausgeschaltet ist, dann ist die Gefahr in fast allen Fällen erst einmal komplett gebannt. Im besten Falle entnehmen Sie noch den Akku des Geräts. Die Regel lautet also immer: Ruhe bewahren und erstmal nichts anklicken. Notieren Sie sich möglichst genau (vielleicht sogar mit Fotos), was passiert ist, schalten Sie das Gerät aus und kontaktieren Sie einen Ansprechpartner mit diesen Details.

Zweiter Kanal

Die ideale Ergänzung zu der ersten Regel ist, sich über einen zweiten Kanal zu informieren und zu erkundigen, ob die Meldung/der Fehler/die Aussage wirklich stimmt. Im Klartext und praxisnah bedeutet das zum Beispiel:
a) Ich erhalte eine E-Mail mit der Aussage, ich müsse sofort tätig werden, da ein Zugriff auf mein Bankkonto erfolgt ist. Nur, wenn man jetzt sofort über einen Link das Passwort ändert, kann das Bankkonto gesichert werden, so steht es in besagter Mail. Mit “zweiter Kanal” ist nun gemeint, dass ich zum Telefonhörer greife und damit den Kommunikationskanal wechsle, und mich auf diesem zweiten Weg **per Anruf** bei der Bank informiere, ob diese Probleme wirklich existieren.

b) Mir wird beim Surfen im Internet eine Meldung angezeigt, dass mein Computer von einem Virus befallen sei und ich mich nur schützen kann, wenn ich sofort eine Bereinigung durchführe, die in der selben Meldung vorgeschlagen und beschrieben wird. In diesem Fall ist mit “zweiter Kanal” gemeint, dass ich meinen eigenen Virenscanner, den ich ja kenne und von dem ich weiß, wie ich auf ihn zugreife, starte und ihn befrage, ob mein Computer wirklich gefährdet ist. Ich “befrage” ihn, in dem ich einen Suchlauf meines Computers starte und **meinem** Virenscanner, den ich kenne, vertraue und nicht der Warnmeldung.
c) Amazon (oder DHL oder Paypal) informiert mich, dass eine Rechnung offen stünde, die ich noch zu zahlen hätte. Weitere Informationen gibt es, indem man auf den im gleichen Text hinterlegten Link klickt. Alles wirkt sehr plausibel, da ich letzte Woche etwas bestellt habe und sogar der Betrag/Betreff der E-Mail stimmt. Trotzdem wähle ich den Weg des “zweiten Kanals” und gehe selbstständig zur Internetseite von Amazon/DHL/Paypal, tippe die Internetadresse selbst in den Browser ein und melde mich mit meinen Zugangsdaten an. (Ich klicke also nicht den Link an, der mir in der E-Mail angeboten wird.) Dort schaue ich nun, ob eine Information über eine angebliche offene Rechnung vorliegt. Jeder Anbieter hat auf seiner Internetseite einen eigenen Nachrichtenbereich, in dem solche Meldungen angezeigt werden.
d) Es erscheint plötzlich eine Meldung, die von Microsoft zu stammen scheint und die behauptet, dass man festgestellt habe, mein Computer sei von einem Problem betroffen. Die Meldung enthält eine Telefonnummer, bei der man direkt bei Microsoft anrufen kann. Die Hilfe sei kostenfrei. Mit “zweitem Kanal” ist in einem solchen Fall gemeint, dass ich nicht sofort auf diesen ersten Vorschlag (der meist eine immense Dringlichkeit in der Formulierung enthält) eingehe, sondern mir **Zeit lasse**. Ich notiere die Meldung des angeblichen Problems im exakten Wortlaut oder fertige ein Bildschirmfoto davon an, schalte danach den Computer aus. Nun nutze ich mein Smartphone oder einen anderen Computer und recherchiere mit den notierten Daten bzw. dem Bildschirmfoto, ob diese Meldung vertrauenswürdig ist. Im besten Fall hat man einen Ansprechpartner, den man mit dem Bildschirmfoto kontaktieren kann. Wir können für unsere Mitglieder eine erste schnelle Einschätzung geben, wenn wir solche Informationen per E-Mail erhalten. Zwar können wir keine individuellen Probleme aus der Ferne lösen, eine kurze Stellungnahme, eine Einschätzung des Falls sowie einen wegweisenden Ratschlag, ob ein Computerexperte vor Ort nötig ist, können wir aber für unsere Mitglieder liefern.

Nur wenn die Information aus beiden Kanälen übereinstimmen, kann ich mir recht sicher sein, dass es sich um keinen Betrug handelt.

Quelle: https://levato.de/antivirenprogramme-ein-falsches-gefuehl-der-sicherheit/