Ein Fall aus der Praxis des (Senioren-)Sicherheitsberaters;
heute: Abfischen von Kontodaten (Folge 82 der Reihe „Aber sicher!“)

Nicht selten werde auch ich Versuchsopfer von Kriminellen und so erhielt ich als Sparkassenkunde Anfang des Jahres eine E-Mail von „Support xodangun1@mein.gmx“. In der E-Mail war als Absender „sparkasse.de 2019“ angegeben, der im Rot, das die Sparkassen als Markenzeichen verwenden, gehalten war. Darin wurde mir mitgeteilt, „dass wir (Anm.: die Absender) uns gezwungen sahen, Ihr (Anm.: mein) Konto aus technischen Sicherheitsgründen zu deaktivieren.“ Da ich den Bestätigungsprozess noch nicht durchlaufen habe, seien meine Nutzerkonten temporär gesperrt worden. Sollte ich mich nicht binnen 14 Tagen melden, werde die zwischenzeitliche Sperre in eine unumkehrbare umgewandelt. Über den angezeigten Button „Fortfahren“ könnte ich den Identifikationsprozess durchlaufen, was Voraussetzung für die Freischaltung meiner Konten sei. Selbstverständlich sei dieser Vorgang für mich kostenlos. Schlussendlich entschuldigten sich die betrügerischen Absender für die Unannehmlichkeiten und bedankten sich „herzlichst“ für Geduld und Aufmerksamkeit.

Derartige oder ähnliche E-Mails habe ich in den vergangenen Jahren schon mehrmals erhalten. Sie alle haben das Ziel, sich über die Kontodaten Zugang zu den Bankkonten zu erschleichen. Hätte ich also im vorliegenden Fall auf den Button „Fortfahren“ geklickt und dann die folgenden Fragen beantwortet, hätte ich die Betrüger praktisch dazu eingeladen, sich meines Ersparten zu bedienen. Da hätte ich nicht schlecht gestaunt, wenn mein Guthaben plötzlich auf Nimmer-Wiedersehen verschwunden gewesen wäre. Und eine Rückbuchung ist bei dieser Art von Betrug so gut wie aussichtslos.

Sind Sie also skeptisch beim Erhalt von derartigen E-Mails und geben Sie niemals Ihre Kontodaten Unbekannten preis. Diesen unumstößlichen Grundsatz sollten Sie sich einprägen, dann brauchen Sie den Umgang mit der modernen Computertechnik auch nicht zu scheuen.

Christoph Fuchs