Blog

Cyberangriffe auf Bankkunden – das sind die aktuellen Betrugsmaschen

15.06.2021

von

Beller, Tanja

Schlagworte

Cybersicherheit
Phishing
Digitalisierung
Verbraucher
Künstliche Intelligenz
Cyberattacken
Cyberkriminalität
Geldanlage
Onlinebanking
Sicherheit Verbraucher

Wenn es um das Thema Cybersicherheit geht, hören viele schnell weg: Meldungen über erfolgreiche Angriffe, gehackte PCs und verlorenes Geld betreffen doch nur andere und nicht mich. Eine trügerische „Sicherheit“, in der wir uns alle aus Bequemlichkeit nur zu gerne wiegen. Denn die Cyberkriminellen arbeiten hochprofessionell, global vernetzt und nutzen alle Möglichkeiten der Digitalisierung. Das Bundeskriminalamt (BKA) hat im Cybercrime-Lagebericht 2020 eine Zunahme von Cyberkriminalität um 8 Prozent im Vergleich zum Vorjahr festgestellt. Die Kriminalität verlagere sich zunehmend in den digitalen Raum und die Intensität der Angriffe würde steigen. Manche Angriffsformen sind seit Jahren bekannt, werden den neuen technischen Entwicklungen beständig angepasst und dadurch immer ausgefeilter.

Mehr in unserem Lexikon Cyberkriminalität

Phishing-Attacken kommen in regelmäßigen Wellen

Der „Oldtimer“ unter den Betrugsangriffen, aber leider kein Auslaufmodell: Laut BKA ist das durchschnittliche Mail-Spam-Aufkommen im Corona-Jahr 2020 um 17 Prozent gegenüber dem Vorjahr gestiegen. Kriminelle haben die Ausnahmesituation der Pandemie gezielt ausgenutzt, um Internetnutzer auf betrügerische Links zu locken. Geben ahnungslose Internetnutzer hier dann persönliche Daten, Passwörter, Kreditkartennummern oder ähnliches ein, werden diese von den Angreifern unbemerkt „abgefischt“. Im Besitz der sensiblen Informationen versuchen sie, an das Geld der betreffenden Person zu gelangen.

Lesen Sie weiter: Tipps zum Schutz vor Phishing im Netz.

Warum die Phishing-Attacken trotz aller Sensibilisierungsmaßnahmen erfolgreich sind, liegt in der Natur des Menschen begründet: Wir sind neugierig. Gerade Informationen, die reißerisch aufgemacht sind und Ängste schüren oder bedienen, erscheinen besonders interessant. Deshalb hat die globale Pandemie unzählige Anknüpfungspunkte für neue Phishing-Mails-Inhalte geboten. Doch es müssen gar nicht ausgeklügelte oder besonders polemische Fake-News sein, ganz sachliche Nachrichten – zum Beispiel die Information einer Versandbestätigung zur Online-Bestellung – verführen uns zum schnellen und unüberlegten Klicken. „Think before you click“ kann dazu beitragen, nicht in eine Cyberfalle zu tappen.

„Falsche Bankmitarbeiter“ – Anrufe reißen nicht ab

Auch diese Betrugsmasche ist nicht neu, und dennoch gibt es regelmäßig neue Opfer: Kriminelle kontaktieren Bankkundinnen und -kunden per Telefon und geben sich als Bankangestellte aus. Oftmals wurde die Telefonnummer so manipuliert, dass es so aussieht, als würde tatsächlich von der Bank angerufen (siehe Call-ID-Spoofing). Häufig werden bei diesen

Anrufen Sicherheitsgründe vorgeschoben, um persönliche Daten, Kontoinformationen oder Passwörter für den Online-Banking-Zugang zu erschleichen. Die Anrufenden arbeiten dabei höchst geschickt, teilweise werden die Anrufe vorab per Brief angekündigt, um die scheinbare Seriosität des Anrufs zu erhöhen.

Alle Alarmglocken sollten klingeln, wenn der Anrufer – mit welcher Begründung auch immer – verlangt Zugriff über den PC mittels einer Fernwartungssoftware zu bekommen. Wird dies zugelassen, ist das vergleichbar mit einer sperrangelweit geöffneten Haustür: eine Einladung für Diebe, hereinzuspazieren. Ohne Wissen der Besitzerin oder des Besitzers kann auf diesem Weg eine Spionagesoftware auf den Computer installiert werden, die später persönliche Daten mitliest bzw. ausspioniert.

Hier gibt es mehr Infos zu der Betrugsmasche mit „Techniker-Anrufen“

Der beste Tipp ist hier der einfachste: Auflegen und sich nicht unter Druck setzen lassen. Natürlich werden in Service-Hotlines einer Bank auch persönliche Daten (Name, Straße, Geburtsdatum) zur Identifizierung des Anrufenden abgeglichen. Aber Angestellte einer Bank werden in keinem Fall eine komplette Telefon-Banking-PIN, die Onlinebanking-PIN oder eine Transaktionsnummer (TAN) erfragen.

Im Zweifel ist es ratsam, die Bank selbst telefonisch zu kontaktieren und nachzufragen. Dabei aber nicht die Rückruftaste drücken, denn bei einer manipulierten Nummernanzeige wird die korrekte Nummer vorgegaukelt (siehe Call-ID-Spoofing). Am besten von der Website oder aus den eigenen Unterlagen die korrekte Telefonnummer der Bank raussuchen und die Nummer selbst wählen.

Mehr Infos zum Schutz vor angeblichen Bankmitarbeitern finden Sie hier.

Anlagebetrug über betrügerische Handelsplattformen

Diese Betrugsform scheint in den letzten Monaten in Deutschland an Fahrt aufgenommen zu haben: Gefakte Anzeigen mit Prominenten weisen auf angeblich enorme Gewinne mit Geldanlagen zum Beispiel in Kryptowährungen hin. Klicken Interessierte auf solche Anzeigen, geraten sie schnell auf betrügerische Online-Trading-Portale. Nach einer Registrierung folgt in Kürze der Anruf eines angeblichen „Brokers“ oder persönlichen „Anlageberaters“. Tatsächlich versucht dieser nichts anderes, als die interessierte Person von anfangs kleinen Anlagen zu immer größeren Investitionen zu überreden. Die Website der Handelsplattformen sind dabei so professionell aufgezogen, dass hohe Gewinne vorgegaukelt werden.

Das Betrugssystem ist sehr ausgeklügelt und perfide: Durch die regelmäßigen Anrufe wird ein persönlicher Kontakt oder gar eine Vertrauensbeziehung aufgebaut, dies wird kombiniert mit professionellem Cyberbetrug. Dennoch gibt es eine Reihe von Warnsignalen, die Anleger davon abhalten können, auf diese Betrüger hereinzufallen.

Hier erfahren Sie mehr über die Betrugsmasche: So werden Anlagesuchende geködert