Achtung: Neue Betrugs-Angriffe haben es auf Ihre Daten abgesehen

01.03.2023

(NRW) Es gibt aktuell **neue Betrugs-Angriffe –** die es auf unsere Daten abgesehen haben. Unser **BRH-Mitglied Georg Scholl** macht uns darauf aufmerksam und mahnt uns zur Vorsicht.

Aktuell sind **Kunden der Sparda-Banken** ins Visier von Cyberkriminellen geraten. Auf der Suche nach neuen Opfern versuchen Betrüger, Kunden der Sparda-Banken zur Preisgabe von Kundendaten zu bewegen. Diese wollen sie dann für ihre kriminellen Handlungen nutzen.

Bei der aktuellen Betrugsmasche haben die Täter die Mails ohne Betreffzeile versendet. In der Nachricht wird ein **angebliches Update für das photTAN-Verfahren** thematisiert. Die Bankkunden sollen das Aktivierungsverfahren aktualisieren. So sei weiterhin ein hoher Sicherheitsstandard garantiert.

In der E-Mail drohen die Kriminellen aber auch, dass das Konto zum 1. März deaktiviert würde, wenn man seinen "PhotoTAN-Aktivierungsbrief" bis dahin nicht "bestätigt" hätte. Im Anschluss müssten Kunden zur Bankfiliale gehen, um ihr Konto wieder entsperren zu lassen. Um das Verfahren zu starten, sollen die Kunden nur auf den beigefügten Button klicken.

Natürlich stammt diese Nachricht nicht von der Sparda-Bank und ist lediglich der schlecht gemachte Versuch von Kriminellen, an die Kontodaten ihrer Opfer zu kommen. Zu erkennen ist dies an der Art, wie die Nachricht verfasst wurde. Sie wurde ohne Betreff verschickt, die persönliche Anrede der Kunden fehlt und zudem ist die Nachricht voller Rechtschreib- und Grammatikfehler. Auch der Druckaufbau mit einer extrem kurzen Frist ist typisch für eine Phishingmail. **Potentielle Opfer sollten sich nicht beunruhigen lassen und die Mail direkt unbeantwortet in den Spam-Ordner verschieben.**

Nun warnt auch der Versandriese **Amazon** dringlich vor einer neuen Betrugsmasche, die im schlimmsten Fall großangelegten Datenklau ermöglicht. Der Versandhändler weist auf eine Betrugsmasche hin, die zunächst wie ein einfacher Anruf von der Kunden-Hotline aus Deutschland klingt und im schlimmsten Fall eiskalten Datenklau mit sich bringen kann.

Während der Amazon-Kauf vollständig online abgewickelt wird, rufen die Betrügerbanden per Telefon an, um mit einer Masche Kunden ihre Daten abzuluchsen. **Der perfide Plan läuft wie folgt ab**: Zunächst machen die Kriminellen ihr Opfer auf Komplikationen bei der Bestellung aufmerksam. Als Folge dessen braucht es eine Bestellbestätigung mit Datenabgleich. Spätestens hier sollten alle Alarmglocken läuten, denn jetzt geht es um persönliche Daten, sowie die Kontonummer. Anschließend werden die Betroffenen dazu aufgefordert, ihre Überweisung erneut zu tätigen – diesmal allerdings auf ein ausländisches Konto. Als wäre das nicht schon genug, sollen die Kunden dann auch noch eine Fernwartungs-Software installieren. Grund dafür: Schnelle Hilfe beim vermeintlichen Bestellproblem. Mit besagter Software laden sich Betroffene dann aber einen Virus, es werden weitere Daten gestohlen und die Verbrecher haben damit Zugang zum Online-Banking-Account der betroffenen Person.

Zur Nachrichtenübersicht