Ganz neuer Betrug: angeblicher PayPal-Anruf

Die Internet-Kriminellen haben sich schon wieder eine neue Betrugsmasche ausgedacht. Dabei setzen die Betrüger nicht auf Viren oder Trojaner, wie man vielleicht vermuten könnte, sondern auf einen Anruf. Wir wurden selbst vor wenigen Tagen auf diese Weise telefonisch kontaktiert.

Und so lief der Betrug ab, so haben wir es erlebt:
Das Telefon klingelt, eine anonyme Nummer ruft an. Wir nehmen den Anruf an. Zuerst meldet sich nur eine Computerstimme. Sie klingt professionell, so wie man es von großen Firmen kennt, wenn man bei einer Kundenhotline anruft und in der Warteschlange landet.
Die Computerstimme erzählt, dass der Anruf von PayPal sei und zu unserer eigenen Sicherheit geschieht. Angeblich sei unser PayPal-Konto kompromittiert worden. Eine größere Summe Geld, in unserem Fall 700€, sei von Betrügern abgebucht worden. Wir müssten nun unser Konto schützen, um weiteren Missbrauch zu vermeiden. Dafür sollen wir am Telefon die Taste 1 drücken. Auch das klingt soweit eigentlich realistisch. Wenn es ein Problem mit PayPal gibt, könnte man ja erwarten, dass man direkt und schnell angerufen wird.
Doch wir werden stutzig, wollen erst einmal unser PayPal-Konto überprüfen, ob es tatsächlich eine Abbuchung gab. Wir überlegen kurz, legen dann aber auf. Falls es wirklich einen Betrug gab und wir diesen sogleich bei der Kontrolle unseres PayPal-Kontos feststellen, dann können wir immer noch in einem weiteren Schritt selbst aktiv werden. Wir überprüfen unser PayPal-Konto und können keine Abbuchung feststellen. Nun wird der Fall klar und was uns bereits schwante, bestätigt sich: Es ist ein neuer Betrugsversuch.
Eine darauffolgende Recherche zeigt: Auch andere Menschen haben diesen Anruf erhalten, es ist ein Betrugsversuch, der gerade besonders “en vogue” ist. Wie es weitergeht, wenn man nicht auflegt, darüber können wir nur spekulieren. Einige andere Opfer berichten, dass man danach mit einer echten Person verbunden wird, die einen dazu überreden will, Überweisungen zu tätigen. Die Falle schnappt demnach offenbar nicht sofort zu, sobald man auf die “Taste Nummer 1” drückt, sondern es erfolgen weitere Schritte, bis der Betrug final wird.

Neu: die Computerstimme
Das Neue an diesem Trick: Eine Computerstimme liest den Text vor. Mit solchen Computerstimmen hat man in letzter Zeit immer häufiger zu tun, wenn es um große Firmen geht, auch bei PayPal. So wird beispielsweise ein Bestätigungscode bei der PayPal-Anmeldung per Anruf von einer solchen Computerstimme übermittelt. Auch in vielen Kundenhotlines hat man es zunächst mit Computerstimmen zu tun, bevor man irgendwann mit echten Mitarbeitern verbunden wird. Der Vorteil für die Betrüger: eine Computerstimme hat keinen Dialekt, wirkt professionell, verspricht sich nie und sagt immer den exakt gleichen Text auf. Daher wirkt der Anruf im ersten Moment, als sei er wirklich von PayPal. Man kann sich als Opfer gut vorstellen, dass dies ein echter, automatischer Sicherheitsanruf sein könnte.

“Woher haben die meine Nummer?”
Eine der häufigsten Fragen, die wir regelmäßig im Zusammenhang mit solchen Anrufen erhalten, lautet: Wie kommen die Anrufer an meine Nummer? Dafür gibt es vor allem drei Erklärungen.

Erstens:
Die Nummer wird “erraten”. Die Betrüger rufen tausende von zufälligen Nummern an. Darunter

sind dann auch genügend tatsächlich existierende Nummern. Diese Anrufversuche erledigen die Betrüger dabei nicht eigenhändig, indem Sie die Nummern eintippen, sondern es gibt “Wahl-Programme”, welche in Millisekunden Telefonnummer per Zufall generieren und per Testanruf versuchen, jemanden zu erreichen. Ob die angerufene Nummer existiert und ob die angerufene Person überhaupt ein PayPal-Konto besitzen, das wissen die Anrufer natürlich nicht. Sie nehmen das in Kauf und bauen auf genügend Zufallstreffer. Denn bei vielen tausenden Anrufen in wenigen Stunden sind immer einige Fälle dabei, die erreichbar sind, ein PayPal-Konto besitzen und Opfer des Betrugs werden. Wenn es nur einen Fall pro Stunde gibt, der auf den 700-Euro-Betrug hereinfällt, dann ist das ein guter Stundenlohn für die Betrüger – könnte man zynisch sagen.

Zweitens:
Die Nummer wurde irgendwann einmal bei einem Datenleck offengelegt und im Internet veröffentlicht. Wenn unsere Handynummer bei einer Firma hinterlegt wurde und diese Firma wurde Opfer einen professionellen groß angelegten Hacks oder hat aufgrund eigener Sicherheitsmängel die Kundendaten nicht gut geschützt, dann geraten die Kundendaten und die Handynummern in den Umlauf und schlussendlich in die Hände der Betrüger. Solche Fälle passieren immer wieder und selbst große Firmen wie die Telekom sind davon betroffen. Oft sind wir gar nicht schuld daran, dass unsere Nummern in die Hände der Betrüger geraten sind.

Drittens:
Ein Bekannter von uns wurde gehackt, bzw. das Adressbuch des Bekannten. In diesem Adressbuch stand auch unsere Nummer.

Was ist zu tun?
Sollten Sie einen solchen Anruf erhalten, so bleiben Sie ruhig, lassen sich zu nichts hinreißen und nicht durch eine überschnelle panische Reaktion dazu hinreißen, auf irgendeine Weise aktiv zu werden. Legen Sie im besten Fall einfach direkt wieder auf. Bedenken Sie: alles an dem Anruf ist frei erfunden. Das bedeutet: Ihr PayPal-Konto, sofern Sie überhaupt eines besitzen, ist durch den Anruf nicht in Gefahr. Eine PayPal-Sprecherin versicherte der Verbraucherzentrale, dass PayPal seine Kunden nicht von sich aus anruft. Auch Ihr Handy und Ihre Daten sind durch den Anruf nicht in Gefahr. Diese Frage erhalten wir auch sehr häufig. Es ist hierbei kein Virus oder Trojaner oder ein ähnliches Schadprogramm im Spiel.

Ähnliche Betrugsmaschen
Die Internetkriminellen setzen in letzter Zeit immer häufiger auf eine Kontaktaufnahme per Anruf oder SMS. Über zwei ähnliche Fälle haben wir bei Levato schon mehrfach berichtet, beide Maschen sind immer noch im Umlauf. Es handelt sich dabei um den **Enkeltrick per WhatsApp** und den angeblichen **Microsoft-Anruf**. Unsere ausführlichen Beiträge dazu können Mitglieder hier im Archiv nachlesen:

Enkeltrick per WhatsApp: *Enkeltrick immer noch per WhatsApp*
Angeblicher Microsoft-Anruf: *Microsoft-Betrug funktioniert 1 Jahr später immer noch millionenfach*