„Die soziale Manipulation hat stark zugenommen“

Markus Bentele von der Kreissparkasse Ravensburg über die Methoden der Onlinebetrüger

WANGEN - Onlinebetrug hat weiterhin Konjunktur, die Kriminellen werden immer professioneller. Betroffen ist davon auch das Onlinebanking, wie Markus Bentele zu berichten weiß. Im Gespräch mit Bernd Treffler spricht der Leiter Zahlungsverkehr und Marktservice der Kreissparkasse Ravensburg über Betrugsmethoden und die menschliche Leichtgläubigkeit.

E-Mails mit Schadsoftware kursieren schon seit einigen Jahren im Netz. Vergangenen Sommer warnte die Polizei in Nordrhein-Westfalen jedoch explizit vor einer „massiven Welle mit gefälschten Rechnungen“. Haben Sie bei der Kreissparkasse Ravensburg auch einen Anstieg beim Betrug mit Onlinebanking festgestellt?
Bei den Betrugsszenarien stellen wir einen Seitwärtstrend fest. Von der Intensität her hat sich dabei nicht viel geändert, aber dafür die Art und Weise. Das Onlinebanking ist weiter sicher, ins Kreuzfeuer geraten mittlerweile jedoch die Menschen. Man spricht hier von „Social Engineering“, einer Art menschlicher Manipulation.

Was heißt das konkret?
Früher wurde nur versucht, über sogenannte Phishingseiten Daten abzugreifen oder über Anhänge oder Links in E-Mails Schadsoftware auf Rechner einzuschleusen. Das ist nichts Neues, Banken haben hier entsprechende Sicherheiten eingebaut. Seit einiger Zeit versuchen Kriminelle aber vermehrt, sich mit einer erfundenen Geschichte das Vertrauen der Menschen zu erschleichen. Die Betrüger geben sich am Telefon oder in einer E-Mail als Mitarbeiter von Computerfirmen, Banken oder der Polizei aus. Es wird dabei ein Szenario aufgebaut, das Menschen unter Druck setzt, persönliche Daten preiszugeben oder Anweisungen zu befolgen. Eine solche soziale Manipulation hat in den letzten Monaten stark zugenommen, die Kommunikation der Betrüger ist hier mittlerweile hochprofessionell. Diese von der Polizei bezeichnete „massive Welle“ hat also wenig mit einer Unsicherheit im Onlinebanking zu tun, sondern zielt auf die Leichtgläubigkeit der Menschen. Mit diesem Problem haben wir seit vergangenem Sommer verstärkt zu tun.

Markus Bentele FOTO: KSK

Die Rücküberweisungsmasche ist auch so eine erfundene Geschichte. Woran erkennt man online beim Überweisungsvorgang, dass Betrüger am Werk sind?
Grundsätzlich erhält der Kunde im Onlinebanking mit seiner Transaktionsnummer, der TAN, weitere Sicherheitsinformationen anhand derer man die Richtigkeit der Überweisung kontrollieren kann. Beispielsweise sollte man sich bei der IBAN-Nummer auch den Ländercode anschauen.

Kann man eine solche falsche Überweisung rückgängig machen?
Wenn jemand unsicher ist, ob alles mit der Überweisung okay ist, sollte man bei der entsprechenden Bank anrufen und nachfragen. Je schneller wir davon erfahren, desto höher ist die Wahrscheinlichkeit, die Überweisung zurückrufen zu können. Hierbei geht es aber um wenige Stunden. Wenn man sich erst nach einigen Tagen meldet, ist es in der Regel schon zu spät.

Habe ich als Kunde die Chance, dass die Bank den verlorenen Überweisungsbetrag erstattet?
Die gesetzliche Regelung ist so: Wenn eine Zahlung vom Kunden autorisiert wurde, wenn also eine sogenannte Transaktionsnummer generiert und vom Kunden eingegeben wurde, dann ist die Bank in der Regel nicht dazu verpflichtet, den Betrag zu erstatten.

Man hört von Betrugsfällen im Onlinebanking, bei denen sich Banken kulant gezeigt haben ...
Dazu kann ich nur sagen, dass wir bei der Sparkasse jeden Fall separat prüfen, es kommt hier wirklich auf den Einzelfall an. Wir versuchen jedoch immer, eine kundenfreundliche Lösung zu ermöglichen.