Tarnen, täuschen und betrügen

Die Caller-ID am Display der Angerufenen zu fälschen, wird seit 2021 eine immer häufigere Vorgehensweise von Betrügern. Es gibt Möglichkeiten, sich davor zu schützen.

Wenn das Handy klingelt und eine dem Anrufer unbekannte Nummer auf dem Display erscheint, werden die wenigsten von einem betrügerischen Anruf ausgehen und schon gar nicht dann, wenn sich angeblich die Polizei zu erkennen gibt: Frau W. erhielt eines Tages einen Anruf aus einer Wiener Polizeiinspektion. Nichts ahnend, nahm die betagte Frau das Telefonat an. Am anderen Ende der Leitung: Betrüger. Sie gaben sich als Polizisten aus und erklärten, dass ein Einbruch in die Wohnung von Frau W. geplant wäre, denn sie hätten einen Zettel mit Adressen potenzieller Opfer bei einer Einbrecherbande gefunden. Um auf Nummer Sicher zu gehen und die Vermögenswerte zu sichern, wäre es möglich, diese der Polizei zur Verwahrung zu übergeben. Die Täter überzeugten die Frau, die Telefonnummer sah zudem plausibel aus. Es kam zur Übergabe und die Frau händigte den Kriminellen Bargeld, Sparbücher und Schmuck im Wert von rund 500.000 Euro aus. Frau W. ist mit ihrer Geschichte nicht allein – so wie ihr geht es unzähligen anderen.

Unter Caller-ID-Spoofing, versteht man die Fälschung der Identität des Anrufers, so dass am Display des Telefons der angerufenen Person eine vorgetäuschte Rufnummer erscheint. Am Display des Opfers kann, wie im Fall von Frau W., die richtige Nummer einer Polizeidienststelle erscheinen, aber es ist auch möglich, dass die Absenderinformation Polizei, Europol, Finanzamt oder dergleichen aufscheint. Ruft der Betroffene die Nummer zurück und ist sie vergeben, landet er beim tatsächlichen Inhaber der Nummer. Welche Rufnummer die Täter wählen, hängt vom Betrugsmodell ab. Besonders kritisch stellt sich die betrügerische Verwendung von gültigen internationalen sowie nationalen Behördennummern heraus, denn hier wird das Vertrauen in öffentliche Institutionen missbraucht.

Betrug. Spoofing wird vielfältig eingesetzt, wie etwa beim Tech-Support- oder Ladebonbetrug und besonders oft beim „falschen Polizisten“. Auch beim Phishing wird das Spoofing oft angewendet – von vermeintlichen Paketdiensten, Finanzämtern oder Banken. Das Trügerische: Durch die Vorgehensweise gelingt es den Tätern, dass die betrügerischen Phishing-SMS etwa im Original-Chat-Fenster der Bank am Handy erscheinen. Ziel der Betrüger ist es, ihre Herkunft zu verschleiern und ihre Opfer über die Authentizität des Anrufs oder SMS zu täuschen.

Bei Anrufen von unbekannten Nummern sollte man skeptisch sein

Hierarchisch und arbeitsteilig. Die Betrugshandlungen haben weltweit ihren Ausgangspunkt und die Täter gehen arbeitsteilig vor. Größer organisierte Tätergruppen verfügen über eigens im Ausland eingerichtete Call-Center, von wo aus die betrügerischen Anrufe getätigt werden. Diese Zentralen konnten oft im osteuropäischen Raum und in Indien ausgeforscht werden. Für die Bewegung der Opfergelder sind zumeist andere Stellen zuständig. So sammeln beim „falschen Polizisten“ Abholer das Vermögen der Opfer an ihren Wohnadressen ein. Auch Geldwäschenetzwerke werden eingesetzt, die den Fluss der illegal lukrierten Gelder über Kryptowährungen verschleiern.

Steigende Anzahl an Fällen. Seit 2021 nimmt die Anzahl an Spoofing-Fällen zu: Wurden 2021 4.054 Fälle und 2022 4.294 Fälle angezeigt, so wurde im Juni 2023 mit 4.072 Anzeigen das Niveau der Vorjahre erreicht.

Grundsätzlich ist in Österreich die Nutzung einer Telefonnummer, an der man kein Nutzungsrecht besitzt, rechtswidrig. Durch die international dynamischen Routings und die manipulierten Metadaten ergeben sich für die Strafverfolgung Erschwernisse: Die gespooften Anrufe können technisch nicht bis zum Quellnetzbetreiber und damit zum Täter zurückverfolgt werden.

Die Problematik beginnt bei der Übernahme von Anrufen aus dem Ausland, die mit verfälschten Rufnummern in das österreichische Netz übergeben werden. In diesen Fällen wird die (ge-/verfälschte) Rufnummer legitim weitergeleitet, da regionale Betreiber keine Veränderungen von inhaltlichen Parametern vornehmen dürfen und bisher auch keine Sicherheitsmaßnahmen, wie eine Rufnummernüberprüfung, vorgeschrieben waren.

Kooperation zwischen Mobilfunkanbieter und Bundeskriminalamt. Das Bundeskriminalamt steht mit Vertretern aller österreichischen Mobilfunkanbieter in Kontakt. Nachdem die Dimensionen von Spoofing-Fällen ersichtlich wurden, wurde ein Treffen al-

FOTO: TANTONIODIAZ - STOCK.ADOBE.COM

ler Stakeholder einberufen, um Lösungsansätze sowohl für die technischen als auch die rechtlichen Problemstellungen zu erarbeiten. Das Ergebnis war ein mehrstufiges Lösungskonzept: Zum einen soll die Bevölkerung zeitnah durch Warnmeldungen auf diversen Betreiberplattformen und polizeilichen Kanälen gewarnt werden, zum anderen wurden konkrete Maßnahmen erörtert, die Spoofing unterbinden sollen.

Verordnungsvorschlag. Die Rundfunk- und Telekom-RegulierungsGmbH (RTR) brachte einen Verordnungsvorschlag ein, durch den Betrügern das Caller-ID-Spoofing in Österreich erschwert wird. So ist künftig jeder Anruf mit österreichischer Rufnummer, der sich aus dem Ausland ins regionale Netz einwählt, von den Providern auf Plausibilität zu prüfen. Wird ein Anruf aus dem Ausland über das Home-Location-Register des heimischen Empfängernetzwerkes an dessen Routingstelle zur Weiterleitung übergeben (Homerouting), wird bei einer österreichischen Nummer überprüft, ob diese in Österreich aktiv ist. Stellt sich dabei heraus, dass die Rufnummer gleichzeitig in zwei Ländern verwendet wird, wird von Spoofing ausgegangen und die Nummer wird blockiert.

Außerhalb des Homeroutings wird die Rufnummer unterdrückt und der Anruf als „anonym“ weitergeleitet; ebenso, wenn es sich um eine österreichische Rufnummer außerhalb des Mobilfunks, beispielsweise Festnetznummer, 05er-Nummer etc. handelt. Durch diese Vorgehensweise können sich Betrüger im Ausland nicht mit 0732 (Festnetznummern Österreich) oder 0664 (Handynummern Österreich) nach Österreich einwählen. Dadurch können österreichische Kommunikationsteilnehmer darauf vertrauen, dass ein Anruf mit österreichischer Nummer tatsächlich aus dem Inland stammt oder einer Anti-Spoofing-Prüfung unterzogen worden ist. Derzeit sind ausländische Telefonnummern und Textnachrichten davon noch ausgenommen.

Derzeit gibt es keine Möglichkeit, den Missbrauch einer Telefonnummer zu verhindern. Die RTR hat eine Meldestelle eingerichtet, bei der sich Betroffene von Spoofing und allen Formen des Telefonnummernmissbrauchs sowie belästigenden Anrufen und Betrugs-SMS melden können *(www.rtr.at)*. Durch die Meldung können nicht nur Spoofing-Wellen und neue Trends erkannt werden, sondern auch Gegen- oder Präventionsmaßnahmen eingeleitet und Gesetzesinitiativen eingebracht werden. Sofern der Verdacht einer strafbaren Handlung besteht, sollte Anzeige bei der Polizei erstattet werden.

Schutzmaßnahmen. Wer sich schützen möchte, hat die Möglichkeit, über den Telekom-Provider einen kostenpflichtigen Dienst in Anspruch zu nehmen, der potenzielle Betrugsversuche erkennt und vor betrügerischen SMS oder Anrufen warnt. Weiters gibt es Apps, die solche Funktionen anbieten. Jedoch gibt es keine Garantie, dass jeder Betrug verhindert werden kann. Grundsätzlich gilt: Bei Anrufen mit unbekannten Nummern gilt gesunde Skepsis. Bei fragwürdigen Inhalten sollte der Anruf beendet werden. Sollte nach persönlichen Zugangsdaten, Passwörtern oder Geld gefragt werden, handelt es sich um einen Betrugsversuch und der Anruf sollte sofort beendet werden. *Romana Tofan*