„Call-ID-Spoofing“

Vorsicht vor gefälschten Nummern im Display

„Call-ID-Spoofing“: Bei dieser kriminellen Methode sind die angezeigten Rufnummern technisch manipuliert

Das Telefon klingelt. In Ihrem Telefondisplay sehen Sie eine Rufnummer, vielleicht sogar eine, die Sie sofort, aus dem Gedächtnis heraus, meinen, konkret zuordnen zu können. Sie sehen zum Beispiel die Nummer einer Ihnen bekannten oder verwandten Person, die eines Unternehmens, Ihrer Bank, einer Behörde oder der örtlichen Polizeidienststelle. Sie ordnen die Nummer automatisch ein, weil sie diesen Telefonkontakt häufig nutzen oder er für Sie wichtig ist.

Stopp! Sie glauben, zu wissen, wer am anderen Ende der Leitung ist?

Nicht, dass Sie sich beim Ablesen der Telefonnummer im Display irren. Denn eine hier angezeigte Rufnummer ist kein sicherer Faktor, jemand eindeutig zu identifizieren. Rufnummern im Display können manipuliert sein. Diesen Vorgang nennt man „Call-ID-Spoofing“. Das ist verboten, aber technisch möglich. So schreibt das Telekommunikationsgesetz in Paragraf 120: „Andere an der Verbindung beteiligte Anbieter dürfen übermittelte Rufnummern nicht verändern…“ Nur leider lassen sich Kriminelle nicht durch dieses Verbot abhalten. Personen mit ein wenig IT-Kenntnissen können diese Manipulation ohne großen Aufwand bewerkstelligen.

Das heißt, jemand täuscht Ihnen mittels App oder anderer Software einen Anruf vor, indem er das Display Ihres Telefons so manipuliert, dass zum Beispiel eine Ihnen geläufige Telefonnummer erscheint. Und das entweder in komplett unveränderter Form oder leicht verändert mit Zahlendreher oder Verlängerung durch weitere Zahlen, die Sie aber nicht sofort wahrnehmen. Praktisches Beispiel: Lassen Sie uns einmal annehmen, Sie hatten schon einen persönlichen Kontakt zu mir. Meine dienstliche Rufnummer lautet 0228 – 15 76 17. Damit Sie mich für Rückfragen in Sachen Kriminalprävention noch einmal kontaktieren können, haben Sie meine Nummer und meinen Namen im Telefonbuch Ihres Telefons gespeichert. So weit, so gut.

Die technikaffinen Anrufenden sitzen in Callcentern!

Da meine dienstliche Telefonnummer auch über das Internet recherchiert werden kann, können sich auch die Täterinnen oder Täter diese Angaben beschaffen. Dann können sie mittels einer Software einen Anruf von einem anderen Anschluss so tarnen, dass meine Telefonnummer auf Ihrem Telefondisplay eingespielt ist. Das heißt, Sie sehen meine Nummer, obwohl ich Sie von meinem Anschluss aus gar nicht anrufe. Und jetzt sagt Ihnen eine weibliche Stimme am Telefon: „Guten Tag, mein Name ist Wichterich, ich bin von der Polizei in Bonn.“ Was denken Sie, mit wem Sie sprechen?

Wichtig zu wissen ist hierbei auch: Beim Einspielen der so manipulierten Rufnummer auf Ihrem Display reagiert das Telefonbuch Ihres Telefons ebenfalls, sollten Sie diese Rufnummer und Namen als Kontakt verknüpft haben. Auf meine Telefonnummer bezogen bedeutet das also: Wenn die Kriminellen meine Telefonnummer in Ihrem Display einspielen, reagiert darauf auch Ihr Telefonbuch. Es wird dann auch mein Name angezeigt, obwohl ich Sie gerade gar nicht anrufe. Aber die Täterinnen und Täter wollen Sie genau das glauben machen und dadurch Ihr Vertrauen gewinnen. Die Anrufenden sitzen jedoch in einem Call Center oder sind technikaffine Einzeltäterinnen und -täter.

Dieses Call-ID-Spoofing ist ein Faktor, der häufig beim Telefonbetrug eine große Rolle spielt.

Die Masche ist Mittel zum Zweck, Sie zu betrügen!

Die Anrufenden wollen, dass Sie personenbezogene Daten, auch Kontodaten, herausgeben. Sie wollen Sie dazu bewegen, Geld, Debitkarte mit PIN oder andere Wertgegenstände, die Sie zu Hause haben, an (falsche) Bankmitarbeitende, (falsche) Polizeibeamtinnen oder -beamte, (falsche) Mitarbeitende anderer Behörden und Institutionen oder an eine Kurierperson herausgeben. Sie fordern Sie auf, Geld zu

überweisen. Sie verleiten Sie, Vermögenswerte aus Ihren Bankschließfächern zu holen und zu übergeben, oder wollen einen Fernzugriff auf Ihren PC erreichen.
Die Täter versuchten mittlerweile sogar mehrfach selbst die Polizei auf den Leim zu führen…
So sind in den letzten Monaten bundesweit wiederholt einzelne (vergebliche) Versuche gestartet worden, fernmündlich durch Anrufe bei Polizeidienststellen personenbezogene Daten abzuschöpfen, in dem die Anrufer vorgaben, angeblich Mitarbeiter einer anderen Polizeibehörde aus NRW oder eines anderen Bundeslandes zu sein.

Und so können Sie sich schützen:

- Verinnerlichen Sie bitte: Die angezeigte Rufnummer im Display ist keine Garantie, wer die Anrufenden wirklich sind. Auch wenn diese Nummer tatsächlich die der Staatsanwaltschaft oder der Polizei ist, bedeutet dies nicht, dass der Anrufende tatsächlich für diese Behörde arbeitet.
- Öffentliche Einrichtungen, Banken oder Verbraucherzentralen fordern grundsätzlich nie telefonisch zur Zahlung von Geldbeträgen auf. Kreditinstitute, Ämter oder seriöse Unternehmen fordern Sie weder am Telefon noch per E-Mail oder SMS auf, persönliche Zugangsdaten oder finanzielle Informationen preiszugeben. Im Zweifelsfall kontaktieren Sie Behörde, Institution oder Unternehmen direkt über einen verifizierten Kontakt.
- Geben Sie keine vertraulichen Informationen am Telefon preis, auch wenn Anrufende vorgeben, diese nur zum Abgleich zu benötigen. Stattdessen vereinbaren Sie lieber ein Gespräch in der Bank oder fragen schriftlich an.
- Installieren Sie keine Fernwartungssoftware, wenn man Sie telefonisch dazu auffordert. Oft geben sich Betrügende als Technikerin oder Techniker aus und fordern dazu auf, die Software zu installieren, um ein angebliches Problem am PC beheben zu können. Fragen Sie Im Zweifel immer selbst bei der Behörde oder dem Unternehmen nach, ob am geschilderten Sachverhalt etwas dran ist.
- Egal, was man Ihnen erzählt oder welchen Druck man ausübt: Bleiben Sie ruhig und handeln Sie überlegt.
- Notieren Sie sich den Zeitpunkt des Anrufs (Datum/Uhrzeit), Details wie den Namen und Rufnummer des Anrufenden sowie, wenn dazu aufgefordert, die Kontonummer, auf die etwaige Geldforderungen überwiesen werden sollen.
- Wenn Sie einen weiteren Anschluss oder ein Mobiltelefon haben, überprüfen Sie *während* des Anrufs über diese weitere Leitung, ob sich die angezeigte Nummer anrufen lässt. Erhalten Sie kein Besetztzeichen, haben Sie wohl gerade einen Call-ID-Spoofing-Anruf erhalten.
- Manipulationen von Rufnummern können bei der Bundesnetzagentur angezeigt werden.
- Wenden Sie sich bei Betrugsdelikten mittels Rufnummernmanipulation an die nächste Polizeidienststelle und erstatten Sie Strafanzeige.
- Wurden in einer Stresssituation dann doch persönliche Daten weitergegeben, zögern Sie nicht, umgehend das Konto und die dazugehörigen Zahlungskarten zu sperren: entweder direkt bei Ihrem Kreditinstitut oder beim Sperr-Notruf 116 116*.
- Bei Ihnen unbekannten Nummern auf dem Mobiltelefon können Sie diese auch über eine Smartphone-Anwendung mit Funktionen zur Anrufer-ID überprüfen (Truecaller). Diese identifiziert unbekannte Nummern, die von Kriminellen genutzt werden, und ermöglicht, den unerwünschten Anruf zu blocken.

Weitere Informationen:

https://www.polizei-beratung.de/presse/detailseite/betrug-am-telefon-gefaelschte-rufnummer-im-display/ [polizei-beratung.de]
https://www.bundesnetzagentur.de/DE/Vportal/TK/Aerger/Faelle/Manipulation/start.html [bundesnetzagentur.de]

Marita Wichterich (Dipl.-Jur.), Kriminalhauptkommissarin
Polizei Bonn - Direktion K - KK Kriminalprävention/Opferschutz
Telefon: 0228 – 15 7617 oder - 7676
seniorenberatung.bonn@polizei.nrw.de