Betrüger am Telefon

Der angebliche freundliche Support-Mitarbeiter, ein plötzlicher Los-Gewinn oder ein angeblicher Polizist, der sich um die Verwahrung von Vermögenswerten kümmern möchte: Die Strategien der Telefonbetrüger sind vielfältig und besonders dreist.

Wenn das Telefon klingelt, sind es nicht immer nur bekannte Stimmen, die mit jemandem sprechen wollen. Derzeit erhalten viele Menschen Anrufe von Kriminellen, die sich als Polizistinnen und Polizisten ausgeben. Die Anrufkriminalität hat viele Facetten: Ob als angebliche Support-Mitarbeiterinnen und -Mitarbeiter namhafter Unternehmen, angebliches Personal einer Betreiberfirma für Ladebons oder einer Lotterie, oder als Verwandte – Betrügerinnen und Betrüger versuchen, über verschiedenste Wege illegal Geld zu lukrieren. Seit Kurzem wird eine Vorgehensweise beobachtet, bei der Call-Bots eingesetzt werden.

Auswertungsteam des Bundeskriminalamts. Um diese Betrugsphänomene bekämpfen zu können und auf neue Vorgangsweisen schnell reagieren zu können, wurde im Bundeskriminalamt in der Abteilung zur Bekämpfung der Wirtschaftskriminalität im Sommer 2021 ein Auswertungsteam mit drei Ermittlern eingerichtet. Seit Anfang 2022 unterstützt das nun fünfköpfige Team rund um Chefinspektor Horst Hakala Ermittlungen zu verschiedenen bundesländerübergreifenden Betrugsphänomenen. Eine operative Fallbearbeitung findet nicht statt.

Tägliche Abfragen. Täglich wird eine Abfrage im Sicherheitsmonitor (SIMO) nach Datum (Vortag) und Delikt gestartet. Abgefragte Delikte sind etwa das missbräuchliche Abfangen von Daten (§ 119a StGB), Betrug (§§ 146, 147, 148 sowie 148a StGB) oder auch Sachwucher (§ 155 StGB), Geldwäscherei (§ 165 StGB) und Datenfälschung (§ 225a StGB).

Diese Delikte sind in der Abfrage beliebig erweiterbar. Die Ergebnisse werden anschließend bearbeitet und wenn der Sachverhalt nicht klar ersichtlich ist, wird Einsicht in die PAD-Akte genommen. PAD (Protokollieren, Anzeigen, Daten) ist das Protokollierungssystem der Polizei. Jede Eintragung wird anhand einer Liste einem Phänomen zugeordnet. Dadurch kann nicht

Betrugsanruf: Ältere Menschen werden von Betrügern oft unter Druck gesetzt.

nur schnell Prävention geleistet werden, sondern auch eine rasche Abklärung bei neu auftretenden Vorgangsweisen. „Neben dieser Tätigkeit führen wir eine Sonderauswertung zum Thema gefälschte Covid-19-Dokumente durch und stellen sie dem fachlich zuständigen Referat zur Verfügung“, sagt Chefinspektor Hakala. „Außerdem fertigen wir einen wöchentlichen Lagebericht an, der dem Covid-19-Führungsstab bereitgestellt wird.“

Technical Support-Scam. Die wenigsten Menschen sind technisch versiert. Das nützen die Täter aus, indem sie ihren Opfern Schäden an ihren technischen Geräten vortäuschen. Sie tarnen sich als Mitarbeiter/-innen namhafter Unternehmen und kontaktieren ihre Opfer telefonisch. Im Gespräch wird behauptet, der Computer des Opfers sei mit einem Virus infiziert und könne nur durch eine kostenpflichtige Fernwartung behoben werden. Für dieses Service verlangen sie Geld. Die Täter verunsichern die Opfer und diese überweisen das Geld für die Behebung eines nicht existenten Defektes. Die Täter versuchen auch, über sogenannte Remote Access Tools (wie AnyDesk) die Kontrolle über den PC des Opfers zu erlangen und in weiterer Folge selbst die Überweisungen zu tätigen.

Falsche Gewinnversprechen. Andere Täter täuschen den Opfern vor, als zufällig ausgewählte Person bei einem Gewinnspiel gewonnen zu haben. Die Täter nehmen häufig unter einer ausländischen Telefonnummer Kontakt mit ihren Opfern auf und teilen ihnen mit, dass sie bei einer Lotterie gewonnen hätten. Für die Auszahlung des Gewinnes sei aber vorab für Transport oder Notar ein festgelegter Geldwert vorzustrecken. Die Opfer werden anschließend beispielsweise dazu aufgefordert Kryptowährungsgutscheine zu erwerben und die darauf angeführten Codes den Betrügerinnen und Betrügern telefonisch zu übermitteln. Zu einer Auszahlung des Gewinnes kommt es nicht.

Ergaunerte Ladebons. Dass Bitcoin-Ladebons ebenso ein beliebtes Ziel von Kriminellen sind, zeigt auch der Betrug mit ihnen. Diese Betrugsmasche ist nicht neu, hat sich jedoch im Laufe der Zeit gewandelt: Waren es früher eher Handy-Wertkarten, iTunes-Gutscheine oder Ähnliches, stehen nun Bitcoin-Bons im Visier.

Die Täter geben sich auch hier als Mitarbeiter von Vertriebsunternehmen aus, die Ladebons für virtuelle Währungen vertreiben, und geben vor, dass die ausgelieferten Ladebons keine Gültigkeit mehr hätten, weshalb sie ausgetauscht und aus dem System genommen werden müssten. Sie kontaktieren die Inhaber oder Angestellten von Trafiken, Tankstellen und Postpartnerstellen und setzen diese unter Druck, drohen mit dem Verlust des Jobs oder einer finanziellen Haftung. Sie argumentieren, dass durch die Bekanntgabe der Ladebons, diese „aus dem System“ genommen und gegen neue ausgetauscht würden. In Wirklichkeit werden die Ladebons von den Tätern eingelöst. Die Kriminellen verschleiern auch bei dieser Betrugsmasche ihre Telefonnummer, sodass die Opfer den Eindruck haben, der Anruf käme tatsächlich von einem Vertragspartner.

FOTO: HIGHWAYSTARZ /STOCK.ADOBE.COM

Falscher Polizistentrick. Seit einiger Zeit häufen sich in Österreich Fälle von Betrügerinnen und Betrügern, die sich am Telefon als Polizistinnen oder Polizisten ausgeben. Bei diesem Betrug gehen die Täter professionell vor: Zumeist beziehen die Kriminellen die Telefonnummer ihrer Opfer aus (digitalen) Telefonbüchern. Die Anrufe selbst kommen oft aus dem Ausland. Mithilfe von Internettelefonanbietern erscheint auf dem Display der Opfer eine österreichische Telefonnummer.

Die Täter schützen bei dem Anruf häufig vor, dass eine Einbrecherbande in der Umgebung ihr Unwesen treibe und als Nächstes bei der oder dem Angerufenen einbrechen würde und daher Gefahr für Hab und Gut bestehen würde. Sie üben während des Gespräches Druck auf ihre Opfer aus und überzeugen sie schließlich, ihre Vermögenswerte an „Polizisten“ oder Mittäter zu übergeben.

Bei einer Abwandlung dieses Tricks erklären die Kriminellen, dass es eine Erhebung ergeben hätte, dass Bankangestellte Geld veruntreut hätten und die Polizei es nun sichern würde. Das Opfer wird angewiesen, das Kontoguthaben abzuheben und auszuhändigen. In einer weiteren Variation gibt sich der Anrufer als Staatsanwalt aus und berichtet von der Einbrecherbande, die die Vermögenswerte der Opfer im Visier hätte. Die Opfer sollten zudem eine bestimmte Zeit Stillschweigen über den Vorfall bewahren, was den Tätern kostbare Zeit zur Flucht verschafft.

Telefonbetrugs-Auswertungsteam des Bundeskriminalamts: Manfred Klein, Dominik Hiehs, Jürgen Schmid.

Der Kautionsbetrug ähnelt dem Enkel- und Neffentrick bzw. Polizistentrick in seiner Herangehensweise. Betrügerinnen und Betrüger bedienen sich einer geschickten Gesprächsführung, um an Informationen zu gelangen, die sie gezielt gegen das Opfer verwenden.

Diese Betrugsmaschen betreffen vorwiegend betagte Menschen, die im guten Glauben abheben und das Gesagte oftmals nicht hinterfragen. Auch hier beziehen die Kriminellen die Telefonnummern aus (digitalen) Telefonbüchern. Sie teilen dem Opfer mit, dass ein naher Angehöriger einen Unfall mit Verletzten verursacht hätte. Um zu verhindern, dass dieser nun ins Gefängnis müsse, soll die angerufene Person eine Kaution bezahlen. Hat sie nicht genügend Bargeld zu Hause, wird sie aufgefordert das Geld von der Bank zu holen. Die meist beträchtlichen Summen werden dann an die Mittäter übergeben.

Vernetzung mit Banken. Banken spielen vor allem in der Vereitelung des Polizistentricks oder Kautionsbetrugs oft eine maßgebliche Rolle. Daher ist die Sensibilisierung der Bankbediensteten ein Eckpfeiler der Prävention der Initiative *GEMEINSAM.SICHER in Österreich*. „Ältere Personen, die einen solchen Betrugsanruf erhalten und unter Druck gesetzt werden, sind verunsichert und ängstlich“, erklärt Dr. Gerald Rak, MSc, MA, Leiter des Büros im Bundeskriminalamt für Finanzermittlungen und Vermögenssicherung. „Die Bankangestellten sind meist die ersten Ansprechpersonen, an die sich die Betroffenen zur Behebung des Geldes wenden. Daher ist es umso wichtiger, die Bankbediensteten regelmäßig zu sensibilisieren und rasch über neue Vorgangsweisen zu informieren.“

Neue Vorgehensweise: Call-Bot-Anrufe. Die Täter bedienen sich bestimmter Computerprogramme – „Call-Bots“ – um potenzielle Opfer anzurufen und sie mit einer Tonbandaufnahme in englischer Sprache zu konfrontieren. Hierbei ist die Nummer, die auf dem Display der Angerufenen erscheint, mit technischen Mitteln gefälscht und daher nicht rückverfolgbar. Die Opfer werden aufgefordert, eine bestimmte Tastenkombination zu drücken, um so misstrauische Personen, die bei solchen Anrufen sofort auflegen würden oder der englischen Sprache nicht mächtig sind, bereits im Vorfeld zu selektieren. An-

TELEFONBETRUG

Präventionstipps

- Lassen Sie sich keinesfalls unter Druck setzen. Teilen Sie der Anruferin/demAnrufer mit, dass es ungünstig ist und bieten Sie einen Rückruf an. Echte Beamte werden Verständnis haben, Kriminelle werden den Druck erhöhen, damit Sie nicht auflegen.
- Beenden Sie das Telefonat.
- Die Polizei übernimmt und verwahrt zu keinem Zeitpunkt Bargeld oder Wertgegenstände für Sie und bittet Sie auch nicht um Überweisungen auf (ausländische) Bankkonten.
- Wenn Sie nach Bargeld oder Wertgegenständen sowie Kontoguthaben gefragt werden, beenden Sie das Gespräch.
- Wenn Sie von einer Hotline angerufen und aufgefordert werden, eine Tastenkombination auf Ihrem Telefon einzugeben, beenden Sie sofort das Telefonat.
- Kein seriöses Unternehmen ruft Kundinnen und Kunden ohne Vorankündigung wegen eines technischen Defektes an.
- Hinterfragen Sie auch, wie Ihr Gegenüber von einem technischen Defekt oder Virus auf Ihrem Computer wissen kann. In der Regel erhalten Sie diese Meldungen direkt von Ihrem Gerät.
- Lassen Sie niemals eine unangemeldete Fernwartung von unbekannten Personen oder solchen, denen Sie nicht vertrauen, auf ihrem Computer zu. Es könnten Daten von Ihrem Gerät ausgelesen werden. Die Polizei fordert Sie niemals auf eine Remote-Software zu installieren.
- Lassen Sie sich Namen und Telefonnummer der Anruferin/des Anrufers geben. Rufen Sie direkt beim deklarierten Unternehmen an und fragen Sie nach dem Bediensteten.
- Klären Sie Verwandte über diese Betrugsmaschen auf.
- Wenden Sie sich im Schadensfall an die nächste Polizeidienststelle und erstatten Sie eine Anzeige.

FOTO: BETTINA FRÖHLICH

schließend melden sich englischsprachige Täter, die sich als (Interpol-) Polizistinnen oder -Polizisten oder Parlamentsangehörige ausgeben. Dem Opfer wird dabei mitgeteilt, es wäre in strafbare Handlungen, wie etwa Geldwäsche, Betrugs-, Suchtmittel- oder Gewaltdelikte, verwickelt. Um sich selbst zu entlasten und wieder ein normales Leben – manchmal mit Verweis auf eine neue Identität – zu führen, wäre es unbedingt notwendig, das Geld zu überweisen. Auf die Nachfrage, warum englisch gesprochen würde, wird dem Opfer mitgeteilt, dass das so sein müsse, es sei ein internationaler Fall und es würden Beamtinnen oder Beamte von Europol mithören.

„Die Täter agieren situationsangepasst und stellen sich auf das Opfer ein. Zu jedem Argument des Opfers erwidert der Täter ein passendes, plausibles Gegenargument. Er kann mitfühlend oder auch aggressiv klingen“, sagt Kontrollinspektor Dominik Hiehs vom Auswerteteam. „Doch eines wird immer der Fall sein: Es ist furchtbar dringend und muss sofort erledigt werden. Dadurch wird Stress, Zeitdruck und Angst beim Opfer aufgebaut.“

Durch die zeitnahe Auswertung der Call-Bot-Anrufe erzielte das Auswerteteam bereits im Jänner 2022 Erfolge: In enger Zusammenarbeit mit der Geldwäschemeldestelle des Bundeskriminalamtes konnten für österreichische Geschädigten rund 110.000 Euro zurückgeholt werden, die sich vermutlich auf Money-Mule-Bankkonten befanden.

Call-ID-Spoofing. Um ihre wahre Identität zu verschleiern, manipulieren die Täter bei den Betrugsanrufen ihre Telefonnummer. Bei Anrufen eine falsche Nummer anzuzeigen, ist relativ leicht und mit wenig technischem Aufwand verbunden. Wenn die Manipulation im eigenen Netz eines Anbieters stattgefunden hat, besteht für diesen kaum eine Möglichkeit zu kontrollieren, ob die signalisierte Telefonnummer stimmt oder nicht. Dazu können existierende – auch aus dem Ausland stammende – Telefonnummern verwendet werden, obwohl die Inhaberin oder der Inhaber der Nummer für den Anruf gar nicht verantwortlich ist. Auch Fantasienummern, also Telefonnummern, die nicht vergeben sind, können eingesetzt werden.

Romana Tofan