TRAU, SCHAU, WEM!

REPORT Neue Phishingmethoden. Internetkriminelle werden immer professioneller, die technischen Möglichkeiten spielen ihnen in die Hände. Niemand ist davor gefeit, einem Betrugsversuch zum Opfer zu fallen. Misstrauen hilft.

Überwachung durch die Hintertür

In der politischen Diskussion wird regelmäßig die Forderung nach einer Aufweichung des Postgeheimnisses im Bereich der digitalen Medien erhoben. Neben den Inhalten von E-Mails und SMS geht es dabei nicht zuletzt um die Zugriffsmöglichkeit der Behörden auf Messenger-Dienste wie WhatsApp, Signal oder Telegram. Dazu bräuchte es einerseits eine gesetzliche Grundlage und andererseits die technischen Voraussetzungen. Man spricht in diesem Zusammenhang auch von einer Hintertür, englisch: Backdoor.

Gründe für eine solche Forderung lassen sich leicht finden. Gerne verwendet werden Schlagwörter wie Terrorismus, Geldwäsche oder Kinderpornografie. Auch wenn die Forderung wohl vielfach in bester Absicht erfolgt, sehen wir sie sehr kritisch. Sind die ersten Schritte gesetzt und die Infrastruktur geschaffen, kann es leicht zu weiteren Verschärfungen der Maßnahmen kommen. Mit pessimistisch angehauchter Fantasie kann man dies gedanklich bis hin zu einem „Social Scoring" weiterspinnen, also einem Überwachungsystem, in dem das persönliche Verhalten jedes Menschen mit Plus- oder Minuspunkten bewertet wird. Beispiele dafür existieren auf dieser Welt bereits.

Cybercrime, so der englische Ausdruck für Internetkriminalität, ist schon seit Langem eine boomende Branche – und das weltweit. Kein Wunder, ist es doch so etwas wie das „Homeoffice für Kriminelle", ortsunabhängig, anonym und bequem vom Schreibtisch aus zu erledigen. Zu den beliebtesten Varianten zählt das Phishing. Dieser Überbegriff steht für „password fishing", also das Angeln nach Passwörtern, Konto- und sonstigen persönlichen Daten gutgläubiger Mitmenschen. Das kann auf unterschiedliche Weise vor sich gehen. Ziel ist es in jedem Fall, die Opfer direkt oder auf Umwegen (etwa im Zuge eines späteren Anrufs, bei dem die erbeuteten Informationen genutzt werden) um möglichst viel Geld zu erleichtern.

Viele Wege, ein Ziel: Ihre Daten und Ihr Geld

Als Reaktion auf derartige Aktivitäten haben der Gesetzgeber, die Finanzmarktaufsichtsbehörden und die Banken auf nationaler wie europäischer Ebene diverse Anstrengungen unternommen, um die Sicherheit für die Konsument:innen zu erhöhen. Beispiele dafür sind die Abschaffung der Papier-TANs oder die Einführung der Zwei-Faktor- Authentifizierung beim Online-Banking.
Das Problem dabei: Sobald eine Lücke geschlossen ist, setzen die Kriminellen ihrerseits alles daran, neue Methoden zu entwickeln, um munter weitermachen zu können. Dabei greifen sie erwartungsgemäß auf moderne technische Möglichkeiten zurück, bis hin zum Einsatz von künstlicher Intelligenz.
Das bedeutet, dass die Zeiten grammatikalisch fehlerhafter E-Mails vorbei und Fälschungen umso schwieriger durchschaubar sind. Auch setzen die Kriminellen auf das Überraschungsmoment. Man rechnet oft einfach nicht damit, dass auf solche Weise ein Betrugsversuch angebahnt wird.

Welche Betrugsmaschen gibt es?

Internetkriminalität ist ein weites Feld, es ist kaum möglich, alle Formen aufzuzählen, in denen sie daherkommt. Im Folgenden schildern wir jene Betrugsmaschen, mit denen man aktuell am häufigsten konfrontiert wird.

Druckaufbau durch Autorität. Per E-Mail, WhatsApp oder SMS kommt von einer (staatlichen) Institution eine Nachricht herein, in der man zu sofortigem Handeln aufgerufen wird. Das kann FinanzOnline sein mit der Aufforderung zur Kontoaktualisierung, um eine Rückzahlung zu erhalten. Das kann eine Bank sein zwecks Datenrichtigstellung, weil sonst die Kontosperre droht. Oder es wird eine Erbschaft, ein Gewinn etc. in Aussicht gestellt, wofür die Bekanntgabe persönlicher Daten (auf einer gefälschten Internetseite) die Voraussetzung ist. Allen gemeinsam ist, dass zeitlicher Druck aufgebaut wird, weil ansonsten ein Anspruch verfällt oder eine unangenehme Situation eintritt.

Angehörige in Not. Was gibt es Schlimmeres als die Benachrichtigung über einen Notfall naher Angehöriger? (Ein Beispiel dafür finden Sie in der Rubrik „Vorsicht, Falle!" auf Seite 2 in diesem Heft.) Die Person hatte angeblich einen Unfall, wurde im Ausland verhaftet oder ausgeraubt; sie braucht jedenfalls dringend Geld, um sich rasch aus der Notlage befreien zu können. Oft wird vorgespiegelt, dass das Smartphone der Betroffenen defekt sei. So wird die fremde Rufnummer erklärt. Dem Opfer soll unter keinen Umständen Zeit gegeben werden, die Sachlage zu überdenken, mit anderen zu besprechen oder etwa durch einen Kontrollanruf bei der bisherigen Rufnummer zu überprüfen. Die Kontaktaufnahme seitens der Kriminellen erfolgt entweder per Textnachricht (z. B. über SMS oder WhatsApp) oder mittels Anruf. Dies ist einer der Fälle, in denen die erwähnte künstliche Intelligenz zum Einsatz kommt. Mittlerweile genügen wenige Sekunden Tonaufnahmen von einer Person, um deren Stimme künstlich nachahmen zu können. Nachdem es heute gang und gäbe ist, in sozialen Medien wie Instagram oder Tiktok Videos von sich zu veröffentlichen, können Kriminelle die Aufnahmen beispielsweise dazu nutzen, um den Eltern am Telefon vorzugaukeln, dass die Tochter oder der Sohn anruft und um Hilfe bittet.

Wenn Gier blind macht. Nicht nur die Sorge um Angehörige, auch der Wunsch nach Reichtum und Ansehen kann den Blick auf die Realität trüben. Das erklärt, warum Betrugsmaschen nach dem Muster des „Prinzen aus Nigeria", der unbekannten Personen die Überweisung einer beträchtlichen Geldsumme verspricht, auch nach bald 30 Jahren noch funktionieren. Eine unerwartete Erbschaft, das Geldgeschenk eines reichen Philanthropen, ein Krypto-Wallet mit hohem Guthaben – all das kann einem bald schon gehören, sofern man bereit ist, nicht nur persönliche Daten bekanntzugeben, sondern vorab eine Gebühr für die „Entsperrung", die „rechtliche Absicherung" etc. auf ein ausländisches Konto zu überweisen. Vorschussbetrug nennt man diese Masche. Wenn man bezahlt, bekommt man weder das in Aussicht gestellte Geld, noch sieht man das eigene wieder.

Liebesbetrug. Nicht zuletzt macht auch die Liebe blind. Mithilfe von künstlich erstellten Bildern und gefälschten Profilen werden auf Partnerplattformen und in den sozialen Medien Kontakte geknüpft. Erst wird versucht, eine emotionale Bindung zum Opfer aufzubauen. Danach folgen Geschichten über persönliche Schicksalsschläge, teure, aber notwendige Heilbehandlungen oder Ausgaben, die getätigt werden müssten, obwohl man gerade knapp bei Kasse sei – all das natürlich verbunden mit der Bitte um Geld.

Finanzbetrug. Ob Armin Assinger, Mirjam Weichselbraun, Christoph Grissemann oder Günther Jauch, so wie andere Prominente werden sie für gefälschte Videos missbraucht, die einmal

Handeln Sie niemals unter Zeitdruck!

mehr mithilfe künstlicher Intelligenz erstellt wurden. Ziemlich glaubhaft sprechen diese Personen darin über das Thema Geldanlage und die Möglichkeiten, schon mit kleinen Beträgen viel Ertrag zu erwirtschaften (siehe auch dazu die Rubrik „Vorsicht, Falle!"). Auch hier kann man letztlich nur draufzahlen, ebenso wie bei Bitcoin-Wallets, die man „zufällig" auf der Straße findet. Tatsächlich werden sie von Kriminellen gezielt dort platziert. Überprüft man sie online, wird einem ein hohes Guthaben vorgespiegelt. Möchte man sich dieses auszahlen lassen, ist dies nur gegen Vorabzahlung einer Gebühr möglich, mit der letztlich nur die Konten der Kriminellen gefüllt werden.

Wie kann ich mich schützen?

Die wichtigste Regel lautet, sich niemals unter zeitlichen Druck setzen zu lassen. Die Aufforderung, umgehend zu handeln, ist typisch für die meisten Betrugsszenarien. Bleiben Sie misstrauisch und setzen Sie keine weiteren Schritte, ohne die Behauptungen überprüft oder eine weitere Meinung eingeholt zu haben. Beachten Sie grundsätzlich auch folgende Punkte:

- Antworten Sie niemals auf verdächtige E-Mails, auch wenn Sie diese immer wieder bekommen und sich davon belästigt fühlen. Markieren Sie solche Nachrichten in Ihrem E-Mail-Programm als Spam oder löschen Sie sie gleich. Das Öffnen und Lesen solcher Nachrichten hat in den meisten Fällen noch keine Konsequenzen.
- Klicken oder tippen Sie auch keinesfalls auf Links, die in solchen E-Mails sowie in SMS oder WhatsApp-Nachrichten enthalten sind. Sie gelangen damit auf gefälschte Internetseiten oder es wird Spionagesoftware auf Ihrem Gerät installiert.
- Wenn Sie unsicher sind und aufgestellte Behauptungen überprüfen möchten, dann ignorieren Sie grundsätzlich die in der Nachricht befindlichen Links und Kontaktdaten. Suchen Sie stattdessen im Internet, im Telefonbuch, in Ihren Bankunterlagen etc. nach den offiziellen Kontaktinformationen.
- Halten Sie das Betriebssystem und die Apps Ihrer Geräte immer auf dem aktuellen Stand (am besten über automatische Updates) und verwenden Sie zusätzlich Schutzsoftware und -apps, die dabei helfen können, Bedrohungen zu erkennen.
- Vereinbaren Sie mit Ihren Verwandten Kennwörter für Notfälle, um eine eindeutige Identifikation zu ermöglichen.

Wer tut etwas gegen den Betrug?

Eingangs haben wir bereits erste Schritte erwähnt, die in der Vergangenheit seitens der Finanzmarktaufsicht gesetzt wurden. Die stark steigenden Fälle und Opferzahlen im Bereich Cybercrime haben mittlerweile zu weiteren Maßnahmen geführt. So wurde zur Bekämpfung von **Spoofing** (= Vorspiegelung einer österreichischen Rufnummer – etwa einer Bank –, während der Anruf tatsächlich aus einem ausländischen Netz erfolgt) eine Verordnung erlassen, die diese Möglichkeit unterbindet. Ab September 2024 müssen die Netzbetreiber diese vorgetäuschte Rufnummer unterdrücken.

Das **Bundeskriminalamt** hat eine eigene Meldestelle für Internetkriminalität eingerichtet. Dort können Fälle gemeldet oder auch Informationen zu Betrugsmaschen eingeholt werden (E-Mail: against-cybercrime@bmi.gv.at; allgemeine Informationen zum Thema Internetkriminalität und den Aktivitäten des Bundeskriminalamts auf nationaler und internationaler Ebene unter: bundeskriminalamt.at und dort Klick auf > Delikte & Ermittlungen > Internetkriminalität). Achtung! Die Anzeige eines Betrugsfalls ist auf diesem Wege bisher nicht möglich, sondern muss in einer Polizeidienststelle erfolgen.

Die Website **Watchlist-internet.at** sammelt bekannte Betrugsmaschen und veröffentlicht diese. Sie ist empfehlenswert, um sich einen Überblick über aktuelle Betrugsmaschen zu verschaffen oder andere vor Betrügereien zu warnen – auch wenn man selbst nicht darauf hereinfällt. Ergänzend dazu veröffentlichen wir auf **Konsument.at** regelmäßig aktuelle Warnungen, konkret unter konsument.at/vorsicht-falle sowie monatlich in KONSUMENT.

Die Rundfunk- und Telekom-Regulierungsbehörde **RTR** bietet die Möglichkeit, Rufnummernmissbrauch zu melden, um Maßnahmen dagegen einzuleiten, und veröffentlicht gleichfalls aktuelle Warnungen: rtr.at und dort Klick auf > Telekommunikation und Post > Schlichtungs- und Beschwerdestellen > Meldestelle Rufnummernmissbrauch.

Was tun im Ernstfall?

Zuerst sollten Sie versuchen, den möglichen Schaden zu minimieren:

- Betroffene Zahlungsdienstleister kontaktieren und die Karten sperren (lassen).
- Abklären, ob Rückforderungen möglich sind (von der Bezahlmethode abhängig).
- Die für Zahlungen genutzten Passwörter, PINs etc. ändern.
- Anzeige in einer Polizeidienststelle.

Danach, zur Warnung und zum Schutz anderer:

- Betrugsversuche bei den oben genannten Stellen einmelden.
- Falls Zugangsdaten bei sozialen Medien betroffen sind, die eigenen Kontakte informieren, um Betrugsversuche dort zu unterbinden.
- Eventuell auch die Institution oder Firma informieren, unter deren Namen ein Betrugsversuch gestartet wurde.

Finanziell unterstützt durch die Europäische Union