

Neue Betrugsmasche: „Pig Butchering“

Mithilfe von täuschend echter Werbung und Fake-Profilen erleichtern **Cyberkriminelle** weltweit ihre Opfer um Milliarden

VON BEN KENDAL

Was haben ein „Tagesschau“-Beitrag über die Fluggesellschaft Lufthansa und eine junge Frau namens Jessica gemeinsam? Sie sind beide nicht real. Besagter Beitrag kursierte in den sozialen Medien. Darin hieß es: Bürgerinnen und Bürger könnten durch ein ganz bestimmtes Investment in Lufthansa viel Geld verdienen. Doch dabei handelte es sich – ermöglicht durch Künstliche Intelligenz (KI) – um einen Deepfake, der Menschen in betrügerische Investments locken sollte.

Hinter dem Social-Media-Profil der attraktiven Jessica, die vor einigen Monaten einen BBC-Reporter reinlegen wollte, steckt in Wahrheit eine Tätergruppe, die vermutlich aus China stammt. Sie verwendete Bilder vom Social-Media-Profil einer deutschen Influencerin, um den Journalisten per Instagram zu verführen und zu hohen Geldzahlungen zu bewegen. Die zwei Fälle haben noch eine Sache gemeinsam: Sie sind Teil einer großen Betrugsmasche, die als „Pig Butchering“, als Schweineschlachtung, bekannt ist.

Menschen werden manipuliert

Kriminelle Gangs nutzen die Methode, um durch Manipulation Vertrauen zu Menschen aufzubauen, sie in betrügerische Investments zu locken – und anschließend ihr Geld abzuzocken. Die Gangs kommen meist aus Südostasien und betreiben dort richtige Betrugsfabriken. „Die Täter haben ganze Listen mit psychologischen Tricks“, sagt Ondrej Kubovic, IT-Sicherheitsexperte bei der Firma Eset. „Sie wissen, wie sie ihre Opfer zunächst zu kleinen Zahlungen zwingen – nur, um sie nach und nach zu

mästen.“ Um Vertrauen zu Menschen aufzubauen, bedienen sich Kriminelle dabei einer Strategie, die im Fachjargon auch Social Engineering genannt wird: Sie manipulieren Menschen, damit diese vertrauliche Informationen preisgeben oder ihnen Geld schicken.

Die zahlreichen Tätergruppen hinter dieser Betrugsmasche haben damit riesigen Erfolg. Das FBI schätzte, dass sie im vergangenen Jahr allein in den USA insgesamt 4 Milliarden Dollar von Zehntausenden US-Bürgerinnen und -Bürgern gestohlen haben. In Bayern hatten Menschen durch Pig Butchering bis März insgesamt 29 Millionen Euro verloren, wie das Justizministerium des Landes in einer Mitteilung bekanntgab.

„Social Engineering hat für Täter den Vorteil, dass sie es nicht auf eine Technologie absehen, sondern auf Menschen und ihre Schwachstellen“, sagt Kubovic. „Die Kriminellen sind gut darin, Menschen ausfindig zu machen, die einsam sind und sich einen Partner wünschen.“ Kurz gesagt: Wer sich nach Liebe sehnt, ist anfälliger für Betrüger oder Betrügerinnen. Die geben sich jeweils als attraktiver Menschen aus und machen ihnen Liebesgeständnisse. Kriminelle nutzen die Bedürftigkeit der Opfer aus. Sie überschütten sie mit Komplimenten oder sprechen sogar über Pläne für eine gemeinsame Zukunft.

Sobald die Kriminellen Vertrauen aufgebaut haben, legen sie ihren Opfern ein Investment nahe. „Sie wollen dabei seriös und vertrauensvoll wirken, deswegen fragen sie zunächst nur nach einer kleineren Summe“, erklärt Sicherheitsexperte Kubovic. Die Täter betonen jedoch stets, dass sie selbst diese Summe wachsen lassen könnten. Und dann beginnt der Betrug erst so richtig.



Obacht geben und Unbekannten nicht blindlings vertrauen – nur so kann man sich vor Cyberkriminellen schützen.

SYMBOLFOTO: ANNA NEKRASHEVICH / PEXELS

Täter mästen die Opfer

Wer sich auf das Investment einlässt, bekommt von den Tätern klassischerweise Screenshots mit vermeintlichen Profiten. „Damit versuchen sie, ihren Opfern zu zeigen: Wenn du noch mehr investierst, bekommst du noch mehr zurück“, erläutert Kubovic. Aus diesem Prinzip leitet sich auch der Name „Pig Butchering“ ab: Die Kriminellen mästen ihre Opfer so lange mit Gewinnversprechen, bis sie sie finanziell völlig ausschachten können. Die Transaktionen finden dabei meist über Kryptogeld statt, da es sich besser waschen lässt und für Strafverfolgungsbehörden schwieriger aufzuspüren ist.

Pig Butchering-Opfer erkennen den Betrug meist erst dann, wenn sie ihr Geld aus dem Investment zurückverlangen. Die Täter fordern dazu dann den Ausweis oder Reisepass, um den Profit aus dem vermeintlichen Investment ausschütten zu können. Doch das ma-

chen die Betrüger nur, um die Dokumente zu missbrauchen – sie haben nie vorgehabt, ihren Opfern das Geld zurückzugeben. Für Betroffene ist es dann schon zu spät. Die Aussichten darauf, das Geld von den Kriminellen durch Strafverfolgungsbehörden zurückzuerlangen, sind eher schlecht – eben, weil die Transaktionen so oft über Kryptogeld stattfinden.

Betroffene können den Schaden dennoch begrenzen. Als Beweise können finanziell Geschädigte Chatprotokolle sichern und der Polizei vorlegen. Jedoch genügt das in den allermeisten Fällen nicht, um die Täter aufzuspüren. Trotzdem ist es sinnvoll, so Kubovic, Anzeige zu erstatten. „Das ist in Versicherungsfällen relevant, da viele Finanzinstitute und Versicherungen eine Anzeige fordern, um helfen zu können“, erklärt der Experte.

Im nächsten Schritt ist es wichtig, einen weiteren Missbrauch des eigenen Geldes und der persönlichen Daten zu verhindern. Wer

Tätern zum Beispiel Passwörter zu wichtigen Onlinekonten verraten hat, sollte diese unbedingt schnell ändern. „Wenn man den Kriminellen seinen Ausweis oder Reisepass geschickt hat, sollte man dies zudem melden und neue Dokumente anfertigen lassen. Die Identität kann ansonsten missbraucht werden“, sagt Kubovic.

Auch wenn Pig Butchering global ein zunehmendes Problem wird, können sich Menschen vor der Betrugsmasche schützen. „Die Quintessenz: Vertrauen Sie niemals jemandem, den Sie nicht kennen und der angibt, ein Experte zu sein und ihnen durch eine unverzichtbare Investment-Möglichkeit zu Geld verhelfen kann“, sagt FBI-Agent William J. DelBagno auf der Website der US-amerikanischen Sicherheitsbehörde.

Kriminelle sind kreativ

Eset-Mitarbeiter Kubovic betont, dass kritisches Denken wichtig ist. Gerade die Onlineinteraktionen mit Unbekannten, die zu verlockend sind, um wahr zu sein, solle man hinterfragen. „Kriminelle geben sich oft unheimlich viel Mühe, um ihre Betrugsmasche als echtes Business zu verkaufen: Sie bauen Websites, kreieren mithilfe von KI täuschend echt aussehende Fake-Videos mit vorgegaukelten Kundenreferenzen“, sagt der Experte. Beim Onlinedating rät er Menschen dazu, über neue Kontakte mit Freundinnen oder der Familie zu sprechen. Gerade dann, wenn der Kontakt plötzlich persönliche Informationen fordert oder mit Investments lockt. „Manchmal sehen vertraute Menschen Warnzeichen, die man selbst gar nicht erkennt, weil man sich von den vielen Komplimenten geschmeichelt fühlt“, sagt Kubovic.

Was beim Einkaufen zählt

Anzeigenblattleser sind bereits empfänglich für Sonderangebote (73,1% LpA). Trotzdem legen sie viel Wert auf Markenqualität und Umweltaspekte.

Quelle: Bundesverband Deutscher Anzeigenblätter

- Werbung in **hallo** wochenende wird von den Lesern als besonders nützlich und informativ bewertet
- Mit uns erreichen Sie verschiedene Zielgruppen
- Mit hoher Lokalkompetenz und starkem Nutzwert sind wir ein Sprachrohr für die Menschen in der Region
- Kontrollierte und zuverlässige Verteilung, Prüfung durch die Weigel GmbH, ein unabhängiges Institut für Qualitätsmanagement

hallo wochenende