hessenschau

LKA-Warnung vor "CEO Fraud"

Hessische Firmen im Visier von Cybergangstern

Veröffentlicht am 22.12.16 um 08:26 Uhr

Bild © Imago Images

Das Landeskriminalamt warnt Firmen vor schwerem Cyber-Betrug: Zu den Feiertagen rechnen die Ermittler verstärkt mit Versuchen, Firmen um große Geldbeträge zu bringen. Die Tricks der Gangster sind originell.

Von Jan Eggers

Man will es kaum glauben: Unbekannte schicken ein paar E-Mails, und schon überweisen Firmen bereitwillig sechs- bis siebenstellige Beträge ins Ausland. Der so genannte "Chefbetrug" oder "CEO Fraud" ist ein kriminelles Wachstumsgeschäft, warnt das Landeskriminalamt (LKA) in Wiesbaden. In Hessen verging in diesem Jahr kaum eine Woche, ohne dass den Ermittlern ein neuer Fall bekannt wurde. Und gerade zu den Feiertagen rechnen die LKA-Experten mit einer neuen Welle.

Mit den vor Fehlern strotzenden "Phishing"-Mails, die in privaten E-Mail-Postfächern landen, hat sie kaum etwas gemein. Die Gangster sind gut organisiert und hoch professionell. Sie sind psychologisch geschult und geschickt. Und sie investieren Wochen, zum Teil Monate, in ihre Raubzüge. Diese laufen in der Regel in drei Phasen ab:

Phase 1: Ausspähen und aushorchen

Die Gangster suchen sich eine Firma - ein mittelgroßes Unternehmen, das Geschäftsbeziehungen ins Ausland hat - und forschen diese Firma aus, zunächst über frei zugängliche Quellen wie das Handelsregister oder einfach mit Google. "Man hat unglaublich viele Möglichkeiten, auch als Privatmann Informationen zu erheben", sagt Kriminalhauptkommissar Axel Schröder von der "Zentralen Ansprechstelle Cybercrime" beim Hessischen Landeskriminalamt (LKA) in Wiesbaden.

Eine weitere Möglichkeit, an Informationen zu kommen, sind gefälschte Profile auf Facebook oder Plattformen wie Xing und Linkedin. Als Berater, Headhunter oder vermeintliche Kollegen befreunden sich die Gangster mit Mitarbeitern des Unternehmens – und erfahren so wertvolle Details: von der Durchwahl des richtigen Ansprechpartners bis hin zum Firmenklatsch. Mit diesen Details wiederum können sie die Informationen erfragen, die sie für den Betrug brauchen.

Bild © Imago Images

„Es wird Ihnen eine Geschichte erzählt, mit Daten von Ihnen, die Sie glauben", erklärt der Betrugs-Spezialist Ronny Wolf, der für die Commerzbank bundesweit Firmen im Erkennen von Cyberbetrug schult. So ist zu erklären, dass sich angerufene Firmen nicht über den freundlichen Anrufer wundern, der Details zu Aufträgen und Zahlungsvorgängen erfragt. Zumal an dieser Stelle häufig ein technischer Trick zum Einsatz kommt: Das Display des Telefons zeigt eine gefälschte, vermeintlich harmlose Rufnummer.

Phase 2: Ködern und isolieren

Die Kriminellen warten nun, bis der Chef im Urlaub oder auf Auslandsreise ist und greifen dann an: Ein zuvor ausgesuchter Mitarbeiter der Buchhaltung wird im Namen des Chefs angeschrieben oder angerufen und um Mitwirkung bei einer streng geheimen Transaktion gebeten. Das kann der angebliche Kauf einer Firma im Ausland sein oder auch eine Strafzahlung oder der Erwerb von Lizenzrechten – auf jeden Fall geht es um viel Geld.

Hier könnten aufmerksame Mitarbeiter stutzig werden, denn die vermeintliche Mail des Chefs kommt in Wirklichkeit nicht aus dem Unternehmen, sondern von einer ähnlichen E-Mail-Adresse. Da die Mail Details aus dem Unternehmen enthält, fallen die kleinen Ungereimtheiten aber praktisch nie auf.

Manche Gangster sind noch raffinierter: In einem Fall, von dem der Commerzbank-Betrugsexperte Wolf berichtet, war sich das Opfer sicher, wirklich mit dem Chef zu sprechen, dessen Stimme ihm bekannt vorkam. Kunststück: Vier Wochen zuvor hatte ihm derselbe Anrufer zu einem Jubiläum gratuliert - es war nicht der Chef gewesen, sondern der Betrüger, der den Betrug vorbereitete.

CEO-Fraud nimmt weltweit zu

Das BKA hat seit 2013 etwa 100 Fälle des so genannten "Chefbetrugs" gezählt. 2015 meldet das BKA eine Schadensumme von mehr als 41 Mio. Euro. Weltweit, so schätzen die Ermittler, sind mehrere Milliarden Euro bereits ergaunert worden. Der Schaden ist mindestens sechsstellig, geht aber mitunter in die Millionen. In Frankreich ergaunerten Betrüger in einem Fall gar 120 Mio. Euro.

Damit der Betrug funktioniert, setzen die Gangster auf zwei Psycho-Tricks: Sie suggerieren dem Mitarbeiter, dass er das Vertrauen des Chefs genießt und deshalb nur er helfen kann. Und sie reden ihm ein, dass er mit niemandem über den geheimen Deal reden dürfe, nicht einmal mit dem Chef selbst – am Telefon könnte schließlich jemand mithören. Und keinesfalls dürfe er mit Dritten reden! Sonst drohten ihm empfindliche Strafen.

Der "Chef" fordert den Mitarbeiter auf, die Details der Transaktion mit einem Sonderbeauftragten zu regeln, zum Beispiel mit einem im Ausland ansässigen angeblichen Anwalt. Der sendet dem Opfer einen Wust furchteinflößender Vertrags- und Behördendokumente und bereitet die Zahlung vor, abermals per Mail.

Phase 3: Das Geld einstreichen und nachfassen

Alles, was jetzt noch fehlt, sind die Unterschriften, um die Zahlung frei zu geben. Das Opfer haben die Gangster meist auch deshalb ausgewählt, weil es zeichnungsberechtigt ist, die fehlende Unterschrift vom Chef liefern sie wiederum per Mail – einfach abkopiert aus dem Handelsregister. Der Mitarbeiter ahnt nichts Böses und gibt die Zahlungsanweisung an die Bank, die die Zahlung ausführt. Überwiesen wird das Geld auf die Auslandskonten von Strohmännern. Diese teilen es wiederum auf und verschieben es auf weitere Zwischenkonten.

Bild © Imago Images

Nicht immer kommen die Gangster mit der Beute davon. Je früher die Unternehmen den Betrug bemerken, desto besser sind die Chancen, das Geld zu retten, berichten Ermittler Schröder und Commerzbänker Wolf übereinstimmend – und raten, Polizei und Geschäftsbank zu informieren. Wenn das Geld beispielsweise nach China geflossen sei, helfe es auch, über die Handelskammern Anwälte vor Ort mit der Jagd nach der Überweisung zu beauftragen. Die mehrgleisige Strategie hat häufig Erfolg.

Oft genug bleibt der Betrug zunächst unbemerkt – was die Gangster sofort für die nächste Stufe nutzen: "Nachdem es beim ersten Mal so gut geklappt hat", lobt der vermeintliche Chef wiederum per Mail, "helfen Sie mir doch sicher auch bei der nächsten Zahlungs-Tranche." Und der Betrug geht von vorne los.

Es hilft, nicht so viel Respekt vorm Chef zu haben

Wie können Firmen sich schützen? "Pflegen Sie ein gesundes Misstrauen gegenüber E-Mail!" predigt Commerzbank-Experte Wolf bei seinen Vorträgen. "Wenn Sie eine E-Mail bekommen mit der Anweisung, etwas nicht mit Ihrem Chef zu diskutieren, tun Sie genau das Gegenteil." Und er rät, nicht den "Antworten"-Knopf der E-Mail zu drücken, sondern die Mail-Adresse des Chefs von Hand einzugeben oder aus dem Adressbuch der Firma zu wählen – so hebelt man Betrüger aus, die sich unter gefälschten Mailadressen als Chef ausgeben.

Auch gegen die Ausforschung ist Gegenwehr möglich. LKA-Experte Schröder nennt die Möglichkeit, telefonische Auskünfte grundsätzlich nur zu erteilen, nachdem man zurückgerufen hat – wobei er diese Empfehlung selbst ein wenig bedauert: "Das Schlimmste ist, dass das Vertrauen verloren geht, das man als Mensch haben muss."

Vor allem müssten sich Firmen fragen, ob Abläufe und Unternehmenskultur es Betrügern zu leicht machen – etwa, weil es kein striktes Vier-Augen-Prinzip für Zahlungen gibt, oder weil in der Firma Kommandoton herrscht. Der LKA-Experte hat Fälle beobachtet, in denen der Betrug nur deshalb funktionierte, weil die Untergebenen den gottgleichen Firmenpatriarchen nicht anzusprechen wagten. "Es kann nicht sein, dass in einem Unternehmen ein Buchhalter sitzt, über Millionenbeträge verfügt und nicht nachfragen kann." Es hilft also, keinen falschen Respekt vorm eigenen Chef zu haben.

Tipps der Polizei: Wie man sich vor "Chefbetrug" schützt

Das Bundeskriminalamt hat einen Flyer für Unternehmen zusammengestellt, der sagt, worauf Chefs und Mitarbeiter achten müssen, um nicht zum Opfer dieser Art des Trickbetrugs zu werden. Sie können ihn hier herunterladen.

Quelle: hessenschau.de