DIE WELT

Mit dieser Masche erbeuten Chinesen Millionen

Mit gefälschten E-Mails und verblüffend simplen Tricks bringen Betrüger aus China internationale Konzerne um Millionensummen. Dabei helfen ihnen leichtgläubige Mitarbeiter. So funktioniert die Masche.

Von Johnny Erling

Heiligabend 2015 klingelte beim Shanghaier Rechtsanwalt Rainer Burkardt das Handy. Der Anruf kam aus Österreich, war aber keine frohe Botschaft zum Fest. Der Finanzchef eines mittelständischen Unternehmens klagte: Internet-Schwindler hätten seine Firma am Vortag ganz unchristlich über den Tisch gezogen.

Mit imitierten E-Mails hätten sie sich gegenüber seiner Buchhalterin als Vorgesetzte ausgegeben und sie angewiesen, sehr viel Geld auf ein Konto der Shanghai Pudong Entwicklungsbank zu transferieren. Angeblich, um rasch einen noch geheimen Unternehmenskauf in China zu finanzieren. Die Mitarbeiterin folgte den Anordnungen, schöpfte dann aber am Nachmittag des 23. Dezember Verdacht.

Österreichs Polizei wurde eingeschaltet, die chinesische Bank per Überweisungssystem Swift informiert. Doch der Transfer war nicht mehr zu stoppen. Ob Burkardt etwas tun könne, fragte der Manager am Telefon aufgeregt. Es gehe um fast vier Millionen Euro.

FBI sieht vor allem US-Firmen als Opfer

"Als ich den Anruf erhielt, dachte ich 'Déjà-vu'. Diese Masche kennen wir", erinnert sich Burkardt in seiner Kanzlei im 25. Stock des Shanghai Bund Center. Der 49-jährige Wirtschaftsjurist nahm sich der Sache an. Seine Kanzlei, die er vor drei Jahren mit lokalen Partneranwälten eröffnet hatte, wusste, wer anzusprechen war.

Es folgten wenig geruhsame Weihnachtstage. Immerhin konnte das noch nicht abgehobene Geld der Österreicher wenigstens eingefroren werden. Auch die österreichische Politik intervenierte rasch hinter den Kulissen, bat die zentralchinesischen Behörden um Amtshilfe. Zwischen Wien und Peking gibt es aber kein Rechtshilfeabkommen. So bleibt es eine Hängepartie, wann und ob die Österreicher ihr Geld zurückbekommen.

Weltweit gehen Unternehmen dieser Masche auf den Leim, die das FBI "Business E-Mail Compromise" nennt, also einen Schwindel mit "kompromittierten Geschäfts-E-Mails". Die meisten Opfer seien US-Firmen. Seit Januar 2015 würden die Betrügereien mit Wachstumsraten von 270 Prozent zunehmen.

Österreichisch-chinesischer Luftfahrtzulieferer FACC betroffen

Zwischen Oktober 2013 und August 2015 zählte das FBI 7000 Fälle, in mehr als 50 Ländern wurden US-Firmen über den Tisch gezogen. Die Verluste addierten sich auf mehr als 740 Millionen Dollar, die bei Überweisungen in 72 Länder verloren gingen. "Aber die Mehrheit der Transfers gingen auf asiatische Banken in China und Hongkong."

Die Dunkelziffer ist hoch. Viele Unternehmer schweigen aus Scham und Angst vor Gespött, nur börsennotierte Firmen müssen den Betrug offenlegen, etwa der österreichisch-chinesische Luftfahrtzulieferer FACC. Im Januar gab er bekannt, durch die neue Masche um 50 Millionen Euro geprellt worden zu sein. Er entließ seine Finanzbeauftragte.

Gleiches widerfuhr dem US-Unternehmen für Netzwerktechnologie Ubiquiti, das in seinem jüngsten Finanzbericht einen Verlust von 46,7 Millionen Dollar eingestand. Im Juni 2015 hatte es den Betrug mit vorgetäuschten Identitäten entdeckt, dem seine Zweiggesellschaft in Hongkong aufsaß. Von den Geldern, die sie an auswärtige Bankinstitute transferierte, konnte sie nur 8,1 Millionen Dollar zurückerhalten und 6,8 Millionen einfrieren lassen.

600 Millionen Euro Schaden

International hat die Masche mit den immer gleichen Manipulationen von E-Mails Vorgesetzter viele Namen. "CEO-Betrug" nennt es Österreichs Bundeskriminalamt. US-Behörden verwenden die Abkürzung FPF für "Fake President Fraud", die französische Polizei warnt vor "fraude au président".

Nach einer gerade veröffentlichten BBC-Recherche wurden in den vergangenen Jahren allein in Frankreich Tausende Fälle mit "Bogus-Boss-E-Mails" bekannt, die einen Schaden von mehr als 600 Millionen Euro anrichteten und auch Konzerne wie Michelin oder Nestlé nicht verschonten. Auch der langjährige Finanzjournalist der "Washington Post", Brian Krebs, analysiert auf seiner Webseite viele konkrete Fälle.

Chinas Kriminalpolizei hat auch ihren eigenen Fachbegriff: Sie nennt die Chef-Imitationen "Huapi-Zhapian", den "Betrug mit der bemalten Haut". Das geht auf die "merkwürdigen Geschichten aus dem Liaochai-Studio" zurück, eine Art chinesischer 1001-Nacht-Märchen aus dem 17. Jahrhundert.

Unter der "bemalten Haut" steckt ein Dämon

Ein Gelehrter namens Wang fällt darin auf ein bildschönes Mädchen herein und nimmt sie bei sich auf. Sie entpuppt sich als grässlicher Dämon unter einer übergestülpten schön bemalten Haut und frisst das Herz des Gelehrten auf. Auch China veröffentlicht regelmäßig Warnungen und macht Fälle von Unternehmen publik, die auf eine "bemalte Haut" hereingefallen sind.

Anwalt Burkardt, der Vertrauensjurist des österreichischen Konsulats in Shanghai ist, hatte einen Fall von "bemalter Haut" im Oktober schon einmal durchspielen müssen. Da klingelte sein Handy nach 22 Uhr. Der Online-Betrug, den er damals auch von einem österreichischen Unternehmen geschildert bekam, verschlug ihm erst einmal die Sprache.

Er war so raffiniert eingefädelt, dass Burkardt inzwischen von einem "perfektem Netzwerk zur Täuschung" der Opfer ausgeht und von kriminellen Profis spricht. Sie brachten einen bekannten, weltweit operierenden Konzern dazu, über neun Tage lang portionsweise hohe Summen an Banken in China und Hongkong zu überweisen. Insgesamt flossen 36 Millionen Euro ins Ausland. Als dem Unternehmen Zweifel kamen, war alles Geld abgeräumt, bis auf die beiden letzten Überweisungstranchen, die bei Banken eingefroren werden konnten

Geldwäsche über Untergrundbanken

Von 15 weiteren, ähnlich betrogenen österreichischen und deutschen Firmen in Shanghai hat Burkardt inzwischen erfahren. Jetzt will er vor den Betrügern warnen. Die Banden würden die Unternehmen systematisch ausspionieren und sich über die Angaben in sozialen Medien Profile der Geschäftsführer und Finanzmitarbeiter erstellen.

Sie kopierten die E-Mail-Adressen der Vorgesetzten fast perfekt, manchmal nur um einen unauffälligen Bindestrich oder Punkt verändert. Manche Betrüger kaperten die Mailkonten sogar komplett. In Telefonaten würden sie sich als Anwälte oder Berater ausgeben und deren Stimmen imitieren. Das erbeutete Geld fließt in ein Geflecht chinesischer Konten bei seriösen Banken, vermutlich über Strohmänner registriert.

"Aufgeschlagene Gelder werden sofort sternförmig weiterverteilt. Das ist oft hervorragend gemacht", sagt Burkardt. Weder Anwälte noch Polizei wissen, wer hinter den Betrügereien steht. Die Geldwäsche läuft offenbar auch über Untergrundbanken, von denen es in China besonders viele gibt.

50 Seiten E-Mails, Anrufe mit verstellter Stimme

Im Fall des 36-Millionen-Euro-Betrugs war der erste Schritt eine angeblich vom Firmenchef an seinen Chefbuchhalter gerichtete E-Mail. Ein geheimer "strategischer Unternehmenszukauf" in China liege in der Pipeline, stand darin. Ein bekannter deutscher Anwalt werde für das Unternehmen die finanzielle Abwicklung koordinieren und den Buchhalter kontaktieren.

Das tat der vermeintliche Anwalt nicht nur per Mail, sondern auch über Telefonanrufe, außerdem gab er Anweisungen, auf welche Bankkonten das Geld in gestückelten Überweisungen gehen sollte. "Zu diesem Vorgang gibt es 50 Seiten E-Mails", sagt Burkardt. Die Betrüger dachten dabei an alle Details. Während der Anrufe des angeblichen Anwalts beim Buchhalter leuchteten auf dessen Display die echten deutschen Nummern auf. Erst eine zufällige Nachfrage brachte den Schwindel ans Licht. Doch da war es schon zu spät.

Die Betrügereien lösten bei allen, die davon hören ungläubiges Staunen und Kopfschütteln aus, sagt Burkardt. "Es ist leicht, mit dem Finger auf andere zu zeigen und zu sagen: Wie kann das sein?"

Mitarbeiter umgehen Sicherheitsprozeduren

Doch offensichtlich fühlt sich so mancher Mitarbeiter in international agierenden Unternehmen angesichts einer vom Online-Tempo geprägten Geschäftswelt unter Druck, schnell zu handeln, um mithalten zu können. So werden langwierige Sicherheitsprozeduren umgangen. Kriminelle Netzwerke nutzen diese Gelegenheit für ihren lukrativen Schwindel.

Dabei würden alle noch so raffinierten E-Mail-Betrügereien sofort scheitern, wenn Buchhalter eine primitive Sicherheitsmaßnahme beherzigen würden: Beim geringsten Zweifel einfach beim Chef telefonisch nachfragen, ob der Überweisungsauftrag auch wirklich von ihm stammt.