Die Dotcom-Räuber

Kriminalität Hackerbanden klinken sich in den Mailverkehr zwischen Firmen und Lieferanten ein und lenken Zahlungen um. Ermittler schauen machtlos zu.

Werbung für Engelbert-Strauss-Kollektion: „Keinerlei Aktivitäten der Staatsanwaltschaft“

Zu den großen Verdiensten – und Verdienstquellen – der Firma Engelbert Strauss gehört es, den deutschen Handwerker nach Jahrzehnten des unauffälligen Handwerkens endlich aus seinem Blaumann befreit zu haben. Die Softshell-Jacke „Roughtough“ zum Beispiel, angeblich der ultimative Sauwetterschutz für die ganz harten Jungs unter den Baggerfahrern, Baumfällern, Betonbauern, gibt es nun auch in den modischen Farben Thymian, Titan und Rubin. Alles zu kaufen im Internet sowie in drei – nein, bewahre, nicht Läden, sondern „Workwearstores“.

Die Marke hat es mit Dreitagebart-Models, jeder Menge Rough-Tough-Englisch und der Bandenwerbung bei Spielen der deutschen Nationalelf geschafft, sich in den Hipster-Händler unter den Arbeitskleidungsherstellern zu verwandeln. Einen dreistelligen Millionenumsatz macht das Unternehmen im Jahr, beschäftigt 1000 Mitarbeiter. Ohne den weißen Strauß auf rotem Grund geht der stilsichere Malocher heute nicht mehr zum Schweißvergießen.

Man kann sagen, dass die Firma aus dem hessischen Biebergemünd in den vergangenen Jahren nicht viel falsch gemacht hat. Aber das eine dann doch: diese Überweisung nach Jakarta im Dezember 2013. Ausgerechnet die angesagten, ausgeschlafenen Marketingprofis sind auf eine neue Cybercrime-Masche hereingefallen. Eine, die exemplarisch für den Trend steht, den Ermittler seit einiger Zeit beobachten – hin zu immer raffinierteren, aufwendigeren Attacken.

Eine Hackerbande hatte sich in den Mailverkehr zwischen Strauss und einem Lieferanten eingeklinkt, hatte sich mit Inhalt und Stil der Korrespondenz vertraut gemacht, um dann mit echt wirkenden, bestens getimten Mails knapp 200 000 Dollar auf ein eigenes Konto umzuleiten. Anders als bei den E-Mail-Massenabwürfen, bei denen die Täter hoffen, dass unter Millionen Empfängern schon 20, 30 Dumme sein werden, die an das Märchen vom Erbonkel in Nigeria glauben, zielte die Attacke nur auf ein Opfer. Dafür bastelten die Hacker Mails, die genau für diesen Betrug taugten.

Der Berliner IT-Strafrechtler Daniel Gutman spricht von der „zweiten Welle“ des Internetbetrugs; die erste, mit billig gemachten Bettelmails, oft in schlechtem Englisch, bringe immer weniger Erfolg. „Deshalb investieren die Täter zunehmend in die Qualität.“ Und der Angriff auf Strauss sei sicher einer der professionellsten gewesen.

Das Vehikel für den Betrug ist im aktuellen Katalog auf Seite 411 zu sehen: sechs Ledergürtel, passend zum Strauss-Anspruch, lifestylebewusste Schwerstarbeiter auch am Feierabend nicht nackt dastehen zu lassen. Geliefert hatte die Riemen die Firma Samo Belt aus Beirut im Libanon, 27 960 Stück für 199 455 Dollar. Die Geschäftskorrespondenz zwischen Biebergemünd und Beirut lief per Mail, bei den Libanesen, langjährigen Geschäftspartnern von Strauss, ging die Post unter der Mailadresse info@samobelt.com ein.

Im Dezember 2013 kam die Ware wie vereinbart in Deutschland an. Strauss reklamierte bei ein paar Gürteln die Länge, keine große Sache, die mit 650 Dollar Nachlass aus der Welt geschafft werden sollte. Ansonsten war alles, wie es sein sollte, und damit klar, dass Strauss nun zahlen würde.

Am Nikolaustag erhielt Strauss daraufhin erst mal eine Mail, angeblich aus Beirut, dass Samo Belt mit dem Nachlass einverstanden sei – man solle doch die 650 Dollar einfach von der Rechnung abziehen. Kein Grund also für den zuständigen Strauss-Einkäufer, argwöhnisch zu werden. Und selbst wenn das Schreiben sein Misstrauen geweckt hätte: Vermutlich hätte er auch dann kaum gemerkt, dass diese Mail nicht von „info@samobelt.com“ gekommen war, sondern von „info@samobelts.com“, mit einem s hinter „-belt“. Also drückte der Strauss-Mann wie immer auf den Antwort-Button – und schickte seine Mails damit, ohne es zu ahnen, nicht mehr an die Firma in Beirut, sondern an Hacker, die sich in den Mailverkehr hineingemogelt und die Fake-Adresse mit dem Extra-s angelegt hatten.

Zwar waren die Mails der Bande in schlechtem Englisch geschrieben, mit Schreib- und Grammatikfehlern; allerdings hatten auch die echten libanesischen Lieferanten bislang nicht mit makellosem Oxford-Englisch aufgewartet – gut möglich also, dass selbst die Fehler in den fingierten Mails nicht zufällig waren. Fest steht jedenfalls, dass sich die Täter mit dem Schreibstil in der Geschäftsbeziehung zwischen Samo Belt und Strauss gut auskannten, offenbar hatten sie schon länger mitgelesen. Und so fing am 9. Dezember eine Mail der Täter mit denselben Worten „Please check the attached file“ an, „Prüfen Sie den Anhang“, mit der auch die echte Samo Belt Tage vorher noch eine Mail eingeleitet hatte.

Mit dieser neuen Mail ließen die Betrüger die Strauss-Leute nun wissen, dass Samo Belt kurzfristig die Kontoverbindung geändert habe – angeblich, weil die Überweisungskosten bei der alten Bank zu hoch gewesen seien, außerdem aus ein paar anderen Gründen, über die sich der Versender der Mail nicht ganz klar ausließ. Das Geld – selbstverständlich abzüglich 650 Dollar „Compensation“ – solle deshalb nun an die United Overseas Bank in Jakarta, Indonesien, gehen; jede weitere Zahlung auf das frühere Konto könne leider nicht verbucht werden.

Um ihre Glaubwürdigkeit zu untermauern, schickten die Täter eine Rechnung über die gelieferten Gürtel mit; sie enthielt die Namen der Modelle, die Stückpreise. Offenbar hatten sich die Gauner die Zahlen und Angaben von einem Rechner besorgt. Für Strauss wirkte das alles plausibel. Nachdem die Hintermänner von „Samo Belts“ auch noch geschrieben hatten, sie brauchten das Geld jetzt wirklich dringend, man sei gerade knapp bei Kasse, überwies Strauss Mitte Dezember.

Erst als der echte Lieferant nachfragte, wann denn mal das Geld ankomme, die Ware sei doch längst geliefert, merkten die Hessen, dass sie Betrügern aufgesessen waren. Der Versuch, die Überweisung nach Asien rückgängig zu machen, lief ins Leere; das Geld war weg.

Dass Computerkriminalität weiter zunimmt, steht schon im Lagebild des Bundeskriminalamts für 2013. Der Fall Strauss bestätigt nun auch den Trend, dass die Täter professioneller vorgehen. „Die Angriffe erfolgen zunehmend zielgerichtet und sind technologisch immer ausgereifter und komplexer“, heißt es dazu in einem Gesetzentwurf der Bundesregierung für ein IT-Sicherheitsgesetz, das Anfang 2015 beschlossen werden soll.

Auch ein Kaufmann aus dem Rheinland fiel auf diese Masche herein. Er hatte 8000 Euro verloren, weil er das Geld auf ein neues Konto überwiesen hatte, das ihm scheinbar sein chinesischer Geschäftspartner genannt hatte – in Wahrheit hatte eine Hackergruppe die Zahlung auf ihr Konto umgelenkt.

Der Trick, bei Experten als „Bankmandatsbetrug“ bekannt, erfordert beides: Vorarbeit und Vorsicht. Und selbst wenn die Täter sich Mühe geben, steigt mit jeder verschickten Mail das Risiko aufzufliegen. Sind sie erfolgreich, winkt am Ende der große Preis, und den vermuten sie vornehmlich bei Unternehmen. „Firmen anzugreifen kommt immer mehr in Mode, weil dort meist mehr zu holen ist als bei Privatleuten“, sagt Florian Oelmaier von der Beratungsfirma Corporate Trust.

Dabei gilt grundsätzlich, dass „jede Firma gehackt werden kann, es ist nur eine Frage des Aufwands“, wie Jan Wolter sagt, Geschäftsführer des ASW-Bundesverbands Allianz für Sicherheit in der Wirtschaft. Das ist zwar im Grunde keine Neuigkeit; früher aber kam das große Instrumentenbesteck meist nur dann zum Einsatz, wenn es um eine besonders wertvolle Beute ging, um Firmengeheimnisse. Heute nutzen es Betrüger dagegen auch schon für den schnöden Geldklau.

Die Täter sitzen oft in Asien oder in Russland. Gerade Russland hat ein Heer gut ausgebildeter, aber schlecht bezahlter IT-Spezialisten, die sich leicht von der organisierten Kriminalität ködern lassen. Sie kennen sich mit dem Hacken aus und wissen, wie man solche Attacken verschleiert. So laufen 75 Prozent aller Angriffe auf Servern, die nur für einen Tag im Internet stehen, klagt ASW-Mann Wolter.

Kein Wunder also, dass die Fahnder sich schwertun, die Täter zu erwischen. Vorausgesetzt, dass die Ermittler überhaupt etwas von den Fällen erfahren, denn eine Untersuchung des Landeskriminalamts Niedersachsen zeigt, dass nur neun Prozent aller Cybercrime-Angriffe angezeigt werden. Zu groß ist die Angst von Firmen, sie könnten auf dem Markt als unzuverlässig gelten, infiziert, schlecht geschützt. Und damit nicht mehr als vertrauenswürdig. Häufig sind sie der Auffassung, eine Anzeige bringe ohnehin nichts. Fakt ist: Computerbetrügereien erfordern in der Regel Ermittlungen im Ausland, und das kann dauern – nicht nur wegen der nötigen Rechtshilfeersuchen. „Die Spuren verlaufen oft im Sand“, gibt ein Cybercrime-Experte zu, egal ob man der Spur der Computerserver oder der Spur des Geldes folge.

Das war auch im Fall Engelbert Strauss so. Als die Firma den Betrug bemerkte, erstattete sie Strafanzeige bei der Staatsanwaltschaft Hanau. Detailliert beschrieb der Anwalt der Firma, wie die Täter vorgegangen waren und dass sie, kurz bevor das Geld von Strauss auf dem Konto in Indonesien landete, auch noch ein Konto in Großbritannien angegeben hatten. Das schien ein Ermittlungsansatz zu sein, Rechtshilfeersuchen an die Briten sind Tagesgeschäft. Aber „wir konnten keinerlei Aktivitäten der Staatsanwaltschaft feststellen“, sagt Engelbert-Strauss-Einkaufschef Christoph Piecha enttäuscht.

Was zu tun war, klärten die Strafverfolger in nur 20 Tagen: nämlich nichts. Sie teilten mit, dass „weitere Nachforschungen zurzeit keinen Erfolg versprechen“. „Zurzeit keinen“ – das kann man in solchen Fällen auch anders sagen: nie.

Jürgen Dahlkamp, Jörg Schmitt