Schmutziger Handel

Betrüger erbeuten Millionen mit ergaunerten Klimaschutz-Zertifikaten der Industrie

Von Markus Balser und Michael Bauchmüller

Berlin/München – Der Angriff war bis ins Detail geplant. Eine eigene Internet-Seite hatten die Betrüger eingerichtet, Titel: „Tradingprotection.com". Darin lobt sich die Firma als „vertrauenswürdiger Anbieter" einer sicheren Plattform. „Millionenfach jeden Tag vertrauen uns Firmen und Kunden", heißt es weiter, schließlich gehe es um „Handel mit Vertrauen". Und wer dann immer noch zweifelte, der fand eine Pressemitteilung, datiert auf den 14. Januar. Da habe Trading Protection den Zuschlag erhalten, das Europäische Emissionshandelssystem abzusichern, gaukelt die Internetbande vor. Wohlweislich nur bis zum Abend des vorigen Donnerstags. Danach erlischt die Seite. Die Firma hatte es ohnehin nie gegeben.

Denn sie ist Teil einer Falle. Schon am Morgen des vorigen Donnerstags nämlich finden Mitarbeiter vieler deutscher Unternehmen eine gefälschte E-Mail im Postfach. Angeblicher Absender: Die staatliche Emissionshandelsstelle in Berlin. Betreff: „Emissionshandelssystem (EU ETS) – Neue Sicherheits-Maßnahme". In allen Ländern des EU-Emissionshandels sei es zu Angriffen auf das System gekommen, warnen die Absender darin in vertraulichem Ton. Deshalb müsse die Sicherheit der Mitgliederseiten erhöht werden. Freundlich, aber bestimmt forderten sie ihre Adressaten auf, die Zugangsdaten auf der Internetseite eines „hochrangigen Sicherheitsunternehmens" doch noch mal einzugeben – bei Tradingprotection.com.

Das Schreiben enthielt so viele technische Details, dass niemand misstrauisch wurde, heißt es in einem Unternehmen, das nicht genannt werden will. „Wir erhöhen den Grad der Sicherheit", verspricht „Sicherheitsmanager" Hans Frederick den Empfängern. Man integriere schließlich neue Standards, „denen Sie folgen müssen, um weiterhin den Service in Anspruch zu nehmen".

Wer mitmachte, wusste wenig später: Die Warnung war mehr als berechtigt. Allerdings diente die E-Mail nicht der Bekämpfung, sondern allein der Ermöglichung des Betrugs. Denn die Betrüger von „Trading Protection" sahnten auf diese Weise den Zugang zu den Emissionskonten ab – ganz nach der Methode jener Bankbetrüger, die sich auf Umwegen Zugang zu Privatkonten verschaffen. Experten nennen das *Phishing*.

„Leider sind solche Praktiken im Internet üblich", sagt Hans-Jürgen Nantke, Chef der Deutschen Emissionshandelsstelle DEHSt. Fast der komplette Handel mit Emissionsrechten läuft online, und zwar europaweit. So gesehen war die Ausbeute der Betrüger bescheiden: Nur sieben von 2000 deutschen Emissionsrechtehändlern fielen auf die Attacke herein. Ihr Schaden ist allerdings enorm.

Die Emissionszertifikate, die Firmen jeweils zum Ausstoß von einer Tonne Kohlendioxid berechtigen, gleichen Aktien. Sie werden gehandelt etwa an der Leipziger Energiebörse EEX und wechseln im virtuellen Raum in Sekunden den Besitzer – indem sie von Konto zu Konto übertragen werden. Broker unterhalten solche Konten, aber auch Betreiber großer Industrieanlagen, die diese Rechte stets vorhalten müssen. Insgesamt 250 000 solcher Zertifikate raubten die Betrüger mit ihrer vorgetäuschten Warnmail. Preis pro Zertifikat am vergangenen Donnerstag: 12,98 Euro an der EEX. Macht insgesamt 3,2 Millionen Euro.

Für die sieben Geschädigten gibt es kaum Hoffnung, ihr Geld je wiederzusehen. Zwar lässt sich jedes einzelne Zertifikat nachverfolgen, denn die virtuellen Papiere tragen Nummern. Doch seit Donnerstag wanderten sie durch viele Hände – und die neuen Besitzer konnten nicht ahnen, dass sie gestohlen sind. Zwar erstatteten sowohl die Firmen als auch die DEHSt Anzeige gegen unbekannt. Doch die Hintermänner sind kaum zu identifizieren. Nach *SZ*-Informationen wurden die Zertifikate zunächst auf ein dänisches Konto transferiert, gingen von dort aber gleich weiter, gestückelt in kleine Pakete und quer durch Europa.

Online-Attacken habe es auch beim Emissionshandel schon früher gegeben, sagt Nantke, „aber nie in dieser Dimension". Eine Zeitlang galt der internationale Emissionshandel überdies auch als Chance, zu unrechtmäßigen Umsatzsteuerrückvergütungen zu gelangen. Doch entsprechende Schlupflöcher sind inzwischen geschlossen. „Da sind womöglich nun Leute auf neue kriminelle Methoden

Für die Geschädigten gibt es kaum Hoffnung, ihr Geld je wiederzusehen.

umgestiegen", mutmaßt Jürgen Hacker, Geschäftsführer des Emissionshändler-Verbands BVEK.

Bei den Unternehmen allerdings wird auch Kritik an der DEHSt laut. Diese sei zu spät aktiv geworden, heißt es. Denn während die österreichische Emissionshandelsstelle noch am Vormittag der Attacke vor der Mail des Herrn Frederick warnte, fielen den Betrügern in Deutschland Unternehmen noch arglos zum Opfer. Die Handelsstelle selbst weist Vorwürfe zurück. Auch sie habe noch am Tag der Attacke gewarnt, heißt es in einer Stellungnahme. Allerdings stand der Verdacht da schon lange im Raum. Österreich hatte schon Mitte Januar generell auf die Gefahr betrügerischer Phishing-Attacken hingewiesen.

Vorerst sind die Konten in Deutschland eingefroren, erst von diesem Donnerstag an sollen Transaktionen wieder möglich sein. Allerdings nur mit ganz neuen Passwörtern – und der Bitte um Diskretion und Sorgfalt. „Das funktioniert sowieso nur einmal", glaubt BVEK-Chef Hacker. „Jetzt sind alle gewarnt." Und die Leute von Tradingprotection sind auf und davon, reicher als mancher ordinäre Bankräuber.

Einen kleinen Spaß auf ihrer Website konnten sie sich aber vorher nicht verkneifen. In der Rubrik „über uns" heißt es zur erfundenen Firma: „Wir haben Erfolg dank eines Teams aus Sicherheits-Experten und Hackern. Wir entwerfen nicht nur völlig neue Systeme, sondern greifen sie auch an, indem wir die weltweite Hackerszene auf sie ansetzen." Die Opfer werden nicht widersprechen: „Technisch sind wir kaum zu schlagen."

Wer Emissionen ausstößt, wie das Braunkohlekraftwerk Lippendorf bei Leipzig, braucht dafür Zertifikate. Der Handel mit den teils wertvollen Papieren wurde nun zum Opfer von Internetbetrügern. Foto: AP