Gefährliches Schnäppchen-Fieber

Amazon bekommt eine Abzock-Masche nicht in den Griff

Betrüger überschwemmen den Amazon-Marktplatz mit Fake-Angeboten, locken Nutzer von der Plattform weg und zocken sie ab. Sie haben leichtes Spiel, weil Amazon seine Kunden nicht ausreichend warnt und Händler kaum prüft.

Von Christian Wölbert

Der langjährige c't-Leser Peter M. bestellt normalerweise alle Elektrogeräte für seine Familie selbst. Im Oktober bat er ausnahmsweise seine Lebensgefährtin Anna W., eine Waschmaschine zu kaufen. Diese entdeckte auf Amazon.de ein gutes Angebot: ein LG-Modell der Energieklasse A+++ für nur 280 Euro.

Seltsam war, dass der Verkäufer darum bat, ihn vor der Bestellung per Mail zu kontaktieren. Die im Online-Shopping wenig erfahrene Anna W. ließ sich davon jedoch nicht irritieren. Sie erkundigte sich nach der Maschine und erhielt daraufhin eine angebliche Amazon-Bestellbestätigung mit einer IBAN mit den Anfangsbuchstaben „RO“. Auch das machte sie nicht stutzig – sie überwies die 280 Euro. „Die Kohle wanderte auf Nimmerwiedersehen nach Rumänien“, musste Peter M. danach entsetzt feststellen.

Abzocke läuft seit vier Jahren

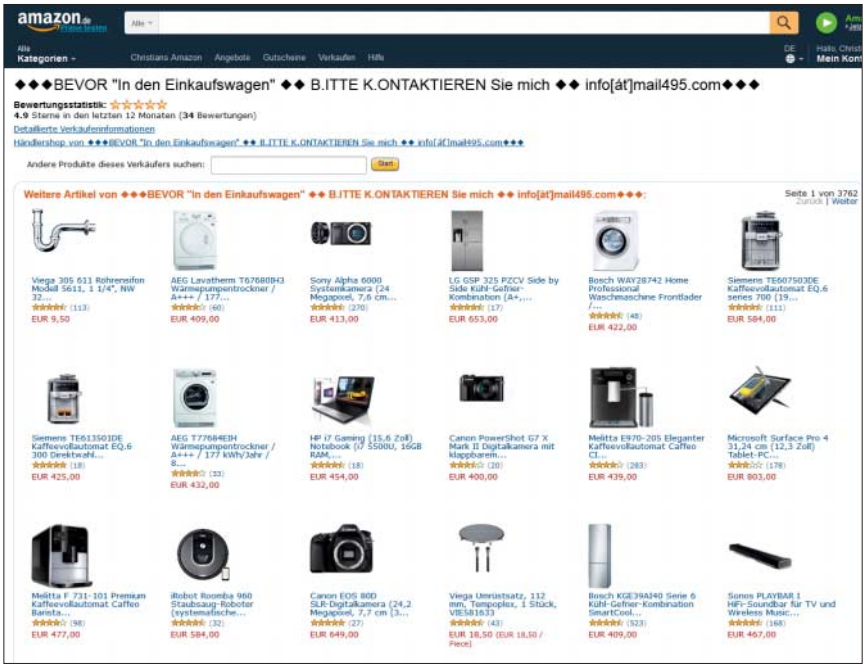
Wer oft online einkauft, würde vermutlich nicht auf diesen Trick hereinfallen. Doch Anna W. ist bei Weitem nicht das einzige Opfer. Die Amazon-Masche funktioniert so gut, dass eine oder mehrere Banden sie seit ungefähr vier Jahren mit hohem Aufwand durchziehen. Sie kapern wie am Fließband Konten von Amazon-Verkäufern und stellen in deren Namen Zehntausende Fake-Angebote online oder eröffnen eigene Konten. Dann überreden sie Kaufinteressenten einzeln per Mail, das Geld zu überweisen. Außerdem rekrutieren sie Privatleute, die ihre Bankkonten zur Verfügung stellen und das empfangene Geld weiterleiten. Man findet kaum noch ein hochpreisiges Produkt auf Amazon.de, das nicht von den Betrügern zum Schein angeboten wird: Laptops von Apple, Boxen von Sonos, Kaffee-Vollautomaten von Siemens.

Mit welchen Tricks die Betrüger die Konten von Verkäufern kapern, musste im Oktober ein PC-Händler aus Nordrhein-Westfalen leidvoll erfahren. Unter der Bedingung, anonym zu bleiben, berichtet er: An einem Sonntagnachmittag erhielt er eine gut gemachte Phishing-Mail mit einem Link, angeblich zu seiner Monatsabrechnung auf Amazons Seller-Central-Portal. Die Webseite sah so echt aus, dass er seine Zugangsdaten eintippte.

60.000 Produkte hochgeladen

Eine Stunde später erhielt er eine – nicht gefälschte – Mail von Amazon: er sei erfolgreich zum „Verkaufstarif Power-Anbieter“ gewechselt. Der Versuch, sich bei Amazon einzuloggen, scheiterte, denn die Betrüger hatten sein Passwort geändert. Er setzte es zurück und loggte sich ein, konnte aber nichts mehr ausrichten. Die Angreifer hatten per Datei-Upload schon über 60.000 Produkte inseriert.

Panisch versuchte er, die Angebote zu löschen, doch er konnte nicht mehr als 250 in einem Rutsch entfernen, und die



Über 66.000 Fake-Angebote wurden in diesen gekaperten Händler-Account eingestellt.

Betrüger legten ständig nach. Er rief bei einer Amazon-Hotline an, wurde jedoch abgewimmelt. Also informierte er den Händler-Support per Mail. Am nächsten Tag sperrte das Unternehmen sein Konto.

Nach einer solchen Konten-Übernahme geben die Betrüger stets im Feld für den Artikelzustand oder für den Verkäufernamen eine Mail-Adresse an. Wer im Schnäppchen-Fieber schreibt, wird nach einer Lieferanschrift gefragt. Dann folgt eine gefälschte Amazon-Bestellbestätigung mit „Zahlungsanweisungen“ und einer Bankverbindung, meist in einem osteuropäischen Land oder in Italien.

Legt ein Interessent hingegen das Produkt auf Amazon.de in den Einkaufswagen und bestellt es, erscheint oft die Meldung, dass es nicht mehr verfügbar sei. Falls die Bestellung durchgeht, wird sie in der Regel nie als „versendet“ markiert, und Amazon zieht kein Geld vom Kunden ein.

Nutzer werden nicht gewarnt

Georg Tryba von der Verbraucherzentrale NRW beobachtet die „massiven Dauerattacken“ seit Anfang 2013. Er verlangt von Amazon, Nutzer an prominenter Stelle zu warnen – zum Beispiel wie Banken auf ihren Login-Seiten. Doch seine Anfragen dazu „wollte Amazon partout nicht beantworten“, sagt Tryba.

Auch beim Landeskriminalamt Baden-Württemberg ist die Methode „natürlich bekannt“, sagt Sprecher Ulrich Heffner. Täter habe man nie ermittelt, weil die Spur immer ins Ausland führte. Auch die Zahl der Fälle ist unbekannt, weil die Polizei in ihrer Statistik zu „Warenbetrug mit Tatmittel Internet“ nicht nach Plattformen wie Amazon oder Ebay unterscheidet.

Amazon erklärte gegenüber c’t, dass „eine sichere Einkaufsumgebung oberste Priorität“ habe. Man lösche unverzüglich unzulässige Angebote, von denen man erfahre. Unsere Rückfragen zu konkreten Schutzmaßnahmen ignorierte Amazon.

Sowohl das Betrugsopfer Peter M. als auch der Händler, dessen Konto gehackt wurde, machen dem Unternehmen Vorwürfe. „Amazon nimmt billigend in Kauf, dass Kunden geprellt werden“, meint Peter M. Der Händler ärgert sich darüber, dass Amazon zwar Kunden-Hotlines anbietet, er aber als Händler niemanden persönlich erreichen konnte, als er schnell Hilfe brauchte. *(cwo@ct.de)* c't

Christian Wölbert, c’t-Redakteur

Typisch Amazon

Amazon wird niemals alle Verkäufer so durchleuchten können, dass kein einziges schwarzes Schaf übrig bleibt. Und man muss auch nicht verlangen, dass Amazon den Schaden erstattet, wenn Nutzer auf gefälschte Mails hereinfallen und abseits der Plattform Geld nach Rumänien überweisen.

Doch der Konzern macht es Abzockern viel zu leicht, Opfer anzulocken. Mit ein paar Klicks können sie Power-Seller-Konten eröffnen und per Datei-Upload Zehntausende Fake-Angebote auf einen Schlag einstellen. Ein simpler ID-Check wie beim Eröffnen eines Bankkontos würde dem einen Riegel vorschieben. Das wäre nicht einmal für alle Händler nötig, denn mit Hobby-Accounts ohne Upload-Funktion kann niemand viel Schaden anrichten.

Konten bestehender Verkäufer könnte Amazon mit simplen Maßnahmen besser schützen. Zum Beispiel durch zwingende Zwei-Faktor-Authentifizierung oder bessere Checks bei Logins mit neuen Rechnern aus dem Ausland.

Doch zu befürchten ist, dass Amazon sich jegliche Präventivmaßnahme, die minimalen Aufwand bedeutet, einfach spart. Egal ob es um gefälschte Markenware, um lebensgefährliche Elektrogeräte oder um Abzocke geht – Amazon reagiert immer erst dann, wenn der Kunde längst reingefallen ist.