Onlinehandel: Auch Verkäufer können Opfer von Betrügern werden, die bestellte Waren nicht bezahlen.

Gefahren beim Onlineshopping

Die Zahl der Fälle von Internetbetrug stieg 2019 an – vor allem Fälle von Bestell- und Warenbetrug. Onlinehändler und Kunden müssen wachsam sein, um nicht Opfer eines Betrugs zu werden.

Aufgrund der Technisierung und fortschreitenden Digitalisierung sowie Vernetzung des Lebens, wird der Alltag oft nicht nur vereinfacht, sondern bietet Kriminellen neue Wege, um sich illegal an den Vermögenswerten anderer zu bereichern. 2019 wurden 28.439 Cybercrime-Delikte zur Anzeige gebracht, ein Plus von 45 Prozent im Vergleich zum Jahr davor (2018: 19.627). Mehr als die Hälfte der Zahl der Anzeigen (59,2 Prozent) entfielen 2019 auf den Internetbetrug – über 3.500 Anzeigen mehr als 2018 (13.328). Laut einer 2018 veröffentlichten Studie des *Centers for Strategic and International Studies (CSIS)* werden 1,5 Millionen Menschen täglich Opfer von Cybercrime. Der jährliche, weltweite Schaden wurde dabei auf 450 bis 600 Milliarden US-Dollar geschätzt.

Boom bei Onlineshopping. Die Welle der Digitalisierung hat die meisten Branchen schon lange erreicht und viele, die noch keinen Onlineshop hatten, mussten ihr Konzept aufgrund von Corona ändern oder erweitern, um die hohen Verluste aus dem stationären Handel abzuschwächen. „Aufgrund von Corona eröffneten viele Händler einen Onlineshop, ohne sich jedoch vorab über die Gefahren und Schutzmaßnahmen Gedanken zu machen“, gibt Mag. (FH) Claus-Peter Kahn, Büroleiter im Bundeskriminalamt für die Bekämpfung von Betrug, Fälschung und Wirtschaftskriminalität, zu bedenken. Bereits vor dem Lockdown war der Onlinehandel eine immer beliebter werdende Alternative, da die Auswahl groß ist, es nur wenige Klicks bis zum Kauf braucht und der Artikel zumeist innerhalb weniger Tage geliefert wird. Doch das Bedürfnis, den möglichst kleinsten Preis für einen hochwertigen Artikel zu zahlen und es schnell geliefert zu bekommen, haben Kriminelle schnell erkannt und für sich genutzt. Die steigenden Fallzahlen im Bereich des Internetbetrugs belegen diesen Trend. Deshalb ist es sowohl für den Käufer als auch für den Verkäufer wichtig, Sicherheitsvorkehrungen zu treffen, um keinem Betrug aufzusitzen. Betrügerinnen und Betrüger konzentrieren sich auf Händler und Kunden gleichermaßen. Doch beim Betrug im Distanzgeschäft gilt es zwischen Bestellbetrug und Warenbetrug zu unterscheiden.

Um Bestellbetrug handelt es sich dann, wenn die Käuferin oder der Käufer das Opfer des Betrugs ist. Im guten Glauben werden von einem legitim aussehenden Webshop oder Marktplatz Waren beziehungsweise Dienstleistungen gekauft, die per Vorauskasse bezahlt werden. Wenn nach einiger Zeit die Lieferung der Waren jedoch ausbleibt und die Verkäuferin oder der Verkäufer trotz Kontaktversuchen nicht reagiert, muss davon ausgegan-

Foto: Adobe.Stock/Gorodenkoff Productions OU

gen werden, dass es sich um einen Bestellbetrug handelt. Der zunächst legitime Webshop entpuppt sich als Fake-Shop, der Verkäufer bei Marktplätzen als Fake-Händler. Das Opfer erhält keine Waren oder Dienstleistungen, für die es aber bereits bezahlt hat. Die Spur des überwiesenen Geldes wird durch Finanzagenten („Money-Mules“) verschleiert, um das Auffinden der Täter zu erschweren.

Prävention. Beim Bestellbetrug gilt es, vorsichtig bei Überweisungen von großen Geldbeträgen ins Ausland zu sein, vor allem wenn sie per Vorauskasse erfolgen. Bevor die Bestellung aufgegeben wird, sollte eine Onlinerecherche über den Webshop erfolgen, um sicherzugehen, dass der Händler echt ist. Zudem sollte der Shop sichere Bezahlsysteme, wie Kreditkarte oder *Klarna* anbieten. Falls nur Vorauskasse angeboten wird, sollte der Händler genau geprüft werden. Zahlungsdaten dürfen auch niemals per E-Mail versendet werden, da das Risiko eines Missbrauchs hoch ist. Ebenso wichtig ist die Absicherung des Onlinekontos. Dafür sollte ein gutes Passwort mit Zahlen, Groß- und Kleinbuchstaben sowie Sonderzeichen genutzt werden.

„Nutzen Sie sichere Passwörter und ändern Sie diese auch regelmäßig. Das soll sicherstellen, dass Täter nicht Ihren Einkaufs-Account übernehmen und auf Ihren Namen und mit Ihren Zahlungsdaten einkaufen“, sagt Claus Kahn. Der Webshop sollte auch das Zertifikat „https://“ aufweisen, denn das stellt ein wichtiges Indiz für einen sicheren Onlinehandel dar.

Warenbetrug. Beim Warenbetrug ist das Opfer der Onlinehändler. Betrügerinnen und Betrüger bestellen Waren von einem Webshop mittels Kaufs auf Rechnung oder dem Missbrauch von echten unbaren Zahlungsdaten. Die Waren werden geliefert, der Händler erhält jedoch kein Geld für seinen Verkauf. Die Täter versuchen, durch Paketagenten die umgerouteten Pakete abzuholen und weiterzuschicken, oder durch Identitätsmissbrauch ihre Identität zu verschleiern.

Präventive Maßnahmen. Die Betreiberinnen oder Betreiber von Webshops müssen nicht nur ihren Web-Auftritt bedenken, sondern auch die Sicherheit des Webshops, die Prüfung der Kundin oder des Kunden auf Identität und Bonität, die angebotenen Zahlungsmethoden und die Logistik. Diese Kategorien können als Stellschrauben verstanden werden, über die der Onlinehändler Sicherheit für seinen Shop beziehungsweise seine Ware erhält.

Claus-Peter Kahn: „Als Onlinehändler sollte man die Prozesse und Stellschrauben zur Erhöhung der eigenen Sicherheit kennen und anwenden.“

Wie sich in den letzten Jahren zeigt, steigen die Zahlen der betroffenen Klein- und mittleren Unternehmen stark an. Umso wichtiger ist es, seinen Webshop genauso abzusichern, wie den lokalen Shop. „In der analogen Welt hat der Handel verstanden, wie wichtig es ist, das eigene Geschäft zuzusperren und mit einer Alarmanlage oder einem Rollbalken abzusichern. Vielmehr gilt es nun für die Onlinehändler oder die neu gegründete digitale Filiale zu erkennen, welche Gefahren auf Sie lauern“, erklärt Kahn. Da der Verkäufer nicht weiß und nicht sicher sein kann, ob die Käuferin oder der Käufer wirklich existiert, sollte eine Strategie entwickelt werden, die sowohl Existenz als auch Liquidität prüft, wodurch ein finanzieller Schaden abgewendet werden kann. Diese Dienste werden von Firmen gegen eine geringe Gebühr angeboten und empfiehlt sich für jeden Onlinehändler.

Auch die Zahlungsmodalitäten stellen einen wichtigen Faktor für Käufer und Verkäufer dar. Der Kauf auf Rechnung ist in Österreich nach wie vor die beliebteste Zahlungsmethode, bildet für den Onlinehändler jedoch ein hohes Risiko, da die Bezahlung der Ware ausbleiben kann. Je mehr Zahlungsarten angeboten werden, desto sicherer ist es für beide Seiten.

Der Logistikpartner ist ein wichtiges Zahnrad im gesamten Bestellprozess. Heutzutage ist es für die Kundin oder den Kunden ausschlaggebend, die Bestellung möglichst schnell – am besten schon am nächsten Tag – zu erhalten. Kleinere Unternehmen, die kein eigenes Logistikzentrum besitzen, müssen, um konkurrenzfähig zu bleiben, die Ware nach Eingang der Bestellung relativ schnell versenden. Das bedeutet, dass, wenn der Verkäufer die Bestellung bereits dem Logistikpartner übergeben hat, sich dann das hinterlegte unbare Zahlungsmittel aber als gefälscht oder gestohlen herausstellt, der Logistiker gefragt ist.

„Die letzte Meile“ wird von guten Logistikpartnern angeboten und beinhaltet das Stoppen der Auslieferung des Pakets bis vor die Tür der Kundin oder des Kunden, wenn die Zahlung fehlgeschlagen ist. „Ganz entscheidend für den Onlinehandel ist, die Prozesse und Stellschrauben zur Erhöhung der eigenen Sicherheit zu kennen und diese auch anzuwenden. Wichtig ist, dass dies kein einmaliges Unterfangen ist, sondern laufend angepasst werden muss“, sagt Kahn. Zu diesem Zweck wurden im Herbst 2019 österreichweite Roadshows veranstaltet, in denen die Unternehmerinnen und Unternehmer direkt angesprochen und geschult wurden.

Im Herbst 2020 startete die von Europol initiierte „E-Commerce Action Week“ ebenfalls für Unternehmerinnen und Unternehmer. Im Zuge dieser „Action Week“ finden zwei große Präventionskampagnen statt, die gemeinsam mit dem Bundeskriminalamt, der Polizei und Europol sowie in einer zweiten Kampagne gemeinsam mit dem Handelsverband unter der *Gemeinsam. Sicher-Initiative* realisiert werden. Das Ziel dieser Präventionskampagnen ist, den Händlern zu zeigen, wie sie ihr Online-Geschäft richtig planen und durch Schutzmaßnahmen absichern können.

Kontakt: Sollten Sie Opfer eines Betrugs sein, bringen Sie dies unbedingt bei der nächstgelegenen Polizeidienststelle zur Anzeige. Weitere Informationen erhalten Sie unter *https://bundeskriminalamt.at/202/Betrug_verhindern/start.aspx*. *Romana Tofan*

FOTO: GERD PACHAUER