



Podiumsdiskussion „Gemeinsam sicher im Handel“: Philipp Ast (Blue Tomato), Gerald S. Eder (CRIF), Thomas von der Gathen (PSA), Patricia Grubmiller (Handelsverband), Bernhard Schafrath (Bundeskriminalamt), Heinz Schiller (Österreichische Post), Moderatorin Gabriele Jiresch.

Onlinehandel im Visier

Die Ergebnisse der Sicherheitsstudie 2021 des Innenministeriums und des Handelsverbands bestätigen: Fast zwei Drittel der Onlinehändlerinnen und -händler waren bereits Opfer von Onlinebetrug.

Die Zahl der Cybercrime-Delikte nimmt Jahr für Jahr zu: 2021 wurden 46.179 Straftaten angezeigt, davon entfielen 22.440 Anzeigen auf den Internetbetrug. Die Digitalisierung öffnet den Menschen zwar viele Türen, birgt aber auch Gefahren. Bedingt durch die Covid-19-Pandemie und die Maßnahmen zur Eindämmung des Virus erlebte der Onlinehandel 2021 einen Aufschwung: Während der stationäre Handel um 3,4 Prozent zurückging, nahm der Onlinehandel um 17 Prozent zu.

Aus der Sicherheitsstudie 2021, die in Zusammenarbeit mit dem Bundesministerium für Inneres (BMI) und dem Handelsverband im Rahmen der Initiative „Gemeinsam.Sicher im Onlinehandel“ erstellt wurde, geht eines deutlich hervor: Mit steigendem Umsatz wächst auch das Risiko für Betrug.

Beim Sicherheitsgipfel 2022 am 24. Mai im Bundeskriminalamt in Wien wurden nicht nur die Ergebnisse der Sicherheitsstudie erörtert, sondern mit Branchenvertreterinnen und -vertretern auch die Wichtigkeit von Cybercrime-Präventionsmaßnahmen besprochen.

62 Prozent der Handelsbetriebe Opfer von Onlinebetrug. Um den Absatz zu steigern und Umsatzeinbußen gering

zu halten, erfuhr der Onlinehandel während der Covid-Krise einen noch stärkeren Aufschwung. Das Wachstum an neuen Webshops und die damit verbundenen Onlinebestellungen nutzten Cyber-Kriminelle, um mit bekannten, aber auch neuen, angepassten Betrugsmasken Geld zu lukrieren. Um sich einen Überblick über Onlinebetrugsfälle in Österreich zu verschaffen, führte der Handelsverband bis 9. November 2021 eine acht Wochen lang dauernde Umfrage unter 143 Webshop-Betreiberinnen und -Betreibern durch.

Das Ergebnis zeigt konkreten Handlungsbedarf: 62 Prozent aller österreichischen Händlerinnen und Händlern wurden 2021 Opfer von Onlinebetrug (2020: 46 Prozent). Bei größeren Unternehmen waren sogar 78 Prozent betroffen. Trotzdem sehen sich kleinere Betriebe nicht in Gefahr: Rund ein Fünftel der Befragten gab an, sich mit Betrugsprävention noch nicht beschäftigt zu haben.

„Keine Onlinehändlerin bzw. Onlinehändler ist vor Betrug gefeit und sollte entsprechende Schutzmaßnahmen ergreifen, denn so wie man sein Geschäftslokal mit Schlössern oder einer Alarmanlage absichert, sollte man auch seinen Onlineshop schützen“, erklärte

der stellvertretende Direktor des Bundeskriminalamtes und Leiter der Initiative „Gemeinsam.Sicher“ Mag. Manuel Scherscher beim Sicherheitsgipfel 2022 im Bundeskriminalamt.

Falsche Namen und Adressen. Onlinehändlerinnen und -händler sehen sich mit verschiedenen Arten von Betrug konfrontiert. Es wird zwischen Identitätsbetrug, Zahlungsunfähigkeit, Zahlungsmittelbetrug, Bestellbetrug, Betrug im Zusammenhang mit der Lieferung bzw. Retouren sowie Cyber-Attacken unterschieden. Die Umfrage zeigt, dass häufig falsche Namen oder Adressdaten angegeben werden (55 Prozent). Bei der Hälfte der Fälle ist der Bestellerin oder dem Besteller schon beim Bestellvorgang klar, dass sie oder er die Rechnung nicht begleichen wird können. Am häufigsten wird jedoch abgestritten, dass die Ware durch die Kundschaft erhalten wurde (63 Prozent). Hinsichtlich des Betrugs bei Lieferungen bzw. Retouren gibt es jedoch Unterschiede zwischen Unternehmen mit weniger bzw. mit mehr als zehn Beschäftigten: Während 25 Prozent der kleineren Händlerinnen und Händler Erfahrungen mit Betrugsfällen bei Retouren machen mussten, sind es bei größeren Unternehmen 64 Prozent.

Immer höherer Gesamtschaden. Im Vergleich mit 2019 zeigen die Ergebnisse der Befragung einen deutlichen Anstieg der Schadenssummen. Lag 2019 die Gesamtschadenssumme in 55 Prozent der Fälle unter 500 Euro, waren es 2020 nur noch 21 Prozent. In 30 Prozent der Fälle verloren die Händlerinnen und Händler 2020 zwischen 5.000 und 10.000 Euro.

Der Anteil der Fälle mit einem Schaden zwischen 100.000 und einer Million Euro ist von zwei auf 13 Prozent angestiegen. Die Studie zeigt außerdem, dass größere Unternehmen durch Onlinebetrug deutlich höhere wirtschaftliche Einbußen zu verzeichnen hatten. In mehr als einem Drittel der Fälle (36 %) lag die Schadenssumme bei Unternehmen mit mehr als zehn Beschäftigten zwischen 5.000 und 10.000 Euro.

Methoden zur Betrugsprävention.

Um das Betrugsrisiko zu minimieren, kombinieren Onlinehändlerinnen und -händler verschiedene Schutzmaßnahmen und verzichten dafür auch auf einen höheren Umsatz. So setzten 55 Prozent der Befragten auf sichere Zahlungsoptionen, wie etwa kein Kauf auf Rechnung. Am zweithäufigsten wird eine Identitätsprüfung durchgeführt (43 Prozent), gefolgt von eigenen Datenbanken mit kritischen Adressen (36 Prozent) und eingeschränkten Lieferoptionen (27 Prozent).

Doch auch hier gibt es zwischen Unternehmen mit weniger bzw. mit mehr als zehn Mitarbeiterinnen und Mitarbeitern Unterschiede: 66 Prozent der größeren Betriebe nutzen eine Identitäts- bzw. Bonitätsprüfung, um ihr Risiko zu reduzieren. Bei kleineren Firmen sind es nur noch vier Prozent, die sich dieser Schutzmaßnahme bedienen.

18 Prozent noch uninformiert. Trotz der Vielzahl potenzieller Schutzmaßnahmen gegen Onlinebetrug, gaben 18 Prozent der Händlerinnen und Händler an, sich mit dem Thema noch nicht auseinandergesetzt zu haben – bei Unternehmen mit weniger als zehn Beschäftigten sind es 24 Prozent. 27 Prozent informierten sich erst nach dem Launch ihres Webshops und 11 Prozent erst nach dem ersten Betrugsfall.

„Die Täter nutzen die Schwachstellen im Bestellprozess, deshalb ist es umso wichtiger, seinen Webshop abzusichern. Kleine und mittlere Unternehmen sind ebenso im Visier der Krimi-



Manuel Scherscher: „Täter nutzen die Schwachstellen im Bestellprozess, deshalb ist es umso wichtiger, seinen Webshop abzusichern.“

nellen und aufgrund der fehlenden oder zu geringen Maßnahmen ein beliebtes Ziel“, sagte Scherscher.

Die Studienergebnisse zeigen den Nachholbedarf, denn mehr als die Hälfte der Betriebe mit unter 10 Mitarbeiterinnen und Mitarbeitern führte an, keine Lösung zur Betrugsvermeidung zu verwenden. Bei größeren Unternehmen sind es 14 Prozent.

ONLINEHANDEL

Präventionstipps

- Wenden Sie sich an Unternehmen mit Erfahrungen im Onlinehandel und tauschen Sie sich aus.
- Setzen Sie beim Onlineshopping auf ein gesundes Misstrauen, besonders bei sehr günstigen Angeboten.
- Auf vielen Shopping-, Preisvergleich- und Auktionsseiten werden Handelsbetriebe beurteilt. Gute Bewertungen können ein Hinweis auf seriöse Geschäftspraktiken sein.
- Besondere Vorsicht ist bei Vorauszahlungsforderungen geboten.
- Zur Bezahlung sollten Konto- oder Kreditkartendaten über eine verschlüsselte Verbindung übertragen werden, erkennbar an „https“ in der Adresszeile und einem Schloss- oder Schlüsselsymbol.
- Erstellen Sie im Schadensfall eine Anzeige bei der nächsten Polizeiinspektion.

76 Prozent wollen Delikte anzeigen.

Hinsichtlich der Anzeigenerstattung bei Onlinebetrug gaben 76 Prozent an, zukünftige Betrugsfälle bei der Polizei anzeigen zu wollen. Dabei liegt das Hauptaugenmerk auf der Servicequalität. So möchten 76 Prozent alles mit einem Besuch erledigt wissen.

„Die Anzeige eines Internetbetrugs oder Cybercrime-Delikts ist besonders wichtig, denn erst dann sind wir in der Lage Täter auszuforschen und mögliche Serien zusammenzuführen“, merkte Scherscher an. „Bestellbetrug ist auch längst ein internationales Phänomen, weshalb das Bundeskriminalamt an mehreren Europol-Projekten teilnimmt. Gemeinsam.Sicher bietet zudem eine Plattform zum Austausch zwischen Polizei, Händlerinnen und Händlern sowie Kundinnen und Kunden.“

Auch Konsumentinnen und Konsumenten betroffen.

Neben der Unternehmenseite wurde die Konsumentenseite näher beleuchtet. 500 österreichische Verbraucherinnen und Verbraucher wurden hinsichtlich ihrer Erfahrungen mit Cybercrime befragt. Ein Drittel der Befragten hatte bereits mit einer Infizierung des Computers mit Schadsoftware, etwa Viren oder Trojaner, zu kämpfen. 15 Prozent waren schon von Datendiebstahl durch Phishing oder Hackerangriffe betroffen und weitere 14 Prozent wurden Opfer von Betrug bei Online-Transaktionen. 78 Prozent versuchen, sich mit Virenschutzprogrammen vor Cyber-Attacken zu schützen, 68 Prozent führen regelmäßig Softwareupdates durch und 63 Prozent haben eine Firewall implementiert.

Ein Problem stellen Fakeshops dar, denn fast ein Fünftel der Konsumentinnen und Konsumenten wurde bereits Opfer eines solchen. „Beim Kauf von Waren im Internet ist Vorsicht geboten, besonders bei Vorauszahlung. Informieren Sie sich auf der Webseite des Bundeskriminalamtes und seien Sie skeptisch bei besonders verlockenden Angeboten, denn auch im Internet wird nichts verschenkt“, sagte Scherscher.

Gefahr Blackout. Beim Sicherheitsgipfel 2022 im Bundeskriminalamt wurde auch die Gefahr eines Blackouts, welche Vorbereitungsmaßnahmen vom Handel bereits gesetzt wurden und welche Punkte Händlerinnen und Händler bei ihren Vorbereitungen bedenken müssen.

Romana Tofan