m retail

Austrian Cybercrime Dossier

Dossier

unter Mitwirkung von Handelsverband, Innenministerium und Bundeskriminalamt sowie führender Experten von PayPal, Taylor Wessing und EY Österreich

Herausgeber
Oliver Jonke
[o.jonke@medianet.at]

Editorial

Dagegen kann man etwas machen

Liebe Leserinnen und Leser!
Einhergehend mit dem wachsenden Komplexitätsgrad neuer Technologien, wächst bedauerlicherweise auch der Erfindergeist von Playern mit krimineller Energie. Und es werden immer mehr Player, die immer häufiger angreifen. Es trifft Konsumenten ebenso wie Unternehmen.

Es zahlt sich in jedem Fall aus, Angebote, die zu schön sind um wahr zu sein, lieber skeptisch und kritisch zu beurteilen. Dies sollten Sie übrigens auch dann tun, wenn jemand von Ihnen z.B. Reisepass- oder Führerscheindaten erfahren möchte. Eine aktuell häufige und durchaus dreiste Masche von Betrügern ist, sich als Vertreter einer Behörde auszugeben und vorzugeben, dringend Daten aus Ihren Dokumenten oder Kopien Ihrer Dokumente zu benötigen. Mit diesen erschlichenen Daten werden dann z.B. Konten eröffnet und Einkäufe getätigt.

Die meisten Unternehmen trifft es bei Angriffen völlig unerwartet, wenn sie z.B. mit „Ransomware" attackiert werden. Oftmals erkennt man sogar erst, dass man angegriffen wurde, wenn man erpresst wird. Manchmal reicht ein Klick auf einen Link in einer Phishing-E-Mail, um Zutritt zu einer Netzwerkumgebung zu erhalten und dort Malware zu installieren …

Prävention
Die Behörden haben immer mehr mit diesem Problemfeld zu tun: Vor über zehn Jahren wurde im Bundeskriminalamt das Cybercrimecenter (C4) installiert.

Jährlich werden hier über 15.000 Meldungen und Anfragen eingebracht –Tendenz stark steigend. Am neuen Standort im zweiten Wiener Gemeindebezirk werden rund 130 Cyber-Ermittler und Forensiker eingesetzt.

Für Unternehmen ist es unumgänglich, sich so gut wie möglich vorzubereiten. Die gute Nachricht: Die ersten und zugleich wichtigsten Schwachstellen, die man beheben kann, sind jene, die auf Unvorsichtigkeit und menschlichen Fehlern beruhen.

Lesen Sie in diesem Dossier über die aktuelle Entwicklung von Cybercrime in Österreich und über effiziente Maßnahmen, die gegen diese Gefahren wirken. Es entstand im Auftrag und unter Mitwirkung vom Handelsverband sowie führender Experten. Nutzen Sie ihre Erfahrungen!

Buchtipp: Lesen Sie gerne über spektakuläre Kriminalfälle? In Cornelius Granigs „Böses Geld" wird etwa der Fall „OneCoin" beschrieben – und wie hier in nur 18 Monaten 4 Mrd. Dollar gestohlen werden konnten.

Eine spannende Lektüre
wünscht Ihnen Oliver Jonke

Dossier: Austrian Cybercrime Dossier

Coverfoto: © PantherMedia/ Frank Peters

Inhalt

© PantherMedia/A. Guillen Fernández

Impressum

Medieninhaber:
medianet Verlag GmbH
1110 Wien, Brehmstraße 10/4. OG
http://www.medianet.at

Diese Sonderausgabe wurde von **media**net unter Mitwirkung vom Handelsverband erstellt.

Konzept: Oliver Jonke (Herausgeber)
Kontakt: o.jonke@medianet.at

Leitende Redakteurin dieser Ausgabe:
Helga Krémer (hk)

Lektorat: Christoph Strolz ***Grafik/Produktion:*** Raimund Appl, Peter Farkas ***Fotoredaktion/ Lithografie:*** Beate Schmid ***Druck:*** Ferdinand Berger & Söhne Ges.m.b.H., 3580 Horn
Erscheinungsort: Wien ***Stand:*** März 2022

Für den Inhalt verantwortlich:
Handelsverband
1080 Wien, Alser Straße 45

Abo, Zustellungs- und Adressänderungswünsche:

abo@medianet.at
oder Tel. 01/919 20-2100

Orientierungshilfe 4.0

Die Speerspitzen des Handelsverbands, Stephan Mayer-Heinisch und Rainer Will, über Vertrauen und Fallstricke in Onlineshops.

© Stephan Doleschal (2)

Vorkämpfer Handelsverband-Geschäftsführer Rainer Will (l.) und Präsident Stephan Mayer-Heinisch haben eine Mission: den sicheren Onlinehandel.

WIEN. Das Einkaufen verlagert sich verstärkt ins Internet. Doch nicht nur Händler und Kunden gehen mit der Digitalisierung mit, auch potenzielle Betrüger passen ihr dubioses Geschäft an. Handelsverband-Präsident Stephan Mayer-Heinisch und Geschäftsführer Rainer Will sprechen darüber, wie man Fake-Webshops erkennt und was Gütesiegel bringen.

medianet: *In der Pandemie mussten viele Shops ihre Filialen temporär schließen, das Shoppen im Internet wurde attraktiver. Daraufhin sind Tausende neue Webshops entstanden. Der persönliche Kontakt ist in den Hintergrund gerückt. Welche Rolle spielt Vertrauen im Webzeitalter?*
Stephan Mayer-Heinisch: Vertrauen spielt eine entscheidende Rolle für den Erfolg oder Misserfolg eines Onlineshops. In Zeiten immer häufiger auftretender Hackerskandale müssen insbesondere jene Onlinehändler, die noch vergleichsweise unbekannt sind, ihre Kundinnen und Kunden davon überzeugen, dass sie in einem seriösen Onlineshop gelandet sind.

medianet: *Wie wichtig ist der erste Eindruck?*
Rainer Will: Der erste Eindruck ist essenziell. Dabei spielen ein ansprechendes Design, gute Usability, eine übersichtliche Struktur und hochwertige Produktbilder eine wichtige Rolle. Tipp- oder Rechtschreibfehler, aber auch tote Links sollten unbedingt vermieden werden, da dadurch das Misstrauen der Kunden rapide ansteigt.

medianet: *Die nationale und internationale Konkurrenz im Onlinehandel ist groß. Wie können Händler im E-Commerce Vertrauen aufbauen?*
Will: Vertrauen kann am einfachsten mithilfe unabhängiger Dritter aufgebaut werden. Dafür eignen sich Kundenbewertungen und Gütesiegel. Kundenbewertungen im Internet sind zu vergleichen mit der klassischen Mundpropaganda. Wenn bereits viele andere in einem Onlineshop gekauft und eine positive Bewertung hinterlassen haben, steigt die Glaubwürdigkeit. Nichts ist aussagekräftiger als Empfehlungen von zufriedenen Käuferinnen und Käufern.

> *Vertrauen spielt eine entscheidende Rolle für den Erfolg oder Misserfolg eines Onlineshops. Die Kundschaft will wissen, mit wem sie es zu tun hat.*
>
> **Stephan Mayer-Heinisch und Rainer Will**
> *Handelsverband*

medianet: *Worauf müssen Händler im Onlinehandel grundsätzlich achten?*
Mayer-Heinisch: Um sich von unseriösen Angeboten abzugrenzen, sollten mehrere vertrauensbildende Maßnahmen gesetzt werden: Transparenz, Sicherheit, Kundenservice und der Einsatz von Kundenbewertungen und Gütesiegel wie das Trustmark Austria des Handelsverbandes stellen die wichtigsten Säulen dar. Ein vollständiges Impressum ist hilfreich, um den Kunden deutlich vor Augen zu führen, wer der dahinterstehende Anbieter ist – also mit wem sie es zu tun haben.
Will: Die Kundschaft will wissen, an wen sie sich wenden kann, wenn es Probleme gibt. Unter Transparenz fällt zudem die umfangreiche Aufklärung über die Verbraucherrechte, etwa das Widerrufsrecht, oder über den Umgang mit Daten. Zu guter Letzt sollten eine verschlüsselte Datenübertragung und das Anbieten von vertrauenswürdigen Zahlungsarten in keinem Onlineshop fehlen. Auf Konsumentenseite wird bekanntlich noch immer der Kauf auf Rechnung bevorzugt.

Online? Aber sicher!

Die gute Nachricht: Der Umsatz im heimischen eCommerce steigt. Die schlechte: Betrüger werden mehr und die verursachten Schäden höher.

© Ihar Ulashchyk/stock.adobe.com

Schon die zunehmende Digitalisierung hat unser aller Einkaufsverhalten maßgeblich verändert. Dann kam noch Corona mit all seinen Unbillen dazu. Diese Gemengelage ließ den Online-Handel schon 2020 um 17% ansteigen, 2021 um 20% – eCommerce boomt. Laut Handelsverband und Wirtschaftsforschungsinstitut (Wifo) werden bereits mehr als 90% der Distanzhandelsausgaben online getätigt.

„Die österreichischen Distanzhandelsausgaben werden vom eCommerce dominiert und erreichen 2021 mit 10,4 Mrd. Euro einen neuen Rekordwert. Von 9,6 Mrd. Euro Onlineumsatz entfallen bereits 2 Mrd. auf den Mobile Commerce – mit einem massiven Zuwachs von 67 Prozent“, sagt Rainer Will, Geschäftsführer des Handelsverbands.

Sichtweise
Wir wollen einkaufen, wann, wo und wie es uns gerade passt. Ehrlichkeit sollte dabei ein ständiger Begleiter sein. Dem ist aber (oft) nicht so.

So weit, so erfreulich, jetzt kommt das „Aber“: Mit steigendem Umsatz wächst auch das Risiko für Betrug, auch das ist im Vergleich zum Vorjahr gestiegen.

Grund zur Vorsicht

Aus der vom Handelsverband in Kooperation mit dem Innenministerium durchgeführten Sicherheitsstudie 2021 geht hervor, dass weit mehr als die Hälfte der heimischen Onlinehändler bereits Opfer von Betrug im Netz war, ein knappes Viertel auch schon mehrmals.

Ein besonders im Vergleich zu 2020 beunruhigendes Szenario; damals waren „nur“ 46% Betrügern aufgesessen, 13% mehrfach – 2021 waren es 62%, 24% mehrfach.

63%

Miese Masche
Das Bestreiten des Erhalts der bestellten Ware war 2021 die häufigste Betrugsform. Fiktive Zahlungsdaten kamen am seltensten vor.

Kurioses Detail der Sicherheitsstudie: Ein Prozent der heimischen Onlinehändler weiß überhaupt nicht, ob sie im Rahmen ihrer Tätigkeit Opfer von Netzbetrügereien wurden.

Immerhin sind 84% an weiterführenden Informationen zum Thema „Sicherheit im Onlinehandel“ interessiert.

Die Gegenüberstellung der verursachten Schadenssummen 2021 zum Jahr davor lässt selbst Hartgesottene schaudern: 2020 war die Mehrheit der Geschädigten noch im Bereich „unter 500 €“ angesiedelt, 2021 ist sie erst im Bereich „unter 10.000 €“ zu finden.

Über die Sicherheitsstudie

Analysten
Die Sicherheitsstudie 2021 wurde vom Österreichischen Handelsverband in Kooperation mit dem Bundesministerium für Inneres (BMI) durchgeführt.

Teilnehmer
143 Unternehmen aller Handelsbranchen und Größenordnungen (vom Ein-Personen-Unternehmen bis zum Konzern) haben teilgenommen und den Fragebogen vollständig ausgefüllt. Der Erhebungszeitraum betrug acht Wochen, Studienende war der 9. November 2021.

Weitere Infos auf: *www.sicherheitsgipfel.at*

Häufigste Formen
Auch bei den Betrugsformen gab es eine Umstellung im „Klassement". Mit 42% standen 2020 falsche Namens- oder Adressangaben ganz oben bei den Betrugsformen, 2021 zeigt sich perfider: Das Abstreiten des Erhalts der Ware kommt auf traurige 63%.

Zu den weiteren gängigsten Betrugsformen zählen, wieder, falsche Namens- oder Adressangaben (55%), in 50% der Fälle wird mit dem Wissen bestellt, dass die Rechnung nicht beglichen werden kann. Bei 48% hat ein Betrug im Zusammenhang mit Retouren stattgefunden. Aber auch die Angabe der Identität einer anderen Person und die Angabe gestohlener Zahlungsdaten, etwa Kreditkartendaten, kommen mit jeweils 43% häufig vor.

Nötige Schutzmaßnahmen
Immerhin haben mehr als drei Viertel der heimischen Onlinehändler konkrete Maßnahmen oder einen Mix dieser Maßnahmen zum Schutz vor Onlinebetrug in Verwendung.

Die meisten (55%) schränken ihr Risiko durch sichere Zahlungsoptionen ein und bieten z.B. keinen Kauf auf Rechnung an. 43% nutzen eine Identitätsprüfung, 36% führen eine eigene Datenbank mit kritischen Adressen, auch „Hotlist" genannt, 33% vertrauen auf eine Bonitätsprüfung, und ein Viertel hat Betrugsvermeidungssoftware im Einsatz. Etwas mehr als ein Viertel fokussiert auf die Lieferoptionen und lässt etwa keine Lieferung ins Ausland zu.

19% hat nichts dergleichen in Verwendung, ist aber an Präventionsmaßnahmen interessiert.

Alleine vs. Unterstützung
Wann sich Österreichs Onlinehändler Gedanken zur Implementierung geeigneter Maßnahmen zur Betrugsvermeidung machen? Die Mehrzahl erfreulicherweise bereits vor Erstellung ihres Onlineshops, 27% erst nachher.

Für 12% reichte ein einmaliger Betrugsfall zur Einführung von Sicherheitsmaßnahmen, 13% lernten es auf die harte Tour und mussten leider öfter Opfer von Online-Betrug werden, bevor sie sich mit dem Thema auseinandersetzten.

18% wähnen sich auf der Insel der Seligen und machen sich keine Gedanken über Präventivmaßnahmen.

Beliebte Geldflüsse
Das mag mit den angebotenen Zahlungsmethoden beim Check-out zu tun haben. 64% setzen auf Vorkasse und liefern erst, wenn der Rechnungsbetrag am Konto eingegangen ist. 85% lagern überhaupt aus und vertrauen auf PayPal bei der Zahlungsabwicklung.

Des österreichischen Onlinehändlers am liebsten angebotenes Zahlungsmittel ist mit 87% die Kreditkarte. Kaum genutzt wird Instant Payment, die SEPA-Echtzeitüberweisung – nur ein Prozent bieten sie an. Vor ein paar Jahren als großer Wurf im Zahlungsverkehr gepriesen, kann sie sich nicht recht durchsetzen, was an den teils horrenden Kosten pro Überweisung liegen kann oder auch nur daran, dass nicht alle Banken daran teilnehmen.

Noch immer beliebt ist der Kauf auf Rechnung, 50% gewähren ihn. Und wer ihn gewährt, der kombiniert ihn zumeist mit einer Bonitätsprüfung, sei es von einem Anbieter oder von einem Payment Service Provider. 14% vertrauen ihrer Kundschaft blind und lassen eine Bonitätsprüfung bleiben.

Bist du wirklich du?
Die Bedeutung der Eindeutigkeit von Kundendaten, also die „Echtheit" der Kunden, wird im ständig wachsenden eCommerce immer größer. Ganzen 91% ist eine verlässliche Authentifizierung/Identifizierung ihrer Kunden in ihrem Online-Geschäft sehr wichtig oder wichtig. Die Identität der Onlineshopper wird auch von den meisten Händlern (70%) überprüft, entweder bei Neukunden, je nach Warenkorbhöhe oder generell, weil es das Gesetz so vorschreibt.

Bei den dazugehörigen Dienstleistern liefern sich CRIF mit 37% und der Kreditschutzverband KSV mit 35% ein Kopf-an-Kopf-Rennen.

Dein Freund und Helfer
Und wenn's doch passieren würde? Was machen unsere Onlinehändler dann? Anzeigen oder nicht? Mehr als drei Viertel gingen sofort zur Polizei, sieben Prozent wären überraschenderweise *nicht* auf die Idee gekommen, den Betrug zur Anzeige zu bringen. Der Rest sieht für sich selber keine Vorteile oder nur Nachteile und lässt etwaige Betrüger lieber weiterhin Schaden anrichten – zum Schaden aller.

Schadenssummen

Schaden durch Onlinebetrug	
0 €	9,84%
unter 500 €	11,48%
unter 1.000 €	9,84%
unter 5.000 €	4,92%
unter 10.000 €	29,51%
unter 100.000 €	21,31%
unter 1 Mio. €	13,11%

Quelle: Handelsverband

© Pixabay/rupixen

Cybercrime das Handwerk legen oder gar verhindern

Die Kriminalität im Internet steigt weiter an, in den unterschiedlichsten Formen. Größter Posten: der Internetbetrug. Besonders betroffen: der eCommerce.

© Pixabay/Dr StClaire

WIEN. Die Digitalisierung öffnet uns weltweit viele Türen, zuweilen leider mit einem bitteren Beigeschmack. Denn egal, ob es sich um Schadsoftware, Datendiebstahl oder digitale Erpressung handelt, die Möglichkeiten von Cyberkriminellen nehmen rasant zu – auch im Onlinehandel.

eCommerce boomt, im Corona-Jahr 2021 ist die Branche in Österreich um 20% gewachsen. Mit steigendem Umsatz wächst aber auch das Risiko für Betrug, so die zentrale Erkenntnis der Sicherheitsstudie 2021, die vom Handelsverband in Kooperation mit dem Innenministerium und dem Bundeskriminalamt (BK) durchgeführt wurde.

Das Internet gilt leider weiterhin als Nährboden für verschiedenste Formen von Kriminalität. Covid-19 zeigt auch hier seine Tücken und befeuert Cybercrime noch zusätzlich – aber, Online-Händlerinnen und Händler aufgemerkt: Die Aufklärungsquote bleibt konstant hoch. Das besagt unter anderem der Lagebericht des Bundeskriminalamts über die Kriminalitätsentwicklung im Internet.

Trauriger Anstieg

Betrug im Netz ist allerdings keine Einbahnstraße: Bereits ein Fünftel der Konsumentinnen und Konsumenten haben laut der Sicherheitsstudie schon Erfahrungen mit Fake-Webshops gemacht.

„2021 sind Cybercrime-Delikte im Vergleich zu 2020 um 26 Prozent angestiegen. Ein Grund dafür ist gewiss die Covid-19-Pandemie, die Auswirkungen auf unterschiedlichste Bereiche unseres Zusammenlebens hat. Auffallend ist, dass sich Kriminalität von traditionellen Formen hin zu neuen Phänomenen wendet“, sagt Gerhard Karner, Bundesminister für Inneres. Die Kriminalität verlagere sich zusehends ins World Wide Web – vom Bestellbetrug bis hin zum Suchtmittelhandel.

Aber was fällt eigentlich alles unter Cybercrime? Cybercrime im engeren Sinne umfasst kriminelle Handlungen, bei denen Angriffe auf Daten oder Computersysteme unter Verwendung der Informations- und Kommunikationstechnik (IKT) begangen werden. Die Straftaten sind gegen die Netzwerke selbst oder aber gegen Geräte, Dienste oder Daten in diesen Netzwerken gerichtet, wie bei der Datenbeschädigung, dem Hacking oder DDoS-Angriffen. Betrügerischer Datenverarbeitungsmissbrauch gehört auch dazu – hier verzeichnete das BK 2020 massive Anstiege. Hauptgrund hierfür sind die zunehmende Verlagerung des täglichen Lebens in das Internet sowie die Schaffung neuer internetbasierter Zahlungsmöglichkeiten. Die betrügerische Verwendung von Near Field Communication (NFC) bei Bankomat- und Kreditkarten mache

© BMI/Karl Schober

hierbei den größten Anteil der Anzeigen aus. Auch die Fälle von Phishing seien angestiegen, heißt es im Cybercrime-Report 2020 des BMI.

Wo es einen engeren Sinn gibt, da ist der weitere nicht fern: Unter Cybercrime im weiteren Sinne werden Straftaten verstanden, bei denen die Informations- und Kommunikationstechnik als Tatmittel zur Planung, Vorbereitung und Ausführung von herkömmlichen Kriminaldelikten eingesetzt wird, wie Betrugsdelikte, Drogenhandel im Darknet, Online-Kindesmissbrauch, Cybergrooming oder Cybermobbing. „Es gibt also nur mehr wenige Bereiche, auch in der traditionellen Kriminalität, in denen Digitalisierung und IT keine Rolle mehr spielen", sagt Karner.

Konstante Aufklärung

Cybercrime in all seinen vielfältigen Erscheinungsformen stieg von 28.439 angezeigten Delikten im Jahr 2019 auf 35.915 im Jahr 2020 – dies bedeutet ein Plus von 26,3%. Trotz des beachtlichen Zuwachses konnte die prozentuelle Aufklärungsquote mit 33,4% nahezu konstant gehalten werden. Den größten Posten nimmt der Internetbetrug ein, er hat mit 18.780 Anzeigen einen neuen Höchststand erreicht.

Mahner

Manuel Scherscher, stellvertretender Direktor des Bundeskriminalamts und Leiter der Initiative „Gemeinsam. Sicher": „Der eCommerce-Boom ist auch den Kriminellen nicht entgangen."

© Bundeskanzleramt/Andy Wenzel

„Fast jeder, der einen Computer oder ein Smartphone hat, war schon einmal von Cybercrime betroffen. In den besten Fällen ist es bei einer versuchten Straftat geblieben und daher werden viele Delikte gar nicht zur Anzeige gebracht. Kriminelle stellen sich rasch auf neue Gegebenheiten ein und passen ihr Vorgehen an. Das haben wir auch während der Covid-19-Pandemie beobachtet", berichtet Andreas Holzer, Direktor des BK. „Unser Ziel als Kriminalpolizei ist, die Kriminellen strategisch zu überholen. Szenarien und Phänomene erkennen, bevor sie auftreten, warnen, ermitteln und Verbrecher schließlich dingfest machen."

Warnende Worte

Rainer Will, Geschäftsführer des Handelsverbands, bringt das pandemiebedingte Wachstum an Webshops und Onlinebestellungen mit den häufigeren Delikten, neuen Betrugsmaschen und deutlich höheren Schäden in Zusammenhang und warnt: „Handlungsbedarf ist gegeben. 2021 waren bereits fast zwei Drittel der heimischen Händler Opfer von Betrug im Netz, ein Viertel sogar schon mehrmals. Damit steht Internetbetrug weit oben auf der Liste potenzieller Bedrohungen für den Handel. Die Schäden nehmen zu und gehen teilweise in die Millionen." Ähnlich sei die Situation auf Konsumentenseite: Jeder Zweite schätze die Gefahren im eCommerce als hoch ein. Für Online-Shopper zähle Sicherheit mittlerweile zu den wichtigsten Kaufkriterien.

Der eCommerce-Boom sei auch den Kriminellen nicht entgangen, mahnt Manuel Scherscher, stellvertretender Direktor des BK und Leiter der Initiative „Gemeinsam. Sicher": „Sie nutzen die vermeintlichen Schwachstellen im Bestellprozess von Webshops für ihre Machenschaften. Die missbräuchliche Verwendung real existierender Identitäten beim Kauf auf Rechnung stellt den Großteil der angezeigten Delikte im Jahr 2021 dar."

Beobachtung

„Auffallend ist, dass sich Kriminalität von traditionellen Formen hin zu neuen Phänomenen wendet", erklärt Gerhard Karner, Bundesminister für Inneres.

Sicherheitsaspekte

Eines zeige die Sicherheitsstudie 2021 deutlich: „Es ist aus Sicht der Polizei unumgänglich, ein besonderes Augenmerk auf den Faktor Sicherheit im Onlinehandel zu werfen", betont Scherscher. Die Polizei forciere neben der Repression, der Verfolgung der Täter, verstärkt auch den präventiven Aspekt.

„Mit dem Programm ‚Gemeinsam. Sicher' im Onlinehandel haben das Bundeskriminalamt und der Handelsverband eine Plattform geschaffen, die es den heimischen Händlern ermöglicht, Sicherheitsaspekte bei der Etablierung ihres Webshops stets mitzudenken. Die Kooperation zwischen Polizei und Privatsektor stellt ein wesentliches Element dar, die Sicherheit im Onlinehandel zu verbessern", erklärt Scherscher das Ziel der Kooperation.

Kriminalität im Internet sei eine Straftat, die nicht hingenommen werde, sagt Karner: „Daher werden wir den Kampf gegen Cybercrime noch stärker forcieren und den Fokus auf die Präventionsarbeit richten."

Mehr Details

Nähere Informationen zum Thema Cybercrime sowie den Cybercrime Report 2020 des BMI unter:

www.bundeskriminalamt.at/cybercrime

Die dunkle Seite des Fortschritts

Wer IKT nutzt, sollte sich zu seiner eigenen Sicherheit mit ein paar unerfreulichen Gegebenheiten vertraut machen.

In der einschlägigen Literatur umfassen die Begriffe Computerkriminalität, Cyberkriminalität oder englisch **Cybercrime** „alle Straftaten, die unter Ausnutzung der Informations- und Kommunikationstechnik (IKT) oder gegen diese begangen werden". Davon abzugrenzen wäre eigentlich die **Internetkriminalität** – Straftaten, die auf dem Internet basieren oder mit den Techniken des Internets geschehen. Eigentlich, denn wer fragt schon nach, wie der Hund heißt, von dem man eben gebissen wurde.

Kenne die Bedrohung …

Im Großen und Ganzen lässt sich Cyberkriminalität in zwei Kategorien unterteilen:

- Kriminelle Aktivitäten, die auf Computer *abzielen.*
- Kriminelle Aktivitäten, die Computer *benutzen,* um weitere Verbrechen zu begehen.

In einigen Fällen können Cyberkriminelle beide Arten gleichzeitig nutzen: Zunächst werden z.B. mit Viren gezielt Computer infiziert, damit diese anschließend genutzt werden können, um Malware auf weitere Netzwerkgeräte zu übertragen.

Hier ein paar konkrete Beispiele für die verschiedenen Auswüchse der Cyberkriminalität:

- **E-Mail- oder Internetbetrug**
- **Identitätsbetrug** (Persönliche Daten werden gestohlen und missbraucht.)
- **Diebstahl von Kreditkarten- und Bankdaten**
- **Diebstahl von Unternehmensdaten**

- **Cyber-Erpressung** (Hacker verlangen Geld, um drohende Angriffe abzuwenden.)
- Angriffe durch **Ransomware** („Ransom", der englische Begriff für „Lösegeld", ist hierfür namensgebend. Der Angreifer verschlüsselt die Daten der Opfer und verlangt ein Lösegeld für den privaten Schlüssel. Darunter fällt die Attacke „WannaCry" im Jahr 2017. Der weltweite finanzielle Schaden, der durch WannaCry verursacht wurde, wird auf 4 Mrd. USD geschätzt.)
- **Cryptojacking** (Zum Generieren von Cryptowährungen benutzen Hacker Ressourcen, die sie nicht besitzen.)
- **Cyber-Spionage** (Hacker verschaffen sich Zugriff auf Regierungs- oder Unternehmensdaten.)

Trügerisch
Kriminelle kommen im Netz als Einzeltäter oder als organisierte „Bande" vor. Cybercrime ist heutzutage ein professionelles Geschäft.

… handle vernünftig …
Experten im Bereich der Cybercrime-Bekämpfung kommen nicht umhin, wieder und wieder zu warnen und zu mahnen: „Halten Sie Ihre Programme und Ihr Betriebssystem aktuell. Verwenden Sie Antiviren-Software und halten Sie diese aktuell." Damit wäre im Bereich der Technik schon einiges getan.

Und sonst? Sonst liegt es im Bereich jedes einzelnen, wie er Folgendes handhabt:

- Die **Qualität der Passwörter:** Sie sollen nicht zu erraten sein und nicht abgeschaut werden können. Gerne werden Passwortgeneratoren empfohlen, die nach dem Zufallsprinzip starke Passwörter generieren und sicher speichern.
- **E-Mail-Gebrauch:** Ein klassischer Weg, um seinen Computer mit Malware-Attacken oder anderen Arten von Cyberkriminalität zu infizieren, geht über E-Mail-Anhänge. Anhänge von unbekannten Absendern besser ignorieren oder die ganze bedenkliche E-Mail ungelesen löschen. Spam-Mails zeichnen sich oft durch „abenteuerliche" Sprache und Schreibweisen aus.
- **Links:** Werden häufig via Spam-Mails versendet oder sie locken auf ohnehin schon dubiose Webseiten. Den Drang, auf den Link zu klicken, sollte man sich, zu seiner eigenen Sicherheit, versagen.

1
Bio. $

Kostspielig
Cyberangriffe kosten die Weltwirtschaft im Jahr 2020 laut einer Studie mehr als eine Billion USD – um die Hälfte mehr als noch 2018.

… sei wachsam & realistisch
Sicher, die Betreffzeile „Sie haben gewonnen!" oder wahlweise „geerbt" klingt auf den ersten Blick verlockend. Genauso, wie die Zahlungsaufforderung eines Inkassobüros gleich einmal bedrohlich daherkommt. Nur: Man hat nirgends gespielt, auch das Erbe des vorgeblich unermesslich reichen, mittlerweile verstorbenen Onkels im afrikanischen Drübsdrü kann mit Sicherheit ausgeschlossen werden. Genauso wie der Erwerb des asiatischen Tigerkrallen-Potenzmittels, das nun zu berappen wäre.

Meist sind die Täter dann erfolgreich, wenn Unerfahrenheit, gepaart mit Leichtgläubigkeit, im Spiel sind. Daher rät das BKA: „Beweisen Sie Hausverstand!"

© PantherMedia/Antonio Guillen Fernández

Vom richtigen Umgang

Zusammengefasst
Kein seriöses Unternehmen fordert telefonisch oder per E-Mail dazu auf, Daten preiszugeben.

Niemals Geld an unbekannte Personen überweisen oder übergeben.

Ist man aller Vorsicht zum Trotz Opfer einer Straftat geworden, alle vorhandenen Beweismittel sichern und Anzeige erstatten. Auch konkrete Hinweise auf einen Täter können angezeigt werden. Dies ist in jeder Polizeidienststelle in Österreich möglich.

Beratung und Hilfe
Im Bundeskriminalamt bei der Meldestelle im Cybercrime Competence Center:
against-cybercrime@bmi.gv.at
www.bundeskriminalamt.at/praevention

Die Internet Ombudsstelle hilft als unabhängige Beratungs- und Streitschlichtungseinrichtung bei Problemen mit Interneteinkauf, Datenschutz, Urheberrecht und Internetbetrug.
www.ombudsstelle.at

© EY Österreich

Cyberexperte Gottfried Tonweber leitet den Bereich Cybersecurity & Data Privacy bei EY Österreich.

Gute Vorbereitung, bessere Geschäfte

Unüberlegtes Handeln hat noch selten Erfolg gezeitigt – besonders im Bereich Onlinehandel und Cybersafety.

Gastkommentar
••• *Von Gottfried Tonweber*

WIEN. „In allen Dingen hängt der Erfolg von den Vorbereitungen ab." Dieses Zitat des chinesischen Philosophen Konfuzius gilt fast immer – auch dann, wenn Handelsunternehmen überlegen, die Präsenz im Internet auf- und auszubauen.

Der Handel im Umbruch
Die Pandemie hat enorme Auswirkungen – gerade auf den stationären Handel. Viele Unternehmen, die noch über kein digitalisiertes Angebot verfügen, sehen sich zunehmend gezwungen, ihre Kunden auch über das Internet zu erreichen und ihnen die Möglichkeit zur Interaktion und zum Warenkauf zu bieten.

Hand in Hand mit den Möglichkeiten, die dem Händler digitale Plattformen bieten, kommen auch die Risiken. Internet-Kriminalität zielt besonders auf Unternehmen ab, und jeder erfolgreiche Angriff bedeutet Schaden – in Geldwert, in der Reputation, in der Fähigkeit zur Geschäftsfortführung.

Von lauernden Gefahren …
Dieses Problem erkennen auch Unternehmen der Handels- und Konsumgüterbranche in Österreich: Rund zwei Drittel der Unternehmen nehmen laut EY-Datendiebstahlstudie an, dass die Gefahr durch Cyberangriffe steigen wird – auch wenn nur ein verschwindend geringer Teil der Unternehmen einen Zuwachs von Cyberangriffen seit Ausbruch der Pandemie im März 2020 feststellen konnte.

Zwei Drittel der Betriebe hatten im Lockdown Mitarbeiterinnen und Mitarbeiter im Homeoffice – häufig ohne genügend Vorbereitungszeit. So steigt natürlich auch das Risiko, Ziel eines Angriffs zu werden. Sicherheit im digitalen Zeitalter gelingt nur dann, wenn Menschen nach effizienten und sicheren Prozessen arbeiten und Vorgaben umsetzen. *Bewusstseinsbildung* ist das beste Gegenmittel gegen jede Form von Schädigung durch illegale Aktivitäten über digitale Plattformen. Aufmerksame und vor allem regelmäßig geschulte Mitarbeitende bilden eine breite Abwehrlinie gegen Betrugsversuche, Ransomware und Phishing. Jede noch so leistungsfähige technische Sicherheitsmaßnahme verliert ihre Kraft, wenn die Belegschaft nicht ausreichend sensibilisiert ist.

… und deren Adressierung
Mit guter Planung, abgestimmten Prozessen und aktueller Technik zur Schaffung von Cybersecurity ist Ihre Transformation in Sachen Digitalisierung kein experimentelles Abenteuer mehr. Wir stehen bereit, Sie und Ihr Unternehmen sicher zu machen – vollumfänglich, mit dem Know-how eines internationalen Beraters und lokaler Expertise.

Better safe than sorry

Entscheidende Faktoren für einen sicheren Bezahlvorgang – wie man es der redlichen Kundschaft angenehm und der bösen richtig schwer machen kann.

WIEN. Der Schutz von sensiblen Kundendaten ist ein wichtiges Thema. Für Onlinehändler gilt es, die eigene Cybersecurity so aktuell wie möglich zu halten, vor Innovationen nicht zurückzuschrecken und Investitionen zu wagen.

Unternehmen und Organisationen sind durch Cyberkriminalität und Online-Betrug großen Risiken ausgesetzt. Eine Umfrage des Ponemon Institute unter 632 Unternehmensleiterinnen und Unternehmensleitern in den USA ergab: Durchschnittlich erleiden Unternehmen Schäden in Höhe von 4,5 Mio. USD pro Jahr durch Cyberkriminalität.

Gleichzeitig stieg laut dem Handelsverband Österreich der Umsatz des eCommerce-Sektors im Jahr 2021 pandemiebedingt auf ein Rekordhoch von 9,6 Mrd. €. Mehr Onlineshopping bedeutet somit auch mehr potenzielle Angriffspunkte für Cyberkriminelle.

Sicheres Einkaufsvergnügen

PayPal möchte als Zahlungsdienstleister kleine und mittelständische Unternehmen dabei unterstützen, Verbrauchern ein sicheres Shopping-Erlebnis zu ermöglichen. Dazu führen PayPals Big-Data-Analysen und maschinelle Lernfunktionen ständig Prüfungen durch, um sicherzustellen, dass eine Transaktion in Sekundenbruchteilen sicher abläuft.

Darüber hinaus können Händlerinnen und Händler mit den richtigen Tools und Prozessen dazu beitragen, ihr Geschäft, aber auch ihre Kundinnen und Kunden zu schützen.

Vielsagende Anschrift

Ein wertvolles Tool, um betrügerische Kundschaft von der willkommenen zu unterscheiden, ist das Address-Verification-System (AVS) – ein Betrugstool, das bei den meisten Zahlungsdienstleistungsprogrammen enthalten ist. Dieses vergleicht den numerischen Part der Rechnungsadresse einer Kreditkarte mit der Adresse, die bei der Kreditkartengesellschaft hinterlegt ist. Darüber hinaus sollte eine kurzfristige Änderung der Lieferadresse genau geprüft werden: Betrügerinnen und Betrüger versenden Bestellungen unter anderem an Postfächer, um unerkannt zu bleiben.

© PayPal (2)

Sicher zahlen
Ganz gleich, auf welcher Seite des Bezahlvorgangs: Wachsamkeit und entsprechende Tools können dabei helfen, sich gegen Cyberkriminalität zu schützen.

Communication is King

Händlerinnen und Händler können ihre Kundschaft durch Aufklärung über sicheres Onlineshopping unterstützen. Gerade neue Kundinnen und Kunden sind oftmals unerfahren und müssen für Sicherheitsstandards sensibilisiert werden.

Zudem ist es wichtig, auch die Mitarbeitenden einzubeziehen, da Betrügerinnen und Betrüger nach Schwachstellen in Systemen und nach menschlichen Fehlern suchen. Die meisten Cyberkriminellen nutzen vor allem die Unwissenheit ihrer Opfer aus.

Moderne Softwaresysteme

Ein stets aktuelles Softwaresystem schützt vor neu entdeckten Sicherheitslücken sowie vor der neuesten Viren- und Schadsoftware. Händlerinnen und Händler sollten außerdem eine angemessene Anti-Malware- und Anti-Spyware-Software installieren und regelmäßig aktualisieren.

cft6&zjmMKO=0pö-_Ä*

Passwörter und der Verlust von Finanzdaten sind zwei der größten Risikofaktoren im digitalen Ökosystem. Ein Vorteil von PayPal für Verbraucher: Die eigenen Finanzdaten müssen nicht im Onlineshop angegeben werden; die Zahlung erfolgt über die Weiterleitung in das PayPal-Konto. Damit unterstützt PayPal aktiv die Onlinesicherheit der Händlerinnen und Händler.

Letztlich geht es bei der Betrugsbekämpfung nicht nur darum, das finanzielle Risiko von Händlern oder den Verlust von Waren zu begrenzen, sondern Kundinnen und Kunden ein sicheres Shopping-Vergnügen zu bieten.

Ausgesperrt
Onlinehandeltreibende sehen sich zunehmend mit Kriminalität im „Netz" konfrontiert und müssen sich die Frage stellen: Wie sperre ich die Bösen aus?

Vom Faktor Mensch

Unternehmenssicherheit ist so gut, wie die Menschen, die in dem Unternehmen arbeiten. Besonders in der Cyberwelt.

WIEN. Der stationäre Handel hat im Laufe der Zeit umfassende Maßnahmen ergriffen, um sich gegen Diebstahl, Einbruch, etc. zu schützen. Im 21. Jahrhundert muss auch das digitale Geschäftslokal, also der Onlineshop, gegen betrügerische Handlungen gesichert werden – unabhängig davon, ob es sich um einen völlig neuen oder einen bereits bestehenden handelt.

Die notwendige Technik lässt sich durchaus an einen profunden Dienstleister auslagern, ebenso die Zahlungsabwicklung. Das eigene Geschäft führt man aber schon noch selbst, zumeist mit mehr oder weniger Mitarbeitern. Und so wie man seinen Onlineshop so cyberfit wie möglich hält – oder halten lässt –, sollte es die Belegschaft auch sein.

© Pixabay/Gerd Altmann

Immer am Ball bleiben

„Halten Sie sich stets auf dem Laufenden hinsichtlich aktueller Betrugsmaschen", empfiehlt Robert Spevak, Leiter des Handelsverband-Ressorts Sicherheit im Handel. „Geben Sie Sicherheitsregeln vor und halten Sie diese ein! Sensibilisieren Sie Angestellte auf Cybergefahren und schulen Sie Cybersicherheit." Eigene Awareness-Schulungen können da hilfreich sein. Wem nun der selige Helmut Qualtinger bzw. sein Alter Ego Travnicek in den Sinn kommt – „Wos brauch' i des?" –, der möge sich folgende Fragen beantworten: Sind meine Mitarbeiter in der Lage, kritisch mit betrügerischen Social-Engineering-Attacken wie fingierten Kundenanrufen, gefälschten Dokumenten, Phishing-E-Mails oder gar vorgetäuschten internen Anweisungen umzugehen? Gibt es in meinem Unternehmen ein Bewusstsein dafür, welche Mails und Webinhalte gefährlich sein könnten und wie man beispielsweise fremde USB-Sticks handhaben sollte?

Know-how

Robert Spevak steht als führender Experte im Bereich Unternehmenssicherheit beim Handelsverband als Ansprechpartner zur Verfügung.

© Robert Spevak

Raffiniert und gefährlich

Cyberangriffe auf Unternehmen sind heute häufiger, raffinierter und gefährlicher als je zuvor. Unternehmen und ihre Mitarbeiter bieten vielfach erhebliche Angriffsflächen für Schadsoftware oder gezielte Recherchen von Cyberkriminellen, um in das Unternehmensnetzwerk einzudringen. Nicht nur auf den Webauftritten der Unternehmen finden sich wertvolle Informationen, Cyberkriminalität macht auch vor (privaten) Social Media-Kanälen nicht halt.

Uferlos

Der kriminellen Energie sind kaum Grenzen gesetzt; umso wichtiger ist es, das eigene und das Bewusstsein der Mitarbeiter auf Cyberkriminalität zu schärfen – und immer wieder nachzuschärfen.

Polizeiliche Unterstützung

Um Mitarbeiter auf Online-Betrug zu sensibilisieren, vertraut Spevak, im Brotberuf Abteilungsleiter Audit & Security bei Metro Cash & Carry Österreich, zudem auf die Polizei. „Wir arbeiten intensiv mit der Polizei zusammen. Die Ergebnisse sind überaus positiv. Die Beamten kommunizieren uns, was aktuell im Umfeld passiert, wir als Unternehmen wiederum geben diese Hinweise an unsere Mitarbeiter weiter, damit sie auf diese Geschehnisse achten können bzw. darauf vorbereitet sind."

Denn der überwiegende Teil aller Security-Vorfälle ist auf menschliches Versagen zurückzuführen; das schwächste Glied in der Security-Kette ist der Mensch. Der ist aber lernfähig.

Vertrauen ist alles
Das Technologieunternehmen CRIF ist spezialistiert auf datenbasierte Lösungen für Identitäts- und Risikomanagement, Betrugsvermeidung sowie Digitalisierung.

„A Matter of Trust“ des eCommerce

Vertrauensprobleme im Onlinehandel sind beiderseits plausibel. Die Lösung: Kauf auf Rechnung + Prüfung.

WIEN. Mit der Pandemie verlagerte sich das Einkaufen bekanntlich zunehmend ins Internet, und der Konsument hat die Vorzüge des Onlineshoppings lieben gelernt. Während des ersten Lockdowns saß gefühlt halb Österreich auf der Couch und shoppte im Netz, bis die Finger glühten.

Ein paar Klicks und schon wird alles, was das Herz begehrt, nach Hause geliefert. Gustiert und probiert wird zu Hause in aller Ruhe. Was nicht gefällt, wird zurückgeschickt – ganz ohne Risiko. Denn bezahlt wird erst, wenn man die Ware auch tatsächlich behalten will – zumindest, wenn man bei der Onlinebestellung die Bezahloption „Kauf auf Rechnung“ gewählt hat, resp. wählen konnte.

Erst die Ware, dann das Geld
Warum die so wichtig ist? Neukunden, die das erste Mal bei einem Onlinehändler bestellen, müssen darauf vertrauen können, dass es sich nicht um einen der immer häufiger im Internet aufpoppenden Fakeshops handelt, der nach der Bezahlung entweder keine Ware oder ein gefälschtes Produkt verschickt. Noch wichtiger ist Konsumenten allerdings, erst dann für Waren zu bezahlen, wenn sie ihre Bestellung in Händen halten und diese auch behalten wollen. Nichts ist für sie ärgerlicher, als bei Retouren auf die Rückabwicklung ihrer Zahlung warten zu müssen.

Kein Wunder also, dass beim Onlineshopping Kauf auf Rechnung in der Kundengunst auf Platz eins der beliebtesten Bezahlmethoden rangiert. Oft gelingt die Conversion vom Interessenten zum Neukunden aufgrund fehlender Bezahloptionen nicht. Und immer muss sich der Onlinehändler fragen: „Ist die Person die zahlungsfähige Person, die sie vorgibt zu sein?“ „Für Onlineshops ist die Bezahlung auf Rechnung ein Conversionstreiber – schließlich kann diese Option den Umsatz um fast 40 Prozent steigern – und Gefahrenquelle zugleich“, weiß Gerald Eder, Sales Director Digital Solutions beim Risikomanagement- und Fraud Prevention-Spezialisten CRIF.

Onlinehändler, die kein Risiko eingehen wollen, haben ihren Webshop mit einer Identitäts- und Bonitätsprüfung im Vorfeld entsprechend abgesichert.

Technische Expertise
Als einziger Anbieter ermöglicht etwa CRIF vernetzt automatisiertes Risiko- und Fraud Prevention Management im D-A-CH-Raum und auch in anderen europäischen Ländern. „Prüfen Sie die Bonität und die Identität Ihrer Kunden *automatisiert* und in *Echtzeit*. Reduzieren Sie auf diese Weise das Ausfallsrisiko auf ein Minimum und beugen Sie Betrug frühzeitig vor“, rät Eder.

Denn reibungslose Bezahlprozesse führen zu zufriedenen Kunden und damit zu mehr bzw. höheren Umsätzen.

Unzureichende Bezahloptionen können Kunden nachhaltig vertreiben.

Digitale Nämlichkeit

Mit verlässlicher Kundenauthentifizierung dem Identitätsmissbrauch einen Riegel vorschieben.

© Payment Services Austria

Entwicklung „Hochsichere Technologien unterstützen den Zahlungsverkehr", so Thomas von der Gathen, General Counsel, PSA.

WIEN. Die sukzessive Umstellung auf neue, einfacher im Internet nutzbare Bankomat-Karten (Debitkarten) erhöhte die Zahl der damit getätigten eCommerce-Transaktionen im Jahr 2021 auf über 44 Mio.: Das damit getätigte Transaktionsvolumen stieg auf knapp 1,8 Mrd. €, rechnet die Payment Services Austria GmbH (PSA), das österreichische Kompetenzzentrum für bargeldloses Bezahlen, vor. Dies bedeute jeweils eine Verdopplung.

Aber gehört die betreffende Karte auch dem demjenigen, der im Onlineshop vorgibt, der Karteninhaber zu sein? „Immer wichtiger wird es für Onlinehändler, ihre Kundschaft zu kennen. 90 Prozent der Befragten geben in der aktuellen Studie des Handelsverbands an, dass ihnen eine verlässliche Authentifizierung/Identifizierung ihrer Kunden sehr wichtig oder wichtig ist", spricht Thomas von der Gathen, General Counsel, PSA, das Problem des Identitätsmissbrauchs an.

Bist du ganz sicher du?

Ein Problem, dessen sich PSA verstärkt angenommen hat, nachdem das Unternehmen 2021 neue Aufgaben zusätzlich zum Kartengeschäft und der Betreuung des Bankomat-Systems übernommen hat, etwa Konto zu Konto-Überweisungen, EPS und Identity Services.

„Der nächste Schritt dazu ist die Erweiterung der PSA Identity Services um eine elektronische Identität (eID), die ich.app. Sie ermöglicht es Unternehmen und Menschen auf einfache und zugleich sichere Art, sich online eindeutig zu identifizieren, digitale Services anzubieten und Geschäfte abzuschließen", so von der Gathen.

Die Händler erhalten mit der ich.app die gewünschten Kundeninformationen genauso bestätigt, wie sie bei der Bank hinterlegt sind. Damit können sie sicher sein, dass der Kunde „echt" ist.

„Cybersicherheit ist Chefsache"

Experten der Anwaltskanzlei Taylor Wessing über rechtliche Aspekte und Cyber Incidents.

WIEN. Wo ein Schaden auftritt, ist die Frage der Haftung nicht weit. Oder, salopper formuliert: Einer muss schuld sein.

Wie es sich mit der Haftung bei Cybercrime-Vorfällen verhält, erklären Andreas Schütz, Partner und Datenschutzexperte bei Taylor Wessing, und Ivo Deskovic, Partner und Experte für Streitbeilegung bei Taylor Wessing, im Gespräch mit **media**net.

medianet: *Wo sind die Grenzen der Cybercrime Haftung im Allgemeinen?*

Ivo Deskovic: Cybersicherheit ist eindeutig ‚Chefsache'. Eine Entscheidung des OGH stellt klar, dass die Datensicherheit jedes Unternehmens immer am Stand der Technik sein muss. Vorstand bzw. Geschäftsführung haften sohin dafür, dass die Systeme up-to-date sind, ausreichend Guidelines bestehen, die Mitarbeiter geschult

Experte für Streitbeilegung und Partner bei Taylor Wessing, Ivo Deskovic.

sind und Umsetzung und Einhaltung auch laufend überprüft werden.

medianet: *Wer haftet für Fehler der Mitarbeiter?*

Deskovic: In vielen Fällen sind Cyber Incidents auf menschliche Fehlleistungen zurückzuführen. Bei ausreichender Schulung haften dafür nicht die Geschäftsleiter, und bei leichtem Verschulden auch nicht die Mitarbeiter. Jedoch kann das Unternehmen selbst haften, vor allem gegenüber Vertragspartnern. Das gilt auch für immaterielle Schäden.

medianet: *Was sind immaterielle Schäden beim Cyber Incident?*

Andreas Schütz: Die DSGVO hat u.a. bei Datenschutz-Vorfällen auch eine Haftung jedes Verantwortlichen für immaterielle Schäden gebracht. Das sind Schäden, die sich nicht direkt in Geld ausdrücken, wie etwa Schmerzensgeld oder Imageschäden. Gerade Letzteres kannten wir in Österreich bisher nicht.

In einem Testfall hat daher der OGH heuer im Zuge eines Vorabentscheidungsverfahrens die Frage an den EuGH gestellt,

© Taylor Wessing/Clemens Mayer (2)

Andreas Schütz ist Partner und Datenschutzexperte bei Taylor Wessing.

ob jeder Datenschutz-Vorfall, also z.B. ein Datenleck von persönlichen Daten, zu einem Ersatz führt, auch wenn gar kein erkennbarer Schaden entstanden ist. Denkbar ist nämlich tatsächlich der Ersatz von rein theoretischen Beeinträchtigungen.

Wehret der Abzocke

„Sein oder Nichtsein“, sinnierte Hamlet bei Shakespeare. Leicht abgewandelt fragt man sich heute: „Fake oder echt?“

WIEN. Auf den ersten Blick zeigt sich die erstmalig aufgerufene Website unauffällig. Auch der dazugehörende Webshop. Zwar gibt es zu diesem Bewertungen, doch die sind ausschließlich positiv und klingen alle fast zu gut, um wahr zu sein. Unsicherheit macht sich breit – ist der Shop echt oder Fake? Aber wen fragen?

Da bieten sich Unternehmen wie Scamadviser an. Mithilfe der globalen Online-Community und künstlicher Intelligenz sieht sich Scamadviser Websites und Shops genauer an und bringt Licht ins Dunkel. Wie man einen online-Fakeshop erkennen kann und wie Scamadviser funktioniert, erklären Patricia Grubmiller, Head of Legal Handelsverband, und Jorij Abraham, General Manager Scamadviser, im Interview.

medianet: *Woran lässt sich ein Fake-Onlineshop erkennen?*
Patricia Grubmiller: Die einfachste Regel lautet: Wenn ein Angebot zu gut ist, um wahr zu sein, dann ist es das sehr wahrscheinlich auch. Ist der Preis auf einer Website um zum Beispiel 40 Prozent günstiger als anderswo, dann sollte man bereits sehr vorsichtig sein. Andere Auffälligkeiten sind: das Fehlen von Kontaktdaten, Grammatikfehler und eine große Anzahl sehr positiver Bewertungen in kurzer Zeit. Denn normalerweise hinterlässt nur einer von 200 Verbrauchern ein Rating, sodass eine neue Website Zeit benötigt, bis sie viele Bewertungen erhält.

medianet: *Herr Abraham, was ist ‚Scamadviser‘?*
Jorij Abraham: Scamadviser hilft Verbrauchern, ihre Entscheidungen beim Online-Shopping zu treffen. Dafür prüft ein Algorithmus mithilfe von 40 unabhängigen Datenquellen, ob die Website legal betrieben wird, ob die darauf veröffentlichten Bewertungen echt sind oder aber, ob es sich um eine Pishing-Website handelt. Jede Website erhält ihren eigenen Trust Score, für dessen Ermittlung unter anderem die IP-Adresse des Webservers, die Verfügbarkeit von Kontaktdaten, das Alter der Domain und Ratings auf Bewertungsplattformen herangezogen werden.

© PantherMedia/Wolfgang Cibura

Gut & böse
Die schwarzen Schafe der Online-Shops spürt Jorij Abrahams Scamadviser mittels Algorithmus auf. Alle „Schafe“ erhalten eine eigene Bewertung, den Trust Score.

© Scamadviser/Eric de Bruijn

medianet: *Und wie kommen Sie zu diesen Daten?*
Abraham: Scamadviser erhält täglich etwa 800 Bewertungen, Kommentare und E-Mails von Verbrauchern über verschiedene Websites. Diese werden automatisch zur Auswertung jeder Website verarbeitet. Dabei verlassen wir uns nicht auf *eine* negative Bewertung, um einer Website einen schlechten ‚Trust-Score‘ zu verpassen, denn sonst müssten z.B. auch apple.com und amazon.com als betrügerische Seiten gelistet sein – was ja in beiden Fällen nicht zutrifft.

Regel Nr. 1
„Ist das Angebot zu gut, um wahr zu sein, besser die Finger davon lasssen“, rät Handelsverband-Juristin Patricia Grubmiller. „Denn dann ist es höchstwahrscheinlich eine Abzocke.“

medianet: *In welchen Ländern spielt Online-Betrug eine besonders große Rolle? Gibt es regionale Auffälligkeiten?*
Grubmiller: Da jedes Land auf seine eigene Weise Daten über Online-Betrug sammelt, ist es schwierig, einzelne Länder zu vergleichen. Indien und Mexiko melden die meisten Betrugsfälle, relativ betrachtet sind das jeweils 103 bzw. 80 pro 1.000 Einwohner. Im Großteil der westlichen Länder liegt diese Zahl eher zwischen 2,5 und 6.
Abraham: Eine Scamadviser-Studie, inklusive eines globalen Betrugsberichts, veranschaulichte, dass jedes Land seine eigenen Präferenzen in Bezug auf Betrug hat.

Chinesen fallen oft auf Gaming-Betrug herein: Es werden virtuelle Skins, also Gaming-Kostüme und Waffen gekauft, die dann aber nicht geliefert, sprich im Game nicht zur Verfügung gestellt werden. Die Amerikaner waren letztes Jahr besonders für Welpenbetrug geeignet. Viele indische Kunden glauben daran, schnell reich zu werden, indem sie in Kryptowährungen und sogenannte High-Yield-Investitionsprogramme investieren.

© Stephan Doleschal

HANDELS VERBAND | 100+1 JAHRE

GEMEINSAM
SICHER
IM HANDEL

Jetzt kostenlos anmelden!
www.sicherheitsgipfel.at

SICHERHEITS GIPFEL 2022

24. MAI

Bundeskriminalamt, Festsaal
Josef-Holaubek-Platz 1 | 1090 Wien

GEMEINSAM.SICHER im Online-Handel

Bundesministerium Inneres

Bundesministerium Landesverteidigung

PSA

ÖSTERREICH WIRD KRISENFIT!

METRO

CRIF