OKT 2018

Inkasso Wirtschaft

AUSGABE 27
DAS MAGAZIN DES BDIU

Bestellbetrug || Ganoven an der Packstation

IT-Sicherheit || Schwachstellen im Unternehmen aufspüren

Datenschutz || Ein Code of Conduct für die DSGVO

www.inkassowirtschaft.de

Sie managen Forderungen.

Forderungen einzuziehen war schon immer eine Aufgabe für Experten. Juristischer und kaufmännischer Sachverstand braucht heute unbedingt auch digitale Skills. Ob Datenschutz-Grundverordnung, elektronischer Rechtsverkehr oder die optimale Kommunikation mit Schuldnern per Brief, via E-Mail oder am Telefon – die Inkasso-akademie hält Sie up to date und macht Sie zu erfolgreichen Forderungsmanagern!

DIA – DEUTSCHE INKASSO AKADEMIE

www.inkassoakademie.de

Die Weiterbildungstochter des Bundesverbands Deutscher Inkasso-Unternehmen e. V. (BDIU)

LIEBE LESERINNEN,

LIEBE LESER,

der Onlinehandel in Deutschland eilt von Rekord zu Rekord, er ist einer der kräftigsten Wachstumstreiber für unsere Wirtschaft. Die Gründe dafür lassen sich wohl am besten bei jedem von uns selbst beobachten: Auch ich möchte es nicht mehr missen, auf dem Handy oder dem Laptop Produkte anschauen, vergleichen und bestellen zu können. Digitalisierung macht den Alltag schneller und leichter.

Leider hat diese schöne neue Einkaufswelt auch ihre Schattenseiten. Die Anonymität im Netz lockt Kriminelle an. Eine besonders perfide Masche ist der Identitätsklau mit anschließendem Bestellbetrug. Shopbetreiber bemerken das Täuschungsmanöver oft erst dann, wenn auf Rechnungen und Mahnungen keine Reaktion erfolgt. Und wenn Verbraucher, deren Adresse für den Betrug missbraucht wurde, dann auch noch Inkassobriefe erhalten, sind sie meist geschockt bis verärgert. Die traurige Wahrheit ist: Auch Inkassounternehmen sind Geschädigte der Bestellbetrüger.

Verbraucher, die verdächtige Rechnungen oder Mahnungen erhalten, sollten die Händler beziehungsweise Inkassounternehmen möglichst umgehend darüber informieren. Unsere Mitgliedsunternehmen nehmen solche Hinweise sehr ernst. Gemeinsam mit Shops, Auskunfteien und den polizeilichen Ermittlungsbehörden arbeiten wir daran, den Tätern ihr Handwerk wenn vielleicht nicht völlig zu legen, so es ihnen aber zumindest so schwer wie nur irgend möglich zu machen. Mehr dazu lesen Sie in dem Artikel ab der nächsten Seite.

Ein anderes wichtiges Thema, das uns auf längere Zeit beschäftigen wird, ist der Datenschutz. Die DSGVO ist noch in aller Munde. Aber gerade für den Bereich Forderungsmanagement gibt es bei der Auslegung der neuen Regeln weiterhin Unklarheiten. Glücklicherweise ändert sich das schon bald. Bereits seit zwei Jahren arbeiten wir gemeinsam mit unserem EU-Dachverband FENCA intensiv an einem Code of Conduct, der die recht weit gefassten Regeln der DSGVO für den Einzug von Forderungen konkretisiert. Für die Branche bringt das Rechtssicherheit. Ende Oktober in Straßburg will die FENCA den Code nun beschließen.

Auch dazu lesen Sie mehr in diesem Heft – bei dessen Lektüre ich Ihnen wie immer viel Vergnügen wünsche.

Ihre

Kirsten Pedd, *Präsidentin des BDIU*

IMPRESSUM

Herausgeber Bundesverband Deutscher Inkasso-Unternehmen e. V.
Friedrichstraße 50–55 || 10117 Berlin
Telefon +49 30.206 07 36-0
bdiu@inkasso.de || www.inkasso.de

Eingetragen im Vereinsregister Berlin,
Amtsgericht Charlottenburg, VR 28841 B
Chefredaktion Marco Weber
Redaktion Kay Uwe Berg, Dennis Stratmann, Marco Weber
Konzept + Gestaltung Nolte | Kommunikation
Bildnachweis Marco Weber (Cover, S. 2); BDIU/Peter Himsel (S. 1); SCHUFA Holding AG (S. 12–13); shutterstock.com: beeboys (Anzeige), Amy Walters (S. 5), William Potter (S. 7, 9), noppawan09 (S. 8), Rattana.R (S. 10), Montri Thipsorn (S. 10); fotolia.de: cmnaumann (S. 11)

Inhalt

BESTELLBETRUG

Ganoven an der Packstation

Axel Prahl badet oft im Blitzlichtgewitter. Als »Tatort«-Kommissar Frank Thiel begleiten ihn Millionen Deutsche bei der Verbrecherjagd. Doch über seine letzten Schlagzeilen dürfte er sich deutlich weniger gefreut haben. Denn diesmal wurde der Schauspieler selbst zum Opfer – von Kriminellen, die in seinem Namen im Internet auf Einkaufstour gingen.

Bestellbetrug grassiert im Netz wie ein Virus. Seitdem das bequeme Onlineshoppen von zu Hause aus boomt, entdecken auch Betrüger immer wieder neue Schlupflöcher für ihre unseriösen Machenschaften. Sie bereichern sich auf Kosten der Händler und bereiten den Menschen, deren Daten sie dazu benutzen, jede Menge Ärger.

Schauspieler, Journalisten, Politiker. Immer mal wieder geraten sie ins Visier der Kriminellen. Personen des öffentlichen Lebens gelten als stärker gefährdet, weil man ihre privaten Daten ganz leicht im Netz finden kann. Vor- und Familienname, aktuelle und alte Anschriften, Telefonnummern und auch das Geburtsdatum – mit nur wenigen Klicks ist das schnell recherchiert. So ausgestattet, ist es für die Schwindler nur noch eine Kleinigkeit, sich online als eine fremde Person auszugeben. Und versteckt hinter der virtuellen Maske jede Menge gefährlichen Unsinn anzustellen.

Axel Prahl fiel der Betrug erst auf, als plötzlich ungebetene Briefe bei ihm landeten. Rechnungen und Mahnungen über Dinge, die er nie im Leben geordert hatte.

Der TV-Ermittler informierte die Polizei, dort kannte man die Masche schon. Man muss aber nicht prominent sein, um Opfer von Bestellbetrug zu werden. Treffen kann es im Prinzip jeden.

PRIVATES AUF DEM PRÄSENTIERTELLER

2017 gab es in Berlin 15.616 solcher Fälle. Das sagt jedenfalls die Kriminalitätsstatistik aus, die die Polizeibehörden der Hauptstadt führen. Dabei entspricht diese Zahl nur den Fällen, die auch zur Anzeige gebracht werden. Die Dunkelziffer dürfte erheblich höher sein. »Bestellbetrug hat sich mittlerweile als Massendelikt etabliert«, berichtet Olaf Borries, Kriminalhauptkommissar beim Berliner Landeskriminalamt. Das Problem: Viele Verbraucher machen es den Betrügern verflixt einfach. Auf Facebook, Instagram und anderen Portalen wird das Private öffentlich und verliert mancher die Kontrolle über das, was er eigentlich über sich preisgeben möchte. Kommissar Borries mahnt: »Die persönlichen Daten gehören nicht auf den Präsentierteller. Wer online zurückhaltend agiert, macht sich für die Kriminellen uninteressant.«

Datensparsamkeit kann also vor Bestellbetrug schützen. Muss sie aber nicht. Denn für findige Betrüger gibt es noch eine ganze Reihe weiterer Möglichkeiten, die persönlichen Informationen über Menschen abzufangen und für ihre Zwecke zu kapern. Manche Datensammelei ist so frech und dreist, dass man es kaum fassen kann. Wer käme schon auf den Gedanken, freiwillig in anderer Leute Müll herumzuwühlen? Die Cybergauner machen das. Papiertonnen können ganz schön verräterisch sein. Rechnungen und Bankauszüge – sie enthüllen sensible Daten, die den Zugriff auf Shops und das Konto frei machen. Oder auch Werbebriefe, Kataloge und Kundenmailings, die sich im Hausflur aus Briefkästen herausangeln lassen. Meist finden sich hier neben ausführlichen Adressangaben auch Kundennummern und bequem ausfüllbare Bestellscheine. Für die Gauner sind solche Beutezüge ein wahres Fest.

MISSTRAUEN IST BESSER

Spam- und Phishing-Mails und unerwartete Anrufe: Jeder Verbraucher muss sich heutzutage mit einer gesunden Portion Misstrauen wappnen. »Wenn man eine Mail von einer unbekannten Person erhält, sollte man auf gar keinen Fall hier enthaltene Links anklicken. Besser ist es, man löscht solche Nachrichten sofort aus seinem Postfach«, sagt Stephan Neumann, Managing Consultant & Pentest Professional der usd AG. Er ist eine Art professioneller Hacker und berät Firmen bei der Optimierung ihrer IT-Sicherheit (*siehe Interview*).

E-Mails sind ein beliebtes Einfallstor. »Auch wenn man den Absender vermeintlich sehr gut kennt, sollte man immer noch vorsichtig sein«, rät Neumann. Gerade bei Firmen ist das sogenannte Spear Phishing inzwischen in allerschlimmster Mode. Die Betrüger fälschen dabei die Identität von Kollegen oder auch Chefs – und nötigen die Empfänger dazu, sensible Daten zu verraten oder teils beträchtliche Beträge zu überweisen, meist auf ausländische Konten. Schaut man nicht genau hin, ist man schnell um viel Geld ärmer.

> WER ONLINE MIT SEINEN DATEN ZURÜCKHALTEND IST, MACHT SICH **FÜR KRIMINELLE UNINTERESSANT**.

Natürlich ist auch am Telefon nicht jeder Anrufer derjenige, für den er sich ausgibt. Der freundliche Bankmitarbeiter, der nur mal schnell die Infos zum Konto abgleichen möchte, harmlose Meinungsumfragen, an deren Ende die persönlichen Daten notiert werden, oder auch Gewinnspiele, die mit tollen Preisen locken. Von der Aussicht auf lukrative Hauptgewinne sollte sich niemand die Urteilskraft vernebeln lassen.

Manche Datenklauer gehen auch immer noch den, sagen wir, »klassischen« Weg über Trickbetrügereien und einfache Diebstahlsdelikte. Gestohlene Handtaschen oder Geldbörsen sind wahre Datenschatzkästchen. Ausweise, Gesundheitskarten, Mitgliedsinfos – damit sind die Cybergauner bestens ausgestattet für Phase zwei ihrer Betrügerei.

AUF FALSCHER FÄHRTE

Nehmen wir mal an, der Kriminelle hat nun alle Daten, die er fürs Shoppen auf fremden Namen braucht. Jetzt sucht er sich einen Versender aus, den er um seine Ware »erleichtern« will. Dazu benutzt er den Namen, die Adresse und das Geburtsdatum der anderen Person – und bestellt. Der Händler muss nun die übermittelten Orderdetails überprüfen, bevor er die Ware verschickt. Denn er will ja auf Nummer sicher gehen, dass er sein Geld auch bekommt. Regulär arbeiten die Versender dafür mit spezialisierten Dienstleistern zusammen, zum Beispiel Auskunfteien. Meldet sich ein neuer Kunde im Shop an und gibt eine Bestellung auf, fragt der Händler bei der Auskunftei nach, ob es tatsächlich eine Person mit den dabei verwendeten Daten gibt, also: Passen Name, Anschrift und Geburtsdatum zueinander? Quatschbestellungen wie die von »Donald Duck« aus dem »Blumenweg« in »Entenhausen« werden sofort herausgefiltert.

Aber es ist ja nicht Donald Duck, der da eine Bestellung aufgibt – der Schwindler täuscht die Identität einer tatsächlich existierenden Person vor. Wieso fällt der Betrug nicht auf? Mehrere Szenarien sind in dieser Phase des Bestellprozesses üblich und stellen die Weichen für das weitere Vorgehen. Was ist zum Beispiel, wenn überhaupt keine Informationen über die Person vorliegen?

3 typische Paketfänger

Hat der Gauner die Identität eines Verbrauchers geklaut und geht damit auf Einkaufstour, gibt es drei häufige Vorgehensweisen:

1. DER **GATE-CRASHER**

Der Gate-Crasher lässt sich die Ware direkt an die Haustür des Betrugsopfers liefern. Den Postboten passt er noch an der Haustür ab. Das geht ziemlich leicht beispielsweise in Mehrfamilienhäusern, wenn sich der Betrüger direkt an der Hauseingangstür postiert. Über die Sendungsverfolgung, die viele Shops inzwischen standardmäßig anbieten, weiß er auch ziemlich genau, zu welcher Uhrzeit er mit der Lieferung zu rechnen hat. In diesem Fall sind Liefer- und Rechnungsanschrift identisch.

2. DER **KUCKUCKSKUNDE**

Hier passiert dasselbe Spiel wie oben: Der Betrüger kauft auf Namen eines anderen und lässt sich die Ware an die Adresse des Betrugsopfers liefern. Der Unterschied hier: Das Opfer wohnt gar nicht mehr an der Adresse. Entweder ist es vor Kurzem umgezogen, befindet sich im Urlaub oder – auch das kommt vor – die Adresse eines jüngst Verstorbenen wird missbraucht. An der Haustür nimmt der Betrüger die Ware an und verschwindet wieder. Auch in diesem Fall sind Rechnungs- und Lieferanschrift identisch.

3. DER **CAMPER**

In diesem Fall kommt die Ware weder bei dem Besteller noch bei dem Betrüger selbst an. Der Camper lässt sie sich vielmehr an eine völlig fremde Adresse liefern. Beliebt sind leer stehende Wohnungen oder Häuser. Dort gibt er sich als der Besteller der Ware aus, nimmt sie in Empfang – und zieht danach weiter. Liefer- und Rechnungsanschrift sind also hier nicht identisch.

Der Camper ist übrigens ziemlich gewitzt. Sehr oft unterbinden Shops die Möglichkeit, dass sich ein neuer Kunde schon bei der ersten Bestellung die Ware an eine andere Adresse liefern lässt. Wie reagiert der Camper auf diese Sicherungsmaßnahme? Er bestellt erst mal »regulär« ein paar günstige Artikel an die dabei angegebene Rechnungsadresse. Dann verändert er sein Verhalten, bestellt teure Ware – und lässt sie sich an eine andere Anschrift liefern.

Dann lautet die Empfehlung an den Shop in der Regel: »Geh nicht in Vorleistung.« Der Kauf auf Rechnung für einen solchen neuen Kunden wäre nicht möglich. Ein Betrüger hat in einem solchen Fall also keine Chance, der Kriminelle wäre gestoppt.

MIT NETZ UND DOPPELTEM BODEN

Es kann aber auch sein, dass die Auskunftei sogenannte Negativinformationen über die entsprechende Person vorliegen hat. Das würde bedeuten, dass der Käufer wahrscheinlich nicht zahlungskräftig genug ist, der Versender also ein relativ hohes Risiko eingehen würde, indem er die Ware in Vorleistung verschickt. In besonders krassen Fällen hat es über die angegebene Adresse in der Vergangenheit bereits einen oder mehrere Betrugsversuche gegeben. Auch das registrieren Auskunfteien und heben dann umgehend ein Stoppschild: »Kein Rechnungskauf möglich!«

Der Normalfall ist aber dieser: Die personenbezogenen Daten über den Kunden sind der Auskunftei geläufig, das heißt beispielsweise, Name und Adresse stimmen mit den bei der Bestellung gemachten Angaben überein – und dem Dienstleister sind auch keine Informationen bekannt, die auf eine schlechte Zahlungsmoral hindeuten würden. Dann gibt es grünes Licht: Der Kunde kann die Ware auf Rechnung kaufen.

Ist die Ware erst mal unterwegs, wird der Kriminelle sich daranmachen, die Sendung irgendwie abzufangen. Auf dem Handy kann er bequem verfolgen, wie die Ware den Shop verlässt, wann sie in welchem Verteilerzentrum landet, auf den Lkw verladen wird – und um welche Uhrzeit er in etwa mit der Zustellung rechnen kann. Er nutzt jetzt verschiedene Tricks *(siehe Kasten)*, die alle eines gemeinsam haben: Derjenige, dessen Identität für die Bestellung missbraucht wird, bekommt nichts davon mit. »Viele Täter nutzen eigens für den Betrug generierte E-Mail-Adressen«, erklärt Kriminalist Borries. »Die komplette Kommunikation mit dem Händler läuft darüber ab. Auch die Rechnung wird an diesen Mail-Account geschickt. Der geschädigte Verbraucher, dessen Identität für diesen Vorgang missbraucht wird, bleibt erst mal völlig ahnungslos. Er kann in dieser ›heißen‹ Phase gar nicht bemerken, dass in seinem Namen betrügerische Aktivitäten stattfinden.«

DIE POST, DIE KEINER WILL

Dem Hamburger Blogger Marcel B. (der richtige Name ist der Redaktion bekannt) ist genau das passiert. In seinem Fall hatte eine fremde Person einen Rucksack bei einem bekannten Sportartikelhändler bestellt. Als auf einmal eine Mahnung in der Post lag, ignorierte B. das Schreiben. »Ich dachte, es handelte sich einfach um ein Versehen.«

Besser wäre es gewesen, er hätte den Shop schon nach dieser Mahnung umgehend auf den Fehler hingewiesen. So ging der Händler davon aus, dass er es einfach nur mit einem zahlungsunwilligen Kunden zu tun hatte. Kunden,

Phase 1 || Der Täter sammelt Daten

aus denen Schuldner werden – jeder Unternehmer kennt das und hat als Mittel gegen solche Risiken einen Mix aus internem Mahnwesen und externer Rechtsdurchsetzung installiert. Im Fall von Marcel B. übergab der Händler die Sache ins Forderungsmanagement, also an einen Inkassodienstleister.

Das Inkassounternehmen erhält nun eine Reihe von Daten übermittelt, die es für die Rechtsdurchsetzung der Forderung benötigt. Dazu gehören etwa der Name und die Anschrift des Schuldners sowie die näheren Umstände zur Forderung – also worum es bei dem zugrunde liegenden Vertrag geht und wann die Forderung entstanden ist. Das Inkassounternehmen prüft jetzt diese Informationen. Das ist wichtig, denn diese Maßnahme bildet die Grundlage für die weiteren Inkassoschritte, mit deren Durchführung der Gläubiger den Rechtsdienstleister beauftragt hat.

Eine wichtige Frage lautet: Stimmt die Adresse überhaupt? Dazu kann das Inkassounternehmen eine Anfrage beim Einwohnermeldeamt stellen.

KONTROLLE IST TEUER

Die Firma braucht dafür aber auch einen guten Grund. »Die Behörden lassen sich diese Anfragen teuer bezahlen«, erklärt Kay Berg vom Bundesverband Deutscher Inkasso-Unternehmen (BDIU). »Und die Kosten dafür muss am Ende der Schuldner tragen, denn das gehört zu dem Verzugsschaden, den er durch das Nichtzahlen der Rechnung verursacht hat. Es gibt hier aber keinen Automatismus. Das Inkassounternehmen ist nämlich auch dazu angehalten, die Kosten für den säumigen Verbraucher so niedrig wie möglich zu halten. Also wird es nur dann eine Verifikation der Adresse vornehmen lassen, wenn es irgendwelche Anhaltspunkte dafür hat, dass mit der Anschrift etwas nicht in Ordnung ist.« Bei Marcel B. gab es dazu keinen Grund. Die Adresse war korrekt, er war nicht umgezogen, die Briefe konnten problemlos zugestellt werden – die Kosten für eine weitere Prüfung waren also nicht erforderlich.

Die Behörden stehen hier allerdings in der Kritik. Eine verlässliche und sichere Prüfung von Adressdaten kann es nur geben, wenn auch die Datenqualität entsprechend hoch ist. Und an diesem Punkt hapert es. »Bei den Meldeamtsanfragen erhalten Inkassounternehmen sehr häufig sogenannte Leermeldungen, also einen leeren Datensatz mit überhaupt keinen Informationen zu der abgefragten Person«, sagt Kay Berg. Auch veraltete Anschriften und das Übermitteln schlichtweg falscher Adressdaten sind keine Seltenheit. Am problematischsten gestaltet sich dabei die Abfrage über Onlineschnittstellen. Bei solchen elektronischen Aus-

An Sicherheit darf man nicht sparen

Kriminalhauptkommissar Olaf Borries vom Berliner Landeskriminalamt über Betrüger aus dem Netz und wie sich Firmen vor virtuellen Attacken schützen können.

Wie oft wenden sich Unternehmen an Sie, weil ihnen über das Netz Schaden zugefügt wurde?

OLAF BORRIES II Wir haben bei der Berliner Polizei eine Zentrale Ansprechstelle Cybercrime, kurz ZAC, eingerichtet. 2017 hatten wir 966 Kontaktaufnahmen, im ersten Halbjahr 2018 sind es schon über 600.

ZACs sind miteinander vernetzte polizeiliche Kontaktstellen des Bundes und der Länder, die speziell für Unternehmen sowie öffentliche und nicht öffentliche Institutionen eingerichtet worden sind, um als kompetenter Ansprechpartner IT-Sicherheitsvorfälle aus diesen Bereichen entgegenzunehmen und zeitnah Erstmaßnahmen mit anschließender Zuweisung an die zuständigen Ermittlungsstellen zu veranlassen. Darüber hinaus werden sie bei der Klärung von IT-Sicherheitsfragen beratend und präventiv tätig.

ZACs initiieren, koordinieren und beteiligen sich an vielfältigen Cybercrime-Kooperationen mit anderen Sicherheitsbehörden, Institutionen der Wirtschaft und des Finanzwesens, der IT-Branche, der Wissenschaft und Forschung auf Bund-, Länder- sowie internationaler Ebene.

Was sind die typischen Betrugsszenarien?

Am häufigsten melden uns Firmen den sogenannten Chefbetrug (»CEO Fraud«). Die Täter sammeln zunächst alle verfügbaren Informationen über das anzugreifende Unternehmen, zum Beispiel über deren Website, Geschäftsberichte, Handelsregister, aber auch in sozialen Medien. Gegenüber einem Verfügungsberechtigten der Firma geben sie sich dann als Chef aus und veranlassen diesen Mitarbeiter zum Transfer eines größeren Geldbetrages ins Ausland. Die Schadenssummen gehen je nach Unternehmen bis in die Millionen Euro. Dagegen helfen einerseits Datensparsamkeit, andererseits aufmerksame Mitarbeiter und entsprechende Prozesse. Empfehlenswert ist ein Vieraugenprinzip, bevor man einen Betrag anweist, oder ein Whitelisting von Zahlungszielen bei Überweisungen.

Erpressungen sind ein weiteres Problem. Hier gibt es zwei wesentliche Bereiche. Zum einen gelangen Täter an Daten und erpressen das Unternehmen mit deren Veröffentlichung. Die andere Variante ist Schadsoftware, die alle erreichbaren Daten in einem IT-System verschlüsselt. Darunter fallen sämtliche Office-Dokumenttypen sowie Bilder und Videos auf allen logisch erreichbaren Geräten einschließlich Cloud-Speicher.

Wie können sich Firmen schützen?

Unsere Erfahrung ist, dass es den Tätern oft viel zu einfach gemacht wird. Veraltete Programme sind so ein Problem. In einem Fall hatte das Unternehmen eine sieben Jahre alte Shop-Software ohne jegliche Updates betrieben. Wenn Firmen über das Internet erreichbare ungesicherte Datenbanken oder Steuerungsgeräte betreiben, dann müssen sie sich nicht wundern, wenn diese jemand entdeckt und sich Zugriff darauf verschafft, Daten herunterlädt oder Anlagen sabotiert. Im Netz sind die unterschiedlichsten Tätergruppen rund um die Uhr unterwegs und suchen permanent nach Schwachstellen. Wenn Lücken gefunden werden, dann werden diese auch zu Geld gemacht, oder es wird zumindest versucht.

Um Schadsoftware abzuwehren, sollte ich meine Mitarbeiter regelmäßig schulen. Das Öffnen von Dateianhängen bei E-Mails zum Beispiel ist hochriskant. Außerdem sollte jedes Unternehmen ein passendes Back-up-Konzept für seine Daten benutzen. Ganz wichtig: Die Rücksicherung aus einem Back-up sollte auch getestet werden, und zwar noch bevor es wegen eines Datencrashs oder einer Cyberattacke unausweichlich ist.

Generell ist zu raten, dass Firmen etwa ein Zehntel ihres IT-Budgets ausschließlich für die IT-Sicherheit verwenden.

Wie merkt ein Verbraucher, dass er Opfer von Identitätsklau und Bestellbetrug geworden ist?

Oftmals stellt der Betroffene unautorisierte Kontoabbuchungen fest, mit denen Warenbestellungen beglichen wurden, die von ihm gar nicht getätigt wurden. Manchmal wird der Betroffene auch erst durch an ihn adressierte Mahn- beziehungsweise Inkassoschreiben auf die Betrugstat aufmerksam.

Ebenso kommt es vor, dass Täter betrügerische Warenlieferungen an die tatsächliche Wohnanschrift des Betroffenen auslösen, in der Hoffnung, der Adressat ist bei Lieferung nicht zu Hause. Sie versuchen dann, die Warensendung bei einem Ersatzempfänger (in der Regel ein gutgläubiger Nachbar) unter Vortäuschen einer Legende in Empfang zu nehmen. Geht dieses Kalkül nicht auf und der Betroffene ist bei Lieferung doch zu Hause, wundert er sich natürlich über den Erhalt einer von ihm nicht bestellten Ware. Verfolgt er die Angelegenheit zurück, meist durch Nachfrage bei dem Warenversender, stellt sich in der Regel heraus, dass zu seinen Lasten ein (versuchter) Bestellbetrug eingefädelt worden ist.

Wie hilft die Polizei, Bestellbetrug aufzuklären? Wie unterstützt sie die geschädigten Verbraucher?

Die Mitarbeiterinnen und Mitarbeiter der Fachdezernate der Betrugsabteilung im Landeskriminalamt Berlin (LKA 2) sind umfangreich sowohl präventiv als auch repressiv tätig. Sie gehen auch in die Öffentlichkeit, geben in Radio, TV und im Netz Präventionshinweise und machen auf Informationsquellen aufmerksam – zum Beispiel im Netz, was die Annahme von Paketen an der Haustür angeht: **https://www.berlin.de/polizei/aufgaben/praevention/betrug/artikel.112402.php**.

Unternehmen werden beraten, ihre Bestellannahme- und Versandabläufe derart zu optimieren, dass betrugsverdächtige Bestellungen möglichst zuverlässig und rechtzeitig erkannt und betreffende Warenauslieferungen zurückgehalten werden. In Anbetracht der Ausprägung des Bestellbetruges mittlerweile als Massendelikt bei gleichzeitig limitierten Personalressourcen ist die jeweilige Ermittlungstiefe im Einzelfall zwangsläufig an der Qualität der Taten und den Erfolgsaussichten auf Täterermittlung auszurichten. Taten ohne erkennbare »Anpacker« müssen folglich aufwandsarm bearbeitet werden. Für intensiv beziehungsweise schadensträchtig handelnde Täter konnten allerdings nach aufwendiger Ermittlungsarbeit im Zusammenwirken mit der Justiz auch schon mehrjährige Freiheitsstrafen erzielt werden.

Phase 2 || Vertragsschluss: Der Täter kauft im Onlineshop unter falschem Namen

künften kann schon ein simpler Buchstabendreher oder die Schreibweise »Str.« statt »Straße« zu einer Fehler- oder Leermeldung führen. »Das erschwert es den Inkassodienstleistern ganz erheblich, Fälle von Identitätsmissbräuchen zu identifizieren«, klagt Berg. Die Meldedaten müssen also besser werden, was ja letztlich auch im Interesse der betroffenen Bürgerinnen und Bürger ist. Berg schlägt dazu vor, dass sich die einzelnen Meldeämter besser untereinander vernetzen. Fehlerhafte oder unterschiedliche Informationen zu einzelnen Personen ließen sich so identifizieren und miteinander abgleichen. Ein Vorbild dafür hat Berg auch vor Augen: die Finanzbehörden. Für diese ist ein solcher Datenabgleich üblich. Warum also nicht auch für die Einwohnermeldeämter?

LANGSAME GANGART MIT FÜNF BUCHSTABEN

Bei dieser Gelegenheit könnten die Ämter auch an der Geschwindigkeit für das Übermitteln der Daten drehen. Beim Onlinehandel erwarten die Käufer ja auch, dass sie Waren in kürzester Zeit mit wenigen Klicks bestellen können. Da wirkt es wie ein Anachronismus, wenn einzelne Meldeämter selbst im Jahr 2018 noch bei Anfragen auf die Schriftform bestehen. Schneckenpost statt Datenautobahn. Um Identitätsklau im E-Commerce besser aufspüren und auch verhindern zu können, wären

Phase 3 || Der Händler prüft die Daten und findet keinen Fehler

also bessere Daten- und einheitliche Übermittlungsstandards der Meldeämter ein echter Schritt nach vorne.

Zurück zu unserem Beispielfall. Dummerweise sieht die Bestellung selbst zu diesem Zeitpunkt noch wie ein ganz normaler Kaufvorgang mit Mahnstufe aus. Aber es gibt jemanden, der den Betrug jetzt aufdecken könnte, und das ist der geschädigte Verbraucher. Marcel B. hätte das Inkassounternehmen jetzt informieren sollen. »Ich kann verstehen, dass das lästig ist, zumal er selbst ja den ganzen Vorgang überhaupt nicht ausgelöst hat«, sagt Berg. »Aber der Ärger, den man mit solchen Betrügereien hat, wird nur noch größer, je länger man mit einer Beschwerde wartet.« Erhält das Inkassounternehmen eine solche Reklamation, wird es den Vorgang aus den normalen Bearbeitungsroutinen herausnehmen – und erneut prüfen. In der Regel wird es dazu Rücksprache mit dem Auftraggeber halten, also in diesem Fall dem Onlinehändler. Spätestens jetzt fliegt der Betrug auf.

MITHILFE IST PFLICHT

Aber reicht das? Es handelt sich doch hier um eine Straftat, und die muss aufgeklärt werden. »Opfer eines versuchten oder vollendeten Bestellbetruges sollten unbedingt bei der Polizei Strafanzeige erstatten«, erklärt Kriminalhauptkommissar Borries. Mit einer Anzeige könnten Betroffene ihre Interessen am besten wahren. Ganz wichtig: Sie sollten alle relevanten Unterlagen aufbewahren beziehungsweise sichern. Es wäre ein fataler Fehler, Rechnungen oder Mahnbriefe aus einem Betrugsdelikt in den Müll zu werfen. Sie sind Beweismittel, die helfen können, den Kriminellen dingfest zu machen. Geschädigte handeln damit im eigenen Interesse. »Häufig besteht der Irrglaube, dass ab dem Zeitpunkt der Anzeigenerstattung alle weiteren Veranlassungen von der Polizei getroffen werden«, weiß Borries aus leidlicher Erfahrung. Richtig ist: »Es bleibt in der Verantwortung des Betroffenen, zum Beispiel sein kontoführendes Kreditinstitut über unrechtmäßige Abbuchungen zu informieren, falls noch möglich eine Rückbuchung zu veranlassen und weitere Folgemaßnahmen zu treffen.« Sicher ist sicher. Und auch die Inkassounternehmen sollte der Geschädigte unbedingt informieren. »Unsere Erfahrungen zeigen, dass der Verweis auf eine bereits erstattete Strafanzeige für den Betroffenen oftmals hilfreich ist.«

Angesichts der Probleme mit Bestellbetrug liebäugeln manche mit radikalen Schritten. Dreh- und Angelpunkt ist dabei der Warenversand ohne vorheriges Bezahlen. »Ich frage mich, warum Bestellen auf Rechnung überhaupt möglich ist«, sagt Claude Kohnen. Er ist Mitarbeiter des Europa-Abgeordneten Prof. Dr. Klaus Buchner (ÖDP), der wiederholt Opfer der Betrüger geworden ist. In seinem Berliner Abgeordnetenbüro kamen mehrfach Mahnschreiben von Inkassounternehmen an. Rechnungen hatte der Abgeordnete zuvor nicht erhalten. »Er hat auch definitiv keine der behaupteten Sachen bestellt.« Die Inkassounternehmen wurden informiert – danach hörte der Spuk auf. »An die Polizei haben wir uns nicht gewandt, denn das erschien uns sinnlos. Ich bin verwundert, dass ein solcher Betrug so einfach möglich ist«, kritisiert Kohnen.

DER KUNDE IST KÖNIG

Also einfach den Rechnungskauf untersagen, am besten per Gesetz, und schon ist das Problem mit dem Bestellbetrug gelöst? Einfache Lösungen sind oft schlechte Lösungen. Schon seit Jahrzehnten gehört der Rechnungskauf zur DNA der deutschen Verbraucher. Kleidung per Katalog ordern und zu Hause erst begutachten, bevor man sie bezahlt – daran hat man sich hierzulande seit Wirtschaftswunderzeiten gewöhnt. Heute ist der Versandhauskatalog ins Netz gewandert, bestellt wird nicht mehr per Postkarte, sondern per Mausklick – aber ansonsten hat sich an dem Prozedere nicht viel geändert.

E-Commerce und damit auch der Rechnungskauf sind in Deutschland ein Topwirtschaftsfaktor. Immer noch wächst der Onlinehandel rasant. Aktuelle Prognosen erwarten in diesem Jahr ein Umsatzplus von 10 Prozent auf dann fast 64 Milliarden Euro. Rund ein Drittel aller Käufer präferiert dabei die Option »Kauf auf Rechnung«.

Der Profi-Hacker

Digitale Einfallstore für Betrüger zu finden und zu schließen – das ist eine Aufgabe von Stephan Neumann, Managing Consultant & Pentest Professional der usd AG.

Phase 4 || Die Ware wird verpackt und verschickt

Herr Neumann, was macht ein Pentester?

STEPHAN NEUMANN II Im Prinzip handelt es sich dabei um einen guten Hacker. Ein Penetrationstester sucht und dokumentiert Schwachstellen in der IT-Infrastruktur eines Unternehmens. Überall können sich Einfallstore für Hacker verbergen, zum Beispiel bei Apps oder einem offenen Kunden-WLAN. Als Pentester spüre ich die auf und empfehle dem Unternehmen praktische Maßnahmen, um diese Schwachstellen zu beheben. Ein guter Pentester ist immer auch ein guter Berater.

Was sind die typischen Einfallstore für Hacker in Unternehmensnetzwerke?

Eigentlich gibt es dafür unendlich viele, man sollte aber zwei Wege unterscheiden. Zum einen den technischen Angriff, der über eine alte Version eines Betriebssystems oder einen Webserver erfolgt. Das ist für die Firma eine existenziell gefährliche Schwachstelle, denn der Angreifer kann unter Umständen das komplette IT-System darüber übernehmen. Komplexe Schwachstellen ermöglichen es so zum Beispiel auch, Kundendaten und Passwörter auszulesen. Genau solche Punkte adressiert ein Pentest. Manchmal sind auch ganz normale Anwendungen fehlerhaft programmiert, weil die Entwickler an bestimmte Möglichkeiten einfach nicht gedacht haben. Ein einfaches Beispiel wäre, wenn man in einem Webshop nicht 1 Smartphone kauft, sondern –1 Smartphone in den Warenkorb legt. So zahlen Sie nicht 600 Euro, sondern –600 Euro. Solche Schwachstellen decken wir auf und bewahren Firmen dadurch vor finanziellem oder auch einem Imageschaden.

Ich brauche als Unternehmen aber auch aufgeklärte Mitarbeiter. Die menschliche Neugier ist so ziemlich das gefährlichste Einfallstor für allerlei Angreifer von außen. Fast jeder hat schon mal dubiose E-Mails bekommen, die so interessant formuliert sind, dass man eigentlich mehr darüber wissen möchte. Die sollte man aber besser löschen, anstatt auf Links zu klicken oder gar mitgeschickte Anlagen zu öffnen. Fast jeder hat sicherlich schon mal einen USB-Stick geschenkt bekommen oder bei einer Messe oder Veranstaltung liegen sehen. Auch wenn es vielleicht noch so sehr reizt, da etwas Genaueres herauszubekommen: Man sollte den Stick auf keinen Fall in den PC stecken. Es sind viele Fälle bekannt, in denen sich Unternehmen darüber Ransomware eingefangen haben – also Erpresserviren, die die Festplatten im System verschlüsseln.

Sie machen Awareness-Schulungen – schärfen also das Bewusstsein für mehr IT-Sicherheit. Warum ist das überhaupt nötig, und was können Mitarbeiter tun, um Angriffe auf ihr Unternehmen zu verhindern?

Die beste Technik nützt nichts, wenn man bei deren Anwendung Fehler macht. Jeder kennt das Gefühl, wenn sich der gesunde Menschenverstand meldet, der einen warnt, dass hier gerade etwas nicht stimmt. Wer schon mal eine Awareness-Schulung mitgemacht hat, der hat live gesehen, wie ein Angreifer typischerweise vorgeht.

Viel zu viele Firmen und deren Mitarbeiter denken: »Warum sollten die mich angreifen?« Die Wahrheit ist: Hacker sind sehr kreativ, wie sie mit ihrer »Arbeit« Profit machen können. Wenn man im Unternehmen das Thema nicht ernst nimmt, dann bietet man für Angreifer erst recht ein einfaches Ziel. Jeder Mitarbeiter sollte sich immer fragen, wenn er per Mail von einem Kollegen, einem Chef oder einem Kunden zu einer bestimmten Aktion aufgefordert wird, ob diese Mail echt ist. Macht es wirklich Sinn, diese 20.000 Euro ohne weitere Rücksprache zu überweisen? Braucht der IT-Mitarbeiter gerade wirklich mein Passwort?

Alleine mit dem Wissen über sie lassen sich Schwachstellen für viele typische Angriffe bereits stopfen. Im Übrigen wirken Investitionen in mehr IT-Sicherheit auf jeden Fall abschreckend, denn auch die Angreifer machen eine Kosten-Nutzen-Analyse: Wenn der Aufwand für einen Angriff zu hoch ist, suchen sie sich ein einfacheres, lukrativeres Opfer.

Vielen Dank für das Gespräch.

Phase 5 || Der Täter nimmt die Ware entgegen

Phase 6 || Der Händler wartet auf sein Geld und mahnt

DER KAUF AUF RECHNUNG GEHÖRT ZUR **DNA DER DEUTSCHEN VERBRAUCHER**.

Würde man diesen Bezahlweg gesetzlich unterbinden, dann behinderte das den Fluss von mehreren Milliarden Euro an Wirtschaftskraft. Wäre es das wert? Und für welchen guten Zweck eigentlich? Absolute Sicherheit ist ein Trugbild. Auch andere Bezahlarten sind risikobehaftet und lassen sich missbrauchen, etwa das Zahlen mit Kreditkarte. Von den sozialen Aspekten einmal völlig abgesehen: Den Rechnungskauf kann jeder Verbraucher in Deutschland, unabhängig vom Einkommen und unabhängig vom Alter bequem durchführen – auch wer keine Kreditkarte hat beziehungsweise haben will oder digitale Bezahlwege aus den verschiedensten Gründen für sich ablehnt. Fragt man die Verbraucher, wären viele regelrecht empört, wenn man ihnen diese bequeme Bestellmöglichkeit nähme. Sie erhalten eine Ware sozusagen im Voraus. Und können beim Auspacken des Pakets prüfen, ob die Angaben des Händlers korrekt waren. Der Kunde entscheidet, ob er das Produkt behalten oder wieder zurückschicken will. Ein finanzielles Risiko geht beim Rechnungskauf eigentlich nur der Händler ein. Er tritt in Vorleistung, obwohl er weiß, dass es dabei auch zum Verlust von Forderungen kommen kann oder Zahlungen nur sehr schleppend bei ihm eingehen.

DIE TÄTER ENTTARNEN

Mehr Sicherheit könnte dagegen ein zentrales Betrugsregister bringen. Eine solche Liste enthält Adressen, die schon mal bei Betrugsversuchen auffällig geworden sind. Händler, Inkassounternehmen, Auskunfteien übermitteln die entsprechenden Infos – Auskunfteien wiederum haben die Möglichkeit, bei ihren Anfragen einen schnellen Gegencheck vorzunehmen. Kritische Adressen oder Datenkonstellationen, zum Beispiel ein bestimmter Name in Verbindung mit einer Adresse oder einem Datum, könnten bei einem Bestellprozess herausgefiltert werden. Bei einer auffälligen Adresse müsste der Kunde dann weitere Nachweise über seine Identität liefern, um einen Rechnungskauf auslösen zu können. Für die Wirtschaft und Verbraucher wäre das

ein guter Schutzmechanismus – denn die Erfahrung zeigt, dass die Betrüger häufig dieselben Adressen in verschiedenen Shops nutzen. »Derartige Datenbanken werden von Auskunfteien bereits angeboten«, sagt BDIU-Hauptgeschäftsführer Berg. »Das sollte weiter ausgebaut und gefördert werden. Mit diesen Maßnahmen schafft der Handel Vertrauen und es ist auch ein echter Fortschritt in der Kriminalitätsbekämpfung und -prävention.«

Eine weitere Stellschraube für mehr Sicherheit findet sich an dem Punkt, wo der Betrüger die Ware in Empfang nimmt, er also selbst aktiv werden muss. Kritisch sind Post- oder Packstationen. »Die Kontrollen sind hier oft viel zu lax«, kritisiert Berg. Mancher Kioskbesitzer guckt halt nicht so genau hin, wenn ihm eine Abholkarte präsentiert wird. Für Betrüger ist das ein leichtes Spiel. »Es wäre sinnvoll, hier durch entsprechende Kommunikation die Betreiber noch besser zu sensibilisieren. Die wenige Zeit, den Ausweis des Abholers zu prüfen, sollte sich wirklich jeder nehmen.« Auch bei Paket- und Abholstationen gibt es Schwachstellen, die sich noch abdichten ließen. Höhere Hürden bei der Registrierung machen den Nutzer genauer identifizierbar. Gauner schreckt das ab.

Phase 7 || Der Verbraucher, dessen Identität geklaut wurde, informiert Händler und/oder Inkassounternehmen und stellt Anzeige bei der Polizei

Mit diesen Maßnahmen würde man auch den Ermittlungsbehörden ihre Arbeit erleichtern. Immer wieder landen Betrüger vor Gericht. Im August zum Beispiel wurde in Waiblingen ein 34-jähriger Mann verurteilt. Er hatte auf falschen Namen bei Versandhändlern eingekauft und die Waren an Paketshops in seiner Umgebung liefern lassen. Dort tauchte er mit einem fremden Personalausweis auf und legte jeweils eine schriftliche Vollmacht vor. Die besagte, dass der Ausweisbesitzer die Waren in Vertretung des eigentlichen Kunden in Empfang nehmen dürfe. Insgesamt 13-mal zog er diese Masche durch, bis er damit aufflog. Die Kunden, auf deren Namen er shoppen ging, erhielten Mahnschreiben und beschwerten sich bei den Versandhändlern. Auch die Mitarbeiter der Paketshops, in denen der Mann die ergaunerten Sendungen in Empfang nahm, wurden misstrauisch. In einer Wäscherei, die als Annahme- und Abholstelle eines Paketzustelldienstes fungiert, gelang der Polizei schließlich der Zugriff.

DIE AUGEN OFFEN HALTEN

Insgesamt hatte der Mann Waren im Wert von mehreren Tausend Euro ergaunert – am Ende kassierte er dafür eine Freiheitsstrafe von eineinhalb Jahren. Die Hinweise der Opfer und aufmerksame Paketshop-Mitarbeiter haben diesen Bestellbetrug entlarvt und dazu beigetragen, dass der Täter gefasst und rechtskräftig verurteilt werden konnte. Computerbetrug und Urkundenfälschung lautete das Urteil. Müsste der Gesetzgeber hier härter durchgreifen, zum Beispiel mit einem schärferen Strafrecht? Möglicherweise. »Bis jetzt fällt das alles in der Regel unter Betrug«, sagt Kay Berg. »Dabei gibt es doch sehr starke Hinweise, dass wir es hier mit einer neuen Form von Kriminalität zu tun haben. Ein eigener Straftatbestand Identitätsdiebstahl könnte abschreckende Wirkung haben.«

Es ist wohl wie so oft im Leben: Das Problem ist komplex, will man es in den Griff kriegen, müssen alle Beteiligten mitmachen. Wenn Gesetzgeber, Unternehmen, Dienstleister und Verbraucher an einem Strang ziehen, lässt sich viel erreichen. Wer Opfer der Betrüger geworden ist, kann sich wehren – indem er die Polizei informiert und die Händler und deren Inkassodienstleister darüber in Kenntnis setzt. Als Betroffener ist man den gröbsten Ärger dann schon los.

»Tatort«-Star Axel Prahl, bei dem ein Gauner schon seit zwei Jahren immer mal wieder eine alte Adresse für Bestellungen nutzt, reagiert auf neue Rechnungen inzwischen ganz cool. »Mittlerweile ist es schon Routine, dann bei der Polizei die Vorgangsnummer für den Betrug durchzugeben.« So hilft der TV-Ermittler den echten Beamten bei deren realen Ermittlungen. Wünschen wir ihnen viel Erfolg.

Datenschutz braucht Klarheit

Die Ängste waren riesig: Abmahnwellen, die durchs Netz rasen, drakonische Sanktionen von bis zu 20 Millionen Euro: Die DSGVO hat für jede Menge Unsicherheit gesorgt. Seit Ende Mai muss sie nun angewendet werden, und vieles ist klarer geworden. Wirklich?

Die ersten Erfahrungen sind überraschend positiv. Die Umsetzung der neuen EU-Datenschutzregeln scheint in der deutschen Wirtschaft weitestgehend störungsfrei gelungen. Auch die Inkassounternehmen haben die Aufgabe bestens bewältigt. Trotzdem: Die Unsicherheiten sind noch lange nicht beseitigt. Das fängt bei Kleinigkeiten im alltäglichen Business an: Muss ich denjenigen, der mir eine Visitenkarte überreicht, DSGVO-konform darüber aufklären, wenn ich seine personenbezogenen Daten in meine elektronische Adresskartei übertrage? Und an wen können sich Unternehmen bei Detailfragen zum neuen Datenschutzrecht wenden?

Die Aufsichtsbehörden in den Bundesländern berichten über einen massiven Anstieg an Anfragen. Alleine in den ersten beiden Monaten nach Anwendungsbeginn der DSGVO wandten sich bis zu zehn Mal mehr Verbraucher an die Behörden mit Hinweisen auf mögliche Datenschutzverstöße. Für die Datenschützer selbst ist das kaum zu bewältigen.

Auch bei Inkassounternehmen fragen seit Ende Mai vermehrt Verbraucher zu datenschutzrechtlichen Fragen an. Hilfe gibt der Branche ein Best Practice Guide zur Anwendung der DSGVO im Forderungsmanagement. Den hat der BDIU bereits Anfang 2017 erstellt und veröffentlicht – also weit vor Anwendungsbeginn der DSGVO. Dieser Best Practice Guide wird schon bald ein Update erhalten. Die Datenschutzexperten der Inkassobranche arbeiten mit Hochdruck an einer erneuerten Fassung, die die bisher gemachten Erfahrungen mit dem neuen Datenschutzrecht berücksichtigt. Mit einer Veröffentlichung ist Anfang 2019 zu rechnen.

Beim Schufa-Branchentreff Anfang September in Bonn war die DSGVO eines der wichtigsten Themen. BDIU-Präsidentin Kirsten Pedd diskutierte darüber bei einer Podiumsveranstaltung *(siehe Bilder)*: »Die Inkassowirtschaft nimmt ihre Verantwortung wahr und hat die neuen Datenschutzregeln bereits frühzeitig umgesetzt. Unsere Unternehmen hat das vor große Herausforderungen gestellt. Nicht immer war der Aufwand verhältnismäßig. Vor allem kleinere Inkassounternehmen hat es an den Rand ihrer Ressourcen gebracht, die teilweise sehr kleinteiligen und arbeitsintensiven DSGVO-Anpassungen vorzunehmen. Und das war alles parallel zum ohnehin bereits anspruchsvollen Tagesgeschäft zu leisten.«

Grundsätzlich sieht Pedd die DSGVO aber positiv. »Datenschutz ist für Verbraucher und Unternehmen eines der entscheidenden Zukunftsthemen. Die DSGVO ist dabei eine Chance. Sie hat dazu beigetragen, für den Umgang mit personenbezogenen Daten noch stärker zu sensibilisieren.« Allerdings sieht Pedd auch weiterhin Probleme. Unklar sei es zum Beispiel, wann eine Datenschutzfolgeabschätzung abzugeben sei, es gibt unbeantwortete Fragen zum Umgang mit Datenpannen und zur datenschutzrechtlichen Ausgestaltung von Verträgen im Forderungsmanagement. »Hier sind wir in der Diskussion und werden das im Sinne unserer Branche weiter begleiten. Ein Meilenstein ist dabei der Code of Conduct (CoC), den unser Europaverband FENCA mit tatkräftiger Unterstützung des BDIU erarbeitet. Dieser CoC wird die Rechtssicherheit bringen, die die DSGVO in vielen für Inkasso relevanten Teilen leider vermissen lässt.«

Ein Code of Conduct zur DSGVO

Mit der DSGVO stehen Datenschutzthemen überall in Europa ganz oben auf der Tagesordnung. Dabei nimmt die DSGVO gewissermaßen eine Helikopterposition ein: Sie betrachtet von oben, wie Unternehmen, Vereine, Institutionen mit personenbezogenen Daten umgehen, und gibt dem Ganzen einen ordnenden Rahmen. Wenn es aber um konkrete Anwendungen beispielsweise für eine spezifische Branche geht, dann lässt die DSGVO einen teilweise sehr großen Interpretationsspielraum. Das ist einerseits zwar sinnvoll – denn nicht alle technischen Datenverarbeitungen, die Unternehmen in ihren ganz alltäglichen Arbeitsroutinen anwenden, müssen durch eine gesetzliche Verordnung bis ins letzte Detail geregelt sein. Andererseits lässt das aber auch Unklarheiten und schafft bei konkreten Fragen immer wieder eigentlich vermeidbare Rechtsunsicherheiten.

Genau hier setzt der Code of Conduct (CoC) der FENCA an. Die Federation of European National Collection Associations (also der europäische Inkassodachverband) hat schon vor zwei Jahren damit begonnen, die Workflows für Inkasso und Forderungskauf mit Blick auf die Datenverarbeitung zu ermitteln. Das ist letztlich die Basis für den CoC. Der Code konkretisiert und interpretiert die DSGVO praxisbezogen für alle inkassorelevanten Datenverarbeitungstätigkeiten. Das heißt, die auslegungsfähigen Teile der Verordnung werden durch den CoC so präzisiert, dass sie auch zweifelsfrei auf das Forderungsmanagement angewendet werden können.

Der Code of Conduct steht auf der Tagesordnung der nächsten Mitgliederversammlung des Inkasso-Europaverbands. Diese findet Ende Oktober in Straßburg statt, wo die FENCA ihren European Collection Congress veranstaltet. Im nächsten Schritt soll der CoC der zuständigen EU-Datenschutzaufsichtsbehörde vorgelegt werden. Wird er durch diese anerkannt, erhält der Code Rechtswirkung, an die sich sämtliche Datenschutzaufsichtsbehörden auf allen Ebenen der EU bei der Auslegung der DSGVO halten müssen.