Michael Freytag (Hg.)

BETRUG IN DER DIGITALISIERTEN WELT

Erkennen. Vorbeugen. Schützen.

Frankfurter Allgemeine Buch

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Michael Freytag (Hg.)
Betrug in der digitalisierten Welt
Erkennen. Vorbeugen. Schützen.

FAZIT Communication GmbH
Frankenallee 71–81
60327 Frankfurt am Main
Geschäftsführung: Peter Hintereder, Hannes Ludwig

Frankfurt am Main 2019

ISBN 978-3-96251-057-2

Frankfurter Allgemeine Buch

Redaktion Eric Czotscher, Georg Poltorak, Jacqueline Preußer, F.A.Z.-Institut für Management-, Markt- und Medieninformationen GmbH
Korrektorat Kirstin Gründel
Satz Jan Walter Hofmann
Umschlag Daniela Seidel
Druck CPI Books GmbH, Leck

Printed in Germany

Die Begriffe Arbeitnehmer, Mitarbeiter, Verbraucher, Kunde etc. bezeichnen in dieser Publikation sowohl weibliche als auch männliche Personen.

Inhalt

Mit Technik gegen Betrug

Alle sind gefordert

Meine Identität gehört mir

Dr. Michael Freytag,
Vorstandsvorsitzender der SCHUFA Holding AG

Einleitung

Die Digitalisierung hat unsere Gesellschaft tiefgreifend verändert: die Art und Weise, wie wir miteinander kommunizieren, wie wir produktive Werte schaffen oder wie wir lernen. Wir verbringen immer mehr Zeit im Netz und verlassen uns bei immer mehr Aufgaben auf elektronische Unterstützung. Digitale und analoge Welt verzahnen sich auf diese Weise eng miteinander. Das „Internet der Dinge" wird nicht nur in der Industrie zu tiefgreifenden Veränderungen führen, und mit den Fortschritten bei der künstlichen Intelligenz werden zunehmend Entscheidungen an Computer delegiert – ob in der Medizin, im Straßenverkehr oder im Handel, um nur einige Bereiche herauszugreifen. Der Mensch profitiert in vielerlei Hinsicht von diesem Umbruch: durch mehr Komfort, mehr Möglichkeiten und letztlich auch mehr Sicherheit.

Diese Entwicklung hat auch Schattenseiten, denn Kriminelle haben ihren Fokus auf die digitale Welt erweitert und sich durch neuartige Werkzeuge und Kommunikationswege zusätzliche Angriffs- und Gewinnmöglichkeiten erschlossen. Die Anonymität im Netz, der Wegfall räumlicher Nähe und neue Verschleierungsmethoden wirken als Verstärker. Jedes Unternehmen, jede Institution und jede Person kann im Internet Opfer von Betrügern, Erpressern oder Saboteuren werden – nicht nur, wer arglos mit seinen Daten umgeht. Die Zahl der Deliktfälle und die Schadenshöhen sind in den vergangenen Jahren deutlich gestiegen und werden voraussichtlich weiter zulegen. Die Abgrenzung zwischen digitaler und herkömmlicher Kriminalität fällt schwer, da auch klassische Betrüger und andere Kriminelle kaum auf elektronische Hilfsmittel verzichten.

Betrug ist selbstverständlich kein neues Phänomen. Insgesamt weist die Polizeiliche Kriminalstatistik (PKS) des Bundeskriminalamts für 2017 rund 910.000 erfasste Betrugsfälle in Deutschland aus. Ihr Anteil an der Gesamtkriminalität, also an allen Straftaten, kam damit auf rund 16 Prozent. Im Bereich der Internetkriminalität war Betrug mit 74 Prozent sogar die vorherrschende Straftat. Allerdings lassen sich hierzu nur schwer belastbare Zahlen ermitteln, da von einer sehr hohen Dunkelziffer ausgegangen werden muss. Eines ist sicher: Betrug gehört zu den am schnellsten zunehmenden Delikten im Internet. Dabei bedeuten betrügerische Handlungen nicht nur einen wirtschaftlichen Schaden für die betroffenen Verbraucher und Unternehmen, sondern sie erzeugen einen hohen Aufwand auch für Behörden, Polizei und die gesamte Gesellschaft. Die Zeche zahlen letztlich die seriösen Unternehmer und ehrlichen Verbraucher, denn Betrugsschäden werden in der Preisgestaltung berücksichtigt.

Vielfältige Betrugsformen

Die Möglichkeit, Waren und Dienstleistungen aller Art im Internet von zu Hause bequem per Knopfdruck zu erwerben und zu bezahlen, ist ein fester Teil unserer Lebenswelt geworden. Immer größer und vielseitiger wird die Auswahl, und immer schneller läuft der Erfüllungsprozess von der Bestellannahme über den Versand bis zur Rechnungsstellung. Dies machen sich Täter zunutze. Das Internet gewinnt deshalb als Tatmittel zunehmend an Bedeutung, wobei die Phantasie der Täter kaum Grenzen kennt: Identitäten werden gestohlen oder gefälscht, Kundenkonten manipuliert oder falsche Lieferadressen angegeben.

Die häufigste Betrugsform ist der Warenkreditbetrug. Die Tatsache, dass eine Zahlung ausbleibt oder der Kunde nicht auf Zahlungsaufforderungen reagiert, ist allerdings allein noch kein zuverlässiges Verdachtsmoment. Deshalb wird Betrug oft erst mit einer erheblichen Zeitverzögerung erkannt – etwa im Rahmen eines Inkassoprozesses, wenn herauskommt, dass der säumige Kunde gar nicht existiert oder zumindest nicht an der angegebenen Anschrift lebt.

Aufgrund der hohen Kaufkraft und der verlässlichen Infrastruktur finden Betrüger in Deutschland besonders günstige Bedingungen für kriminelle Transaktionen. Auch die hierzulande übliche und besonders verbraucherfreundliche Möglichkeit des Rechnungskaufs ist in anderen Ländern nicht selbstverständlich. Unternehmen, die ihren

Kunden diese Bezahloption aus Sicherheitsgründen nicht anbieten, haben es schwer, sich im Wettbewerb zu behaupten.

Betrug verhindern

Weil Betrug innerhalb der Cyberkriminalität ein so hohes Gewicht hat, ist es sinnvoll, hier einen Schwerpunkt auf Präventionsmaßnahmen zu setzen. Das Vertrauen aller in Möglichkeiten und Angebote ist eine äußerst wichtige Voraussetzung, damit die Gesellschaft als Ganzes von den vielfältigen Vorteilen der Digitalisierung profitieren kann. Denn nur so kann die digitale Wirtschaft in Deutschland ihr Wachstumspotential heben – ob als Start-up oder als etabliertes Unternehmen. Die Fragen, die sich heute stellen, sind vielfältiger geworden. Neben der Frage „Kann der Kunde zahlen?“ – also der Frage nach der Bonität – spielen immer häufiger auch Fragen wie „Ist der Kunde auch wirklich der, der er vorgibt zu sein?“ (Identität), „Darf ich mit ihm überhaupt Geschäfte machen?“ (Compliance) und „Will der Kunde überhaupt zahlen?“ (Betrug) eine Rolle. Um Zahlungsausfälle zu verhindern, müssen Unternehmen deshalb bei allen Geschäften mit Neu-, aber auch mit Bestandskunden entscheiden, welches Spektrum an Bezahlarten sie anbieten wollen. Außerdem wägen sie ab, ob sie die Lieferung an eine von der Rechnungsadresse abweichende Lieferadresse ermöglichen. Im Spannungsfeld zwischen Betrugsvermeidung und Geschäft kommt dem Risikomanagement eine entscheidende Rolle zu. Ein gut funktionierendes Risikomanagement steigert den Umsatz.

Die SCHUFA ist bereits seit vielen Jahren mit Lösungen rund um Identität, Betrugsprävention und Compliance am Markt. Als Schutzgemeinschaft auf Gegenseitigkeit ist es ihr Ziel, Unternehmen, Bürger und die Gesellschaft wirksam vor Schaden durch betrügerische Handlungen zu schützen.

Gegenseitiger Austausch ermöglicht Schutz

Um einen wirksamen Schutz für alle zu gewährleisten, befassen sich die Sicherheitsbehörden verstärkt mit Cyberkriminalität und Identitätsmissbrauch. Das geschieht auch in Kooperation mit privaten Wirtschaftsunternehmen, denn von Cyberkriminalität betroffene Organisationen registrieren als erste, welche Betrugsformen und -muster zur Anwendung kommen. Aufbauend auf deren Erfahrun-

gen, lassen sich dann entsprechende Lösungsansätze entwickeln. Beispielsweise kooperiert der German Competence Centre against Cyber Crime e.V. (G4C), in dem auch die SCHUFA engagiert ist, eng mit dem Bundeskriminalamt (BKA) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI). Der G4C fördert den Austausch zwischen seinen Mitgliedern und Kooperationspartnern aus öffentlicher Hand und Privatwirtschaft. Erkenntnisse zu aktuellen Entwicklungen der Internetkriminalität und der Betrugsprävention werden unmittelbar geteilt. Auch die SCHUFA ermöglicht durch das bewährte Gegenseitigkeitsprinzip sowie durch neuartige Produkte und Verfahren, dass sich Unternehmen gegenseitig informieren und warnen – mit Informationen zur Bonität und Identität ihrer Kunden sowie zu Betrugsfällen. Auf diese Weise kann sich die Wirtschaft vor Schäden schützen, und eine schnelle und sichere Kreditvergabe wird möglich. Unternehmen und Verbraucher profitieren hiervon gleichermaßen.

Das vorliegende Buch befasst sich mit unterschiedlichen Formen des digitalen Betrugs und seinen weitreichenden Auswirkungen auf Wirtschaft, Gesellschaft und Kultur. Es zeigt aber auch Möglichkeiten auf, Menschen und Institutionen bei ihren alltäglichen Aktivitäten im digitalen Raum wirksamer zu schützen. Vor allem unterstreichen die Expertenbeiträge, dass der Kampf gegen Online-Betrug nur mit vereinten Kräften gewonnen werden kann. Das spiegelt die Vielfalt der zu Wort kommenden Experten und Expertinnen aus Wissenschaft, Unternehmenspraxis, Behörden und aus der Kultur deutlich wider. Den Autorinnen und Autoren dieses Buchs, die mit ihrer Expertise und ihrem Engagement dazu beitragen, dem digitalen Betrug einen Riegel vorzuschieben, gilt mein besonderer Dank. Sie werden im Folgenden mit ihren jeweiligen Themen in der Reihenfolge der Buchkapitel kurz vorgestellt.

Mit vereinten Kräften gegen Cyberkriminalität

Um Unternehmen und Verbraucher gleichermaßen gegen Cyberkriminalität zu schützen, hat die deutsche Internetwirtschaft besondere Maßnahmen ergriffen. Oliver Süme, Vorsitzender des eco – Verband der Internetwirtschaft e.V., stellt Projekte vor, die der eco gemeinsam mit seinen Partnern ins Leben gerufen hat und die bereits heute für Betrugsprävention im Internet sorgen. Nicht selten haben es Angreifer auf die Daten ihrer Opfer abgesehen, die sie weiterverkaufen oder für eigene kriminelle, betrügerische Zwecke nutzen. Im Gespräch erläutert der IT-Forensiker und Leiter des Bereichs Compliance &

Forensic bei der KPMG AG Wirtschaftsprüfungsgesellschaft, Alexander Geschonneck, wie Hacker bei ihren Angriffen auf Computersysteme vorgehen, und erklärt, was im Ernstfall eines IT-Sicherheitsvorfalls zu tun ist.

Die kontinuierlich zunehmende globale Vernetzung erleichtert es Kriminellen, sich auch über Landesgrenzen hinweg zusammenzuschließen und weltweit User zu schädigen. Um angesichts dieser digitalen Bedrohungslage die Bevölkerung schützen zu können, hat die EU eine eigene Institution gegründet: die European Union Agency for Network and Information Security (ENISA). Sie hat nicht nur zahlreiche Initiativen und Kooperationen gegen Cyberkriminalität gestartet, sondern formuliert Leitlinien für die Sicherheit im Internet. Der geschäftsführende Direktor der ENISA und Honorarprofessor der Universität der Bundeswehr München, Prof. Dr. Udo Helmbrecht, erklärt, wie seine Behörde Finanzdienstleister dabei unterstützt, Betrug frühzeitig zu erkennen und Angriffe abzuwehren. Oberstaatsanwalt Andreas May, Leiter der Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) in Gießen, ist mit seiner Ermittlungsarbeit Cyberkriminellen auf der Spur. Oftmals stößt er dabei an die Grenzen der deutschen Rechtsprechung, was Fragen zur Strafverfolgung im digitalen Raum aufwirft. Als nationales Pendant zur ENISA befasst sich das Bundesamt für Sicherheit in der Informationstechnik (BSI) unter anderem mit den Risiken der allgegenwärtigen Digitalisierung. Der Präsident des BSI, Arne Schönbohm, benennt zentrale Cyberbedrohungen und zeigt auf, worauf es bei einem wirksamen Schutz ankommt.

Gesellschaftliche Folgen betrügerischer Machenschaften

Welche tiefgreifenden Auswirkungen Betrug auf die Gesellschaft haben kann, beschreibt der Regisseur und Autor David Spaeth. In seinem Dokumentarfilm „Betrug“ zeigt er, was einen Hochstapler dazu bewegte, sich das Ersparte einer Münchener Elterninitiative zu erschleichen. Zusätzlich beleuchtet er auch den Standpunkt der Opfer, die ihre Erfahrungen im Umgang damit beschreiben, von einem Betrüger systematisch getäuscht und finanziell sowie sozial ausgenutzt worden zu sein.

Prof. Dr. phil. Hans-Dieter Hermann, Hochschulprofessor an der Deutschen Hochschule für Prävention und Gesundheitsmanagement in Saarbrücken sowie Honorarprofessor an der Universität Tübingen, weist darauf hin, dass Vertrauen die Basis für eine funktionsfähige

Gesellschaft bildet. Anhand von Erkenntnissen aus der Soziologie, der psychologischen Forschung und der Neurobiologie erklärt der DFB-Teampsychologe der deutschen Nationalmannschaft, wie Vertrauen entsteht und welche Auswirkungen es auf unser gesellschaftliches Zusammenleben hat. Nicht nur im zwischenmenschlichen Kontext, sondern auch im Umfeld digitaler Märkte spielt Vertrauen eine entscheidende Rolle. Vor diesem Hintergrund diskutieren Prof. Dr. Lucia A. Reisch, Hochschulprofessorin an der Copenhagen Business School im Fachbereich Interkulturelle Konsumforschung und europäische Verbraucherpolitik, und Prof. Dr. Hans-Wolfgang Micklitz, Hochschulprofessor für Wirtschaftsrecht am Europäischen Hochschulinstitut in Florenz, über die Herausforderungen, denen sich der Verbraucherschutz und die Verbraucherpolitik im digitalen Zeitalter stellen müssen.

Doch was treibt Betrüger an? Dieser Frage widmen sich Prof. Dr. Detlef Fetchenhauer, Hochschulprofessor im Fachbereich Wirtschafts- und Sozialpsychologie an der Universität zu Köln, Anne-Sophie Lang, wissenschaftliche Mitarbeiterin am Lehrstuhl für Wirtschafts- und Sozialpsychologie an der Universität zu Köln, und Prof. Dr. Dominik H. Enste, Hochschulprofessor für Wirtschaftsethik an der TH Köln. Sie erläutern, welche Erkenntnisse die psychologische Forschung über betrügerisches Verhalten und dies begünstigende Faktoren hervorgebracht hat.

Mit der flächendeckenden Akzeptanz des E-Commerce durch die Verbraucher hat sich das Potential betrügerischen Verhaltens deutlich erhöht. Christoph Wenk-Fischer, Hauptgeschäftsführer des Bundesverbands E-Commerce und Versandhandel Deutschland (bevh), und Sebastian Schulz, Leiter des Bereichs Rechtspolitik & Datenschutz des bevh, informieren, wie Betrugsprävention im E-Commerce durch eine angemessene Risikosteuerung funktioniert.

Neue Technologien helfen, Betrug zu erkennen und zu verhindern

Die Journalistin Anna Biselli analysiert in einem gemeinsamen Beitrag mit Dr. Ivan Gudymenko, IT Security Architect bei der T-Systems Multimedia Solutions GmbH, und Prof. Dr. Thorsten Strufe, Inhaber des Lehrstuhls für Datenschutz und Datensicherheit an der Technischen Universität Dresden, die vielfältigen Betrugsmöglichkeiten im Internet. Dabei gehen die Experten für IT-Sicherheit auch auf die technischen Möglichkeiten ein, die Cyberkriminellen für ihre

betrügerischen Aktivitäten zur Verfügung stehen. Als Manager Fraud Detection verantwortet Luisa Stock die Betrugsprävention beim Zahlungsanbieter Klarna. Im Interview erläutert sie, wie der Anbieter von Zahlungslösungen durch sein Angebot das Risiko, beim Online-Shopping betrogen zu werden, für Verbraucher und Online-Händler gleichermaßen reduziert.

Dr. Gjergji Kasneci, Chief Technology Officer und Bereichsleiter Innovation und strategische Analyse bei der SCHUFA Holding AG, beleuchtet, welche Technologien bei der Betrugserkennung angewendet werden können. Eine dieser Technologien ist künstliche Intelligenz (KI). Das Traditionsunternehmen Otto hat bereits langjährige Erfahrung mit Betrugsbekämpfung. Hans-Georg Spliethoff, Bereichsleiter Kreditmanagement bei Otto GmbH & Co. KG, weist im Gespräch darauf hin, dass Technologien mit dem Know-how von Experten kombiniert werden müssen, damit Verbraucher optimal vor Betrug im Online-Handel geschützt werden können.

Prof. Dr. Jürgen Bott, Professor im Fachbereich Betriebswirtschaftslehre an der Hochschule Kaiserslautern, und Dr. Udo Milkau, Chief Digital Officer im Transaction Banking der DZ BANK AG, veranschaulichen die Möglichkeiten bei der Betrugserkennung, die durch den Einsatz von KI im Rahmen von Echtzeitbezahlverfahren gegeben sind.

Achtsamkeit ist geboten

In der digitalen Welt sind Vertrauen und ethisches Handeln die Voraussetzung dafür, dass Innovation und neue Technologien eine breite gesellschaftliche Zustimmung erfahren können. Demgemäß erläutert Karl-Heinz Streibich, Präsident und Vorsitzender des Senats von acatech (Deutsche Akademie der Technikwissenschaften e.V.), den Ethikbegriff im Zusammenhang mit der Digitalisierung.

Zusätzlich spielt das individuelle Verhalten der Nutzer von digitalen Technologien und Internet eine zentrale Rolle bei der Betrugsprävention. Dr. Ibrahim Karasu, Geschäftsführer Retail Banking und Banktechnologie beim Bundesverband deutscher Banken e.V., plädiert in diesem Zusammenhang für einen bewussteren Umgang mit den weiter zunehmenden elektronischen Transaktionen. Er zeigt auf, wie sich Menschen in Berufsalltag und Privatleben vor potentiellen Angriffen und daraus entstehenden finanziellen Schäden schützen

können. Vor allem bei der Preisgabe sensibler persönlicher Daten sei Vorsicht geboten.

Seit dem 25. Mai 2018 regelt die Datenschutz-Grundverordnung (DSGVO) den Umgang mit personenbezogenen Informationen. Prof. Eike Richter, Oberregierungsrat und Hochschulprofessor für Öffentliches Recht, Recht der Digitalisierung und für IT-Sicherheitsrecht an der Hochschule der Akademie der Polizei Hamburg, weist auf das Spannungsverhältnis zwischen Betrugsbekämpfung und Persönlichkeitsschutz hin. Der Rechtsanwalt und Leiter des Bereichs Recht & Regulierung beim Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e.V. (VATM), Dr. Frederic Ufer, beleuchtet das Thema Betrugsbekämpfung und Verbraucherschutz bei mobilen Mehrwertdiensten. Er zeigt auf, welche Maßnahmen der Gesetzgeber und die Telekommunikationsbranche ergriffen haben, um das betrügerische Geschäft mit sogenannten Ping-Anrufen und Internetabofallen zu unterbinden.

Der Mensch im Fokus

Um an die persönlichen Daten ihrer Opfer zu gelangen, greifen Hacker und Online-Betrüger auch auf Methoden des sogenannten Social Engineering zurück. Prof. Dr. Stephan G. Humer, Leiter des Forschungs- und Arbeitsbereichs Internetsoziologie (FABIS) an der Hochschule Fresenius Berlin, und Denise Burkert, ehemalige Mitarbeiterin bei FABIS und derzeit Studierende im Masterstudiengang Security Management an der TH Brandenburg, erklären, was diese besondere Angriffsstrategie ausmacht. Damit der Mensch nicht zur Schwachstelle der Sicherheitsarchitektur wird, plädieren die Autoren für umfassende Schulungsangebote. Nur wer seinen Gegner und die entsprechenden Methoden der Betrüger kenne, könne sich effektiv vor Angriffen schützen.

Betrugsopfer müssen oft einen immensen Aufwand betreiben, um den Schaden in den Griff zu bekommen. Tina Groll, Autorin und Redakteurin bei ZEIT ONLINE im Ressort Politik & Wirtschaft, war in den Jahren 2009 und 2010 selbst Opfer von Identitätsmissbrauch und wehrte sich erfolgreich dagegen. Gemeinsam mit Cem Karakaya, ehemaliger Interpol-Agent und Experte für Internetkriminalität bei der Polizei München, berichtet sie von ihren Erfahrungen. Darüber hinaus geben beide wertvolle Hinweise, wie man sich vor Identitätsmissbrauch und -diebstahl schützen kann.