

B u c h r e z e n s i o n

Michael Büchel/Peter Hirsch, Internetkriminalität, Phänomene – Ermittlungshilfen – Prävention, Kriminalistik Verlag, Heidelberg u.a. 2014, 164 S., € 29,99.

Straftaten im Internet bzw. in dessen Umfeld sind in der heutigen Zeit längst zu einem Problem des täglichen Lebens geworden, und die Anzahl derartiger Delikte in den Kriminalstatistiken ist mehrheitlich im Begriff, (deutlich) zu steigen. Hacking, Skimming, Phishing, Trojaner, ARP-Spoofing, Ransomware, Cash Trapping, Filesharing, etc. – die regelmäßige Konfrontation mit diesen neuen Ausprägungen strafbaren Handelns verlangt daher auch von (angehenden) JuristInnen immer öfter, zumindest grundlegend über Internetkriminalität und deren rechtliche Beurteilung im Bilde zu sein.

Einen wertvollen Beitrag zur Aneignung eines dahingehenden Wissens stellt das gegenständliche Werk der beiden Kriminalhauptkommissare *Michael Büchel*, LL.M., und *Peter Hirsch*, M.A., dar, die neben ihrer polizeilichen Tätigkeit u.a. auch regelmäßig als Gastdozenten in verschiedenen Aus- und Weiterbildungseinrichtungen tätig sind.

Die beiden *Verf.* zeigen in ihrem Werk den Facettenreichtum der Internetkriminalität auf und beschreiben, wie vielfältig die darunter verstandenen Tathandlungen sein können, was sich nicht zuletzt in den divergenten Definitionen des Begriffs „Internetkriminalität“ widerspiegelt.

Ebenso vielfältig und unterschiedlich stellen sich die einzelnen Kapitel dieses Buches dar, die sich zumeist einem Delikt bzw. einer Deliktsgruppe widmen. So beschäftigen sich die *Verf.* beispielsweise mit den unterschiedlichen Ausprägungen des Identitätsdiebstahles, des Social Engineerings bzw. Social Hackings, des Phishings und Skimmings, der Ransomware („Online-Erpressung“), der Kinderpornographie oder des Cyber-Mobbings/Cyber-Bullyings. Darüber hinaus werden etwa auch die Themenkreise Onlinebanking, Telefonanlagen- bzw. Router-Hacking, Passwortsicherheit sowie Finanz- und Warenagenten behandelt sowie Grundzüge des Urheberrechts und der Computerforensik erläutert und schließlich Organisationen und Einrichtungen der IT-Sicherheit kurz vorgestellt.

Die *Verf.* beschreiben dabei zunächst umfangreich das jeweilige Phänomen und mögliche Ausprägungsformen desselben, wobei sich diese Darstellungen in einer Art präsentieren, die auch für auf diesem Gebiet bis dato kaum bewanderte Personen verständlich ist. Danach wird kurz erläutert, unter welche strafrechtlichen Normen sich das beschriebene Verhalten subsumieren lässt, wobei auf die einzelnen Merkmale der genannten Tatbestände (bewusst) nicht eingegangen wird, sodass hier allenfalls vertiefende Literatur zu den einzelnen Delikten herangezogen werden muss. Eine Aufarbeitung der einzelnen Tatbestände aus strafrechtlicher oder gar strafrechtsdogmatischer Sicht bietet das Buch daher nicht; einen derartigen Anspruch erheben die *Verf.* allerdings auch nicht, wie sie in ihrem Vorwort (Seite V) darlegen: Für sie ist vielmehr bedeutend, dass in ihrem Werk „die Phänomene als solche im Mittelpunkt“ stehen. Aus strafrechtswissenschaftlicher Sicht hingegen ausgesprochen wertvoll erscheinen in

diesem Zusammenhang die auch in diesen kurzen strafrechtlichen Abrissen enthaltenen Hinweise darauf, wie die einzelnen Delikte voneinander abzugrenzen sind bzw. worin die Unterschiede in Hinblick auf die strafrechtliche Bewertung der dargestellten Formen kriminellen Handelns bestehen.

Im Anschluss an die strafrechtliche Beurteilung des jeweiligen Verhaltens folgen kursorische Ausführungen darüber, wie der in diesem Kapitel dargestellten Form der Internetkriminalität auch auf zivilrechtlicher Ebene begegnet werden kann bzw. welche zivilrechtlichen Folgen diese jeweils nach sich ziehen kann. In diesem Zusammenhang wird etwa dargelegt, ob (und auf welcher gesetzlichen Grundlage) Schadensersatzpflichten oder allfällige andere, nicht auf finanziellen Ersatz gerichtete Ansprüche (wie beispielsweise auf Unterlassung, etc.) bestehen können.

Der starke Praxisbezug der *Verf.* erschließt sich nicht zuletzt beim Lesen der anschließenden „Checkliste für die Ermittlungspraxis“, in der die Vorgehensweise der Polizei bei Anzeigenerstattung und anschließender Ermittlung grundlegend dargestellt wird. Dadurch wird herausgestrichen, worauf es bei der Ermittlung – etwa auch in Hinsicht auf die Beweisbarkeit von Delikten aus dem Bereich der Internetkriminalität – in der Praxis tatsächlich ankommt.

Die (fast) jedes Kapitel abschließenden Erläuterungen zu in Frage kommenden „Präventionsmaßnahmen“ zeigen Möglichkeiten auf, wie man sich wirksam vor der jeweiligen Form von Internetkriminalität schützen kann. Die dort aufgelisteten Maßnahmen reichen von der Auswahl sicherer Passwörter und dem richtigen Umgang mit spam-verdächtigen E-Mails über regelmäßige Sicherheitsscans und den Einsatz von Virenschutzprogrammen bis hin zur sicheren Aufbewahrung von berührunglosen Zahlungsmitteln in Hosens- oder Handtaschen. Darüber hinaus wird beispielsweise erläutert, welche schwerwiegenden Folgen die achtlose Entsorgung von Poststücken, die persönliche Daten wie Namen, Adressen oder Kunden- bzw. Kontonummern enthalten, nach sich ziehen kann – und mit welchen einfachen Mitteln man derartige kriminelle Handlungen zu verhindern oder zumindest deren Begehung zu erschweren vermag.

Kurz gesagt: Als Einführungswerk, das sich insbesondere an Polizeibeamte in Ausbildung (und andere „Neueinsteiger“ in diese Materie) richtet, ist dieses Buch jedenfalls auch für Studierende der Rechtswissenschaften geeignet, die einen ersten Einblick in das Problemfeld „Internetkriminalität“ gewinnen möchten. Kleinere Versehen (etwa das vereinzelt Vertauschen von „StGB“ und „BGB“) sind angesichts der – gut aufbereiteten – Fülle an Information und des sehr verständlichen Schreibstils zu vernachlässigen. Besonders hervorzuheben ist darüber hinaus, dass aufgrund des starken Praxisbezugs, den die beiden *Autoren* aus ihrer alltäglichen Arbeit einfließen lassen, nicht bloß rechtliches Grundlagenwissen vermittelt wird, sondern auch ein Eindruck davon entsteht, worin Schwierigkeiten in der realen Ermittlungspraxis bestehen können. Ergänzende Ausführungen zu den zivilrechtlichen Aspekten unterstreichen den ganzheitlichen Zugang der *Verf.* zu diesem Themenkomplex und runden das Werk ab. Die abschließenden Präventionsmaßnahmen komplettieren nicht nur die Ausführungen, sondern verschaffen

der Leserschaft auch über den Wissenserwerb hinaus die Möglichkeit, sich selbst (besser) vor Internetkriminalität zu schützen. Damit ist die Lektüre dieses Werkes sogar in mehrfacher Hinsicht ein wahrer Gewinn!

Univ.-Ass. Mag. iur. Sebastian Gölly, Graz