Eberhard Zehendner

Cybercrime – Editorial zum Schwerpunkt

Der Schwerpunkt *Cybercrime* handelt von massiver Internetkriminalität: *Cybercrime* (deutsch *Internetkriminalität*, manchmal fälschlich mit *Computerkriminalität* gleichgesetzt) ist ein schillernder Begriff, unter dem mancher zu verstehen vorgibt, was seinen Partikularinteressen nutzt. Denn nicht jedes Vergehen, bei dem ein Computer benutzt wird, ist *Cybercrime*. Und *Skriptkiddies* sind sicher anders zu be- (und ver-)urteilen als hochprofessionelle Vermieter von *Botnetzen*. Denn hinter *Cybercrime* können – obschon Beute und Schaden selten genau und nachprüfbar bezifferbar sind – gewaltige finanzielle Interessen stehen, die z. B. mit Identitätsdiebstahl oder Erpressung arbeiten. Aber – das haben diverse Enthüllungen der letzten Jahre wieder einmal deutlich gezeigt – auch Regierungen und Geheimdienste fungieren mitunter als Auftraggeber systematischer und umfassender krimineller Akte im Internet. Ganz aktuell nutzen fremdenfeindliche Organisationen das Netz, um ihre Hasskampagnen zu orchestrieren – und einem bundesdeutschen Justizminister fällt dazu nicht mehr ein, als *Facebook* um freundliche Mithilfe zu bitten, eine ganz neue Auffassung von *Public Private Partnership,* wie es scheint.

Dominik Brodowski und *Felix Freiling* sehen in ihrem Beitrag *Cyberkriminalität – Erscheinungsformen, Entwicklungslinien, Herausforderungen* Begriff und Thematik im Schnittfeld von rechtlichen und technischen Fragen. Aus zentralen Besonderheiten des *Cyberspace* leiten sie ein – im Vergleich zur klassischen Kriminalität – anderes oder erhöhtes Bedrohungspotential (insbesondere für ökonomisch motivierte Kriminalität) ab. Die Autoren beschreiben die historische Entwicklung von Cyberkriminalität und deren strafrechtlicher Erfassung, und thematisieren daraus entstandene Herausforderungen, bis hin zu noch wenig verstandenen und strafrechtlich noch kaum thematisierten Deliktsformen.

Carlo Schäfer beleuchtet in seinem Beitrag *Die Rolle von Spam im Cybercrime* die Zusammenhänge zwischen Spam, Phishing und Botnetzen als Grundlage vieler kleiner täglicher Akte von Internetkriminalität, die sich – mögen sie auch als Einzelne genommen eher unbedeutend erscheinen – bereits zu weltweit dramatischen volkswirtschaftlichen Schäden summiert und nicht selten auch Fälle spektakulärer *Cyberspionage* vorbereitet haben. Er kritisiert die bisher übliche Vorgehensweise der Spam-Bekämpfung, die nicht an der Quelle des Problems ansetzt und daher Service-Einschränkungen und *Blacklisting* von E-Mail-Providern nicht verhindern kann, und verweist auf tatsächlich wirksame Alternativen – deren Wirkungsweise zwar veröffentlicht, aber vielen Verantwortlichen anscheinend noch nicht bekannt ist.

In seinem Beitrag *Wardriving – die unterschätzte Gefahr* erläutert Stefan Jäger eine Technik, die Schüler der *Thüringer Junior-Akademie* 2013 ebenso benutzt haben wie zuvor schon der berüchtigte *Albert Gonzalez*. Während jedoch die Schüler sich (und die Bevölkerung) damit nur – und lobenswerterweise – über die (Un-)Sicherheit zahlreicher WLAN-Router am Akademieort informierten, stahl Gonzalez, u. a. mit Hilfe von *Wardriving,* in den Jahren 2005 bis 2007 die Daten von mehr als 180 Millionen Kredit- und Bankkarten. Der *SchlussFIfF* streift in einer satirischen Kurzbiografie von Gonzalez auch das Thema der Verflechtungen zwischen Internetkriminellen, Sicherheitsbehörden und Geheimdiensten.

In ihrem weiteren Beitrag *Transnationale Cyberkriminalität vs. nationale Strafverfolgung: Mögliche Auswege aus einem grundsätzlichen Dilemma* widmen sich *Dominik Brodowski* und *Felix Freiling* vertiefend der – häufigen – Situation, dass Akte von Cyberkriminalität über Staatsgrenzen hinweg verübt werden bzw. Täter sich und/oder ihre Daten in einen anderen Staat in Sicherheit bringen. Die Autoren diskutieren dabei drei Wege, wie dieser Problemlage grundsätzlich begegnet werden könnte.

Alle Beiträge des Schwerpunkts zitieren aus zahlreichen Quellen, die schon für sich genommen interessant sind und tiefer in die Thematik eintauchen. Besonders hingewiesen sei dabei auf das Werk (Brodowski & Freiling, 2011), zu dem es in diesem Heft auch eine Rezension gibt. Die von der Schwerpunktredaktion auf den Seiten 25–28 sowie 38 eingeschobenen Erläuterungsblöcke basieren auf dem Vortrag *Verbrechen im Netz: Cyberkriminelle und ihre Tricks*, den *Felix Freiling* am 15. Juni 2015 im Rahmen der Reihe *Wissenschaft auf AEG* auf dem *Energie Campus Nürnberg* gehalten hat.

Hacking is no Cybercrime!

*„Es geht hierbei **nicht** darum, irgendwelche Passwörter zu knacken, sondern lediglich darum, Systeme und Methoden zu analysieren und zu verstehen, die uns alle alltäglich umgeben. Wenn Firmen Hardware und Software verkaufen, die den Eindruck von Sicherheit vermitteln, dann soll man sich darauf auch verlassen können. Wenn allerdings schon Laien ohne besondere Vorkenntnisse diese Sicherheitssysteme aushebeln und Verschlüsselungsmethoden erkennen können, dann stellt das für Profis erst recht keine Hürde mehr dar. Diese Seite dient dazu, solche Sicherheitsrisiken aufzudecken und Thesen für schwache Verschlüsselungsmuster aufzustellen."*

Wardriving-Forum.de Enzyklopädie, Standardpasswörter http://bit.ly/1nagMvR, Stand: 07.01.2016, CC BY-NC-SA 3.0