Pikett Strafverteidigung, Zürich, 5. September 2023

Strafverteidigung im IT-Recht

Rechtsanwalt Martin Steiger

Steiger Legal

Strafverteidigung im IT-Recht?

Strafverteidigung? ✅

Strafverteidigung im IT-Recht? 

Man könnte auch sagen: Cybercrime, Technologie-Strafrecht, …

Beratung und Verteidigung in der Schnittmenge von Straftaten und Technologie

Unter anderem:

- «Hacking»
- Betrug 💸
- Verbotene Gewaltdarstellungen oder Pornografie
- «Meinungsdelikte»
- Urheberrechtsverletzungen
- Datenschutzverletzungen / Identitätsmissbrauch 💡

Kennzahlen 2022

	Total	davon mit einem Modus Operandi der digitalen Kriminalität	Anteil
Total	**88 478**	**33 345**	**37,7%**
Betrug (Art. 146)	24 195	18 338	75,8%
Betrügerischer Missbrauch einer Datenverarbeitungsanlage (Art. 147)	10 641	3 858	36,3%
Geldwäscherei (Art. 305bis)	3 751	3 025	80,6%
Pornografie (Art. 197)	3 220	2 748	85,3%
Erpressung (Art. 156)	1 770	1 303	73,6%
Unbefugte Datenbeschaffung (Art. 143)	1 395	1 080	77,4%
Datenbeschädigung (Art. 144bis)	731	659	90,2%
Unbefugtes Eindringen in ein Datenverarbeitungssystem (Art. 143bis)	843	601	71,3%
Verletzung des Geheim- oder	951	378	39,7%

	Straftaten	Aufklärungsrate
Total digitale Kriminalität	**33 345**	**34,3%**
Cyber Wirtschaftskriminalität	29 677	27,9%
davon Cyberbetrug	22 207	30,1%
Cyber Sexualdelikte	2 820	92,9%
Cyber Rufschädigung und unlauteres Verhalten	847	62,9%
Darknet	0	-
Andere (Data Leaking)	1	0,0%

Stand der Datenbank: 16.02.2023
Quelle: BFS - Polizeiliche Kriminalstatistik (PKS) 2022

‹ Kriminalität und Strafrecht

Polizei

- Straftaten
- Beschuldigte Personen
- Geschädigte Personen
- Gewalt
- Häusliche Gewalt
- Vermögen
- Digitale Kriminalität
- Betäubungsmittelsubstanzen
- Strassenverkehrsdelinquenz
- Häufigkeitszahlen

Digitale Kriminalität

Einleitung

Die digitale Kriminalität (auch Cyberkriminalität genannt) umfasst alle sogenannten "digitalen" Straftaten, die im Wesentlichen den Straftaten entsprechen, die in den Telekommunikationsnetzen und insbesondere im Internet, begangen werden. In der polizeilichen Kriminalstatistik werden Straftaten der digitalen Kriminalität anhand der Tatvorgehen (Modus Operandi) identifiziert. Es handelt sich folglich nicht um neue Straftatbestände, die in der PKS erfasst wurden, sondern um die Identifizierung von Straftaten mit einer digitalen Komponente.

Methodik

Die digitale Kriminalität wird anhand der Kombination «Straftat – Tatvorgehen» ermittelt. Das untenstehende Schema ermöglicht der Polizei die Auswahl der richtigen Straftat(en) in Bezug auf das angetroffene Phänomen. Einige Phänomene sind sehr ähnlich, und es ist wichtig, nicht nur das korrekte «Straftat – Tatvorgehen»-Paar zu erfassen, sondern vor allem den Hauptmodus

Kontakt

Bundesamt für Statistik
Sektion Kriminalität und Strafrecht
Espace de l'Europe 10
CH-2010 Neuchâtel
Schweiz

Kontakt

Was macht Strafverteidigung im IT-Recht aus?

Zeit für eine Geschichte! 

Hinweis: Die erzählte Geschichte bleibt dem Publikum vor Ort vorbehalten

Wieso habe ich diese Geschichte erzählt?

Was macht Strafverteidigung im IT-Recht aus?

Vor allem: Strafrecht + «Spass am Gerät»

Ziel: Beschuldigte Personen sollten in technischer Hinsicht nicht bei Null beginnen müssen

Hinweis: Die gezeigten praktischen Beispiele bleiben dem Publikum vor Ort vorbehalten

Ziel: Technische Zusammenhänge so erklären, dass sie ~~sogar~~ auch Jurist:innen verstehen

Hilfreich: Aktive Mitarbeit durch die beschuldigte Person

Ziel: Überzeugung durch eigene alternative «Geschichten» im Vorverfahren

Ziel: Kein finanzieller Aufwand für Gutachten! 

Hilfreich: Open Source Intelligence (OSINT)

Schliesslich: Aktuelle Entwicklungen in Recht und Technologie im Auge behalten

www.ntc.swiss/news/rechtsgutachten-strafbark

Nationales Testinstitut für Cybersicherheit

Auftrag | Über Uns | Karriere | Neuigkeiten | Kontakt | DE

Zurück zur Übersicht

Rechtsgutachten Strafbarkeit von Ethical Hacking

Team NTC, 26. Juni 2023

Tags: Publikationen | Medienmitteilungen

Im Auftrag des Nationalen Testinstituts für Cybersicherheit NTC hat die Anwaltskanzlei Walder Wyss unter dem Titel "Strafbarkeit von Ethical Hacking" ein ausführliches Rechtsgutachten erstellt. Ein Ergebnis des Gutachtens ist, dass Ethical Hacking unter Einhaltung gewisser Rahmenbedingungen straffrei ist. Mit der Veröffentlichung des Rechtsgutachtens leistet das NTC einen Beitrag zur aktuellen Nationalen Cyberstrategie des Bundes, die ethisches Hacking institutionalisieren will.

Executive Summary Rechtsgutachten

Rechtsgutachten Strafbarkeit Ethical Hacking

Das Nationale Testinstitut für Cybersicherheit NTC testet, was sonst nicht getestet wird. Es untersucht digitale Produkte und Infrastrukturen, die nicht oder nicht ausreichend geprüft werden - auch auf eigene Initiative. Das Aufspüren von Sicherheitslücken ohne ausdrücklichen Auftrag und ohne Einwilligung ist nach schweizerischem Recht strafbar, sobald die Zugangssicherung eines fremden Systems überwunden oder der Versuch dazu unternommen wird. Zudem stellt das Strafgesetzbuch die Manipulation und Veränderung von Daten unter Strafe.

Rechtfertigender Notstand

Wird im Rahmen von Schwachstellenanalysen gegen Strafnormen verstossen, kann man sich unter bestimmten Umständen auf den rechtfertigenden Notstand nach Art. 17 StGB berufen. Das

podcast.datenschutzpartner.ch/150-ethical-ha

DATENSCHUTZ PLAUDEREIEN

Startseite | Alle Episoden | Abonnieren

DAT150 Ethical Hacking ohne Strafbarbarkeit (Gina Moll und Tobias Castagna, Teil 1)

24. July 2023

DAT150 Ethical Hacking ohne Strafbarbarkeit (Gina Moll und Tobias Castagna, Teil 1)

Was ist Ethical Hacking? Was ist das Nationale Testinstitut für Cybersicherheit in der Schweiz?

Play episode 14:07

podigee Subscribe Share •••

Shownotes

- Teil 2: Responsible Disclosure
- Teil 3: Klimakleber und White-Hat-Hacker

Thematisierte Fragen:

- Was ist das Nationale Testinstitut für Cybersicherheit (NTC)? Was sind seine Aufgaben?
- Wer finanziert das private NTC? Welche Verbindungen gibt es zu den Bundesbehörden?
- Was ist Ethical Hacking? Wie definiert man technische Begriffe, dass sie rechtlich fassbar sind?
- Welche Straftatbestände können White-Hat-Hacker verletzen?
- Was versprach sich das NTC vom Auftrag für das Rechtsgutachten?

Auch im Ausland: Mehr Rechtsprechung!

Mitschuld des Nutzers bei Phishing-Angriffen

Von Rechtsanwalt Jens Ferner (Fachanwalt für Strafrecht & Fachanwalt für IT-Recht)

· 15. Juli 2023 · In Cybercrime Blog, IT-Sicherheit, Wirtschaftsrecht

Beim Phishing nutzen Täter die „Schwachstelle Mensch" aus, um personalisierte Sicherheitsmerkmale auszuspähen und in der Folge Zahlungen auszulösen. Phishing-Angriffe sind daher nicht ohne erhebliche Mitwirkung des Zahlungsdienstnutzers möglich (OLG München, 19 U 2204/22).

Die von Zahlungsdienstnutzern zu erwartende Sorgfalt besteht in diesem Zusammenhang darin, dass sie ihre Zugangsdaten niemandem anvertrauen, der sie dazu auffordert, sei es am Telefon, per E-Mail oder im Internet. Zulässig und wegen der Warnwirkung sogar geboten ist es, wenn die Zahlungsdienstleister ihre Kunden darauf hinweisen, dass sie die Zugangsdaten ausschließlich über die Eingabemasken auf den institutseigenen Internetseiten abfragen und daher jede andere Weitergabe der personalisierten Sicherheitsmerkmale sorgfaltswidrig ist. Bei einer anderweitigen Weitergabe liegt dann stets ein Sorgfaltspflichtverstoß und – abhängig von den Besonderheiten des Einzelfalls, insbesondere subjektiven Gesichtspunkten – der Vorwurf grob fahrlässigen Verhaltens vor.

Wenn sich jedem Zahlungsdienstnutzer in der jeweiligen Situation und dem betroffenen Zahlungsdienstnutzer individuell geradezu aufdrängen musste, dass es sich nicht um einen gewöhnlichen Vorgang handeln kann, ist von grober Fahrlässigkeit auszugehen. Ob der Zahlungsdienstnutzer erkennen muss, dass es sich konkret um einen Phishing-Angriff handelt, ist stets eine Frage des Einzelfalls.

Ein grob fahrlässiger Verstoß gegen die Pflicht, personalisierte

Erlangen von Passwort kein Ausspähen von Daten (AG Jülich)

Von Rechtsanwalt Jens Ferner (Fachanwalt für Strafrecht & Fachanwalt für IT-Recht)

· 27. Juni 2023 · In Cybercrime Blog

Das Amtsgericht Jülich, 17 Cs-230 Js 99/21-55/23, hat den Erlass eines Strafbefehls abgelehnt, der beantragt wurde, nachdem jemand durch Dekompilierung ein Passwort im Klartext erhalten haben soll, mit dem dann Zugriff auf einen Datenbankserver möglich war. Die Entscheidung stelle ich hier im Wesentlichen ein, ohne gesonderte Kommentierung, da ich sie im Juris Praxisreport Strafrecht kommentieren werde.

Hinweise: Die Entscheidung ist nicht rechtskräftig, die Staatsanwaltschaft hat Beschwerde eingelegt, die Sache liegt derzeit beim Landgericht Aachen. In meinem LinkedIn-Posting kommentiere ich kurz, warum ich skeptisch bin, ob das technisch und juristisch korrekt aufbereitet ist. Zudem sollte man meinem längeren Beitrag zur Strafbarkeit des Suchens nach Sicherheitslücken lesen.

Update: Das LG Aachen hat aufgehoben und zurückverwiesen, es muss nun verhandelt werden. Dazu kurz auf LinkedIn von mir sowie die kurze Vorstellung der Entscheidung des LG Aachen.

Amtsgericht Jülich, 17 Cs-230 Js 99/21-55/23

> Nach den Ergebnissen des vorbereitenden Verfahrens erscheint der

Weiterbildung? 🤔

«Dank dem praxisorientierten MAS in Information Security habe ich das notwendige Rüstzeug für die Leitung des Fachbereichs Sicherheit bei der Luzerner Kantonalbank erlangt und konnte mein persönliches und berufliches Netzwerk erweitern.»

Roger Marty, Leiter Fachbereich Sicherheit, Luzerner Kantonalbank

CAS Information Security – Advanced Themen der Informationssicherheit mit Fokus Technik vertiefen

Das CAS Information Security – Advanced vertieft und verbreitert das Wissen, das im CAS Information Security – Technology vermittelt wird. Es fokussiert auf technische Themen, adressiert aber auch die Bereiche Management und

Prof. Armand Portmann
Programmleiter
+41 41 757 68 57
E-Mail anzeigen

Prof. Dr. Maurizio Tuccillo

Und wie immer: «Learning by Doing»


GAMES
CYCLES
FS4
VGACOPY
VIRSCAN
SUB-DIR 11-23-92 7:33p
SUB-DIR 11-23-92 8:59p
SUB-DIR 11-22-92 11:27a
SUB-DIR 12-22-92 7:15p
HIGHSCREEN MB 145P
VIELHAUER
PCTOOLS
BAND 2
PCTOOLS
BAND 1
PCD AND PCL 200 & 300 SERIES
MS-Word 5.0

Diskussion / Fragen ✋

martinsteiger.ch