Cybercrime

Cybercrime (zusammengesetzt aus engl. „cyber“ = im Internet und lat. „crimen“ = Vorwurf/Anklage) bezeichnet Vergehen beziehungsweise Verbrechen in Zusammenhang mit dem Internet. Alternative Ausdrücke sind Internetkriminalität und Internetdelinquenz.

Formen von Cybercrime

Das Spektrum der Internetkriminalität reicht von Straftaten wie Volksverhetzung und Kinderpornografie über neue Formen des Betrugs, Wirtschaftskriminalität und Werbe-Mails („Spam“) bis hin zu Computerviren und Bedrohungen durch „Cyberterrorismus“. Dabei sind nicht nur Online-Accounts oder Computer Ziel der Attacken, sondern zunehmend auch mobile Endgeräte. Denn auch auf diesen leistungsfähigen „Minicomputern“ befinden sich Daten, auf die es Kriminelle abgesehen haben. Beim „Tracking“ der Handybesitzer werden zum Beispiel Standortdaten, Surfgewohnheiten und weitere persönliche Daten für Werbezwecke zusammengeführt. Zu Cybercrime gehören unter anderem:

- Volksverhetzung und extremistische Propaganda
- Gewaltdarstellungen
- schwerwiegende und menschenverachtende Formen der Pornografie
- Betrug, etwa auf eCommerce-Portalen oder Phishing beim Onlinebanking
- Ausspähen und Abfangen von Daten, zum Beispiel Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten
- Datenfälschung und Täuschung im Rechtsverkehr bei Datenverarbeitung
- Verstöße gegen das Urheberrechtsgesetz
- Datenveränderung und Computersabotage
- Digitaler Identitätsdiebstahl, zum Beispiel das Ausspähen von Zugangsdaten, Passwörtern und Kreditkartendaten
- Hacking, Bots ,Viren, Würmer und Trojaner
- Spam-E-Mails

Die Polizeiliche Kriminalstatistik

Laut Polizeilicher Kriminalstatistik ist die Anzahl der Cybercrimedelikte 2021 gegenüber dem Vorjahr deutlich gestiegen: Insgesamt wurden 146.363 Fälle von Computerkriminalität gezählt (2020: 130.611 Fälle). Dazu gehören unter anderem das Ausspähen und Abfangen von Daten sowie die Datenänderung und Computersabotage. Den größten Anteil hat allerdings der Computerbetrug mit 113.002 Fällen, wozu etwa der Betrug mittels rechtswidrig erlangter Daten von Zahlungskarten oder Leistungskreditbetrug zählen. Die Aufklärungsquote in diesem Deliktfeld ist mit 29,3 Prozent sehr niedrig und gegenüber dem Vorjahr (32,1 Prozent) nochmals gesunken.

Prävention in den Bundesländern

Nicht nur das Bundeskriminalamt, auch die Polizei in den einzelnen Bundesländern hat den Kampf gegen die Computer- und Internetkriminalität verstärkt. Dort sind meist so genannte „Zentrale Ansprechstellen Cybercrime“ (ZAC) für die Wirtschaft eingerichtet. Eine Liste dieser Ansprechstellen stellt das BKA zur Verfügung.

Das Bürger-CERT ist ein Projekt des BSI und soll helfen, Bürger und kleine Unternehmen online und per Newsletter vor Viren, Würmern und anderen

Staatliches IT-Krisenmanagement

Bricht durch einen Cyberangriff die gesamte IT (Informationstechnik) zusammen, kann das verheerende Folgen für den Staat, die Wirtschaft und die Gesellschaft haben. Um Angriffe gezielt zu verhindern und abzuwehren, sind in Deutschland unter dem Dach des Bundesamts für Sicherheit in der Informationstechnik (BSI) vier Stellen für das IT-Krisenmanagement zuständig:

Sicherheitslücken zu warnen.

- CERT-Bund (Computer Emergency Response Team für Bundesbehörden, bearbeitet Sicherheitsvorfälle und betreibt einen regelmäßigen Warn- und Informationsdienst.)
- IT-Lage- und Analysezentrum (Bewertung die Sicherheitslage in Deutschland rund um die Uhr.)
- IT-Krisenreaktionszentrum (schnelle Analyse, Koordination und Reaktionen bei Vorfällen.)
- Cyber-Abwehrzentrum (2011 unter Federführung des BSI eingerichtete, gemeinsam mit Bundeskriminalamt, Bundespolizei, Zollkriminalamt, Bundesnachrichtendienst und Bundeswehr betriebenes Zentrum, dient der Zusammenarbeit staatlicher Stellen und der Koordinierung von Schutz- und Abwehrmaßnahmen)

(FL 30.06.2017)

Siehe auch:
Darknet
Cyber-Dschihad
Hacker

Zurück

© Verlag Deutsche Polizeiliteratur