Cybercrime

Cybercrime (zusammengesetzt aus englisch „cyber“ = im Internet und lateinisch „crimen“ = „Vorwurf, Anklage, Verbrechen“) bezeichnet Vergehen beziehungsweise Verbrechen in Zusammenhang mit dem Internet (Internetkriminalität).

Formen von Cybercrime

Das Spektrum der Internetkriminalität reicht von Straftaten wie Volksverhetzung und Kinderpornographie 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 Form 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

Zahl der Übergriffe steigt

Die Zahl der Fälle von IuK-Kriminalität (IuK = Informations- und Kommunikationstechnologie) in Deutschland ist laut Polizeilicher Kriminalstatistik im Jahr 2011 minimal um 0,7 Prozent gestiegen. Gab es in 2010 noch 84.377 Fälle, waren es im Folgejahr 604 Delikte mehr. Die Aufklärungsquote hat sich etwas verschlechtert: Sie sank von 35,8 Prozent der Fälle auf 32,6 Prozent.
Um 84 Prozent und somit am stärksten gestiegen ist die Zahl der Taten im Bereich „Computersabotage, Datenveränderung“: von 2.524 Fällen im Jahr 2010 auf 4.644 Taten im Jahr 2011. Dieser extreme Anstieg wird in der Polizeistatistik auf zunehmende Angriffe mittels Schadsoftware zurückgeführt. Allerdings stieg auch die Aufklärungsquote von Computersabotagen und Datenveränderungen stark an: von 32,1 Prozent in 2010 auf 41,2 Prozent in 2011.
Auch die Zahl der „Fälschung beweiserheblicher Daten“ und der „Täuschungen im Rechtsverkehr bei Datenverarbeitung“ ist gestiegen. Gab es im Vorjahr noch 6.840 solcher Fälle, waren es in 2011 bereits 7.671 (+12,1%). Bei Delikten dieser Art ist die Aufklärungsquote am höchsten: im Jahr 2010 betrug sie 52 Prozent, ein Jahr später 47 Prozent.

Prävention in den Bundesländern

Nicht nur das Bundeskriminalamt, auch die Polizei in den einzelnen Bundesländern verstärkt den Kampf gegen die Computer- und Internetkriminalität. Im Landeskriminalamt NRW beispielsweise ist dazu im Juli 2011 ein Cybercrime-Kompetenzzentrum in Düsseldorf eingerichtet worden. Dazu gehören Ermittlungskommissionen, die Zentrale Internetrecherche, die Auswertestelle für Kinderpornografie und weitere Experten für Computerforensik, Telekommunikationsüberwachung, Auswertung, Analyse und Prävention. Für Unternehmen und Behörden in NRW gibt es zudem eine zentrale Ansprechstelle beim LKA. Dieser „Single-Point-of-Contact (SPoC)“ ist rund um die Uhr erreichbar unter Tel. 0211/9394040 oder Mail an cybercrime.lka@polizei.nrw.de.
In Hessen wurde im Jahr 2011 sogar für den schlimmsten aller Fälle geprobt: Erstmals wurde in einer Übung zusammen mit Bundeswehr, Polizei und andere Behörden der Katastrophenschutz geprobt. Das Szenario: „Cyberwar“. Fazit der Übung: Die technische Fehlersuche funktionierte bestens, die Einschätzung der Konsequenzen eines Cyber-Angriffs war hingegen schwierig. Letztlich waren die Übenden mehr damit beschäftigt, ihre eigene Arbeitsfähigkeit aufrecht zu erhalten, als sich um den eigentlichen Angriff zu kümmern.

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:

- 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.)

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

Zurück