Cybercrime – mögliche Tatbestände

Cybercrime ist in aller Munde. Auch die Strafverfolgungsbehörden setzen mittlerweile spezialisierte Einheiten in diesem Bereich ein bzw. bauen die bestehenden Teams aus. So führte z.B. auch der Kanton St. Gallen im Herbst 2018 ein neues Kompetenzzentrum Cybercrime ein, in welchem spezialisierte Polizisten und Staatsanwälte integriert sind.

■ **Von Fatih Aslantas, lic. iur., LL.M., Rechtsanwalt**

Möglich Formen

Doch was heisst Cybercrime eigentlich? Der Begriff findet sich im Strafgesetzbuch («StGB») freilich nicht. Auch Schlagworte wie Phishing, Grooming, Spyware, Rogueware, etc. kennt das StGB nicht. Das Bundesamt für Polizei fedpol führt auf seiner Website eine gute Übersicht über die verschiedenen Deliktsarten auf. Auf die gängigsten Begriffe möchte ich im Folgenden kurz eingehen:

Als *Pishing* wird bezeichnet, wenn die Täter durch verschiedene Tricks Passwörter in Erfahrung bringen. Auch an weiteren persönlichen Daten wie Name, Geburtstag, Anschrift oder Online-Banking-Zugangsdaten sind sie interessiert. Mit diesen Daten können sie Missbrauch betreiben und unter der Identität des Opfers Geschäfte abwickeln (Geld überweisen, Online-Einkäufe tätigen etc.).

Beim *Grooming* nehmen Erwachsene vor allem in Chatrooms Kontakt mit Minderjährigen auf. Dabei bauen sie langsam ein Vertrauensverhältnis zum Opfer auf und versuchen, an intime Details und vor allem (Nackt-)Fotos zu gelangen. So erhaltene Fotos/Filme werden anschliessend insofern missbraucht, um das Opfer zu erpressen oder zu bestimmten Handlungen zu nötigen.

Bei *Spyware* handelt es sich um Programme, die dazu eingesetzt werden, Passwörter und Zugangsdaten zu erhalten, um finanziellen oder anderen Schaden anzurichten.

Als *Cryptolocker* wird eine Schadsoftware, eine sogenannten Crypto-Ransomware, bezeichnet, die einen Computer infiziert (häufig durch das Öffnen eines E-Mail-Anhangs oder den Besuch einer infizierten Webseite) und sämtliche Daten verschlüsselt. Anschliessend werden die betroffenen Personen aufgefordert, einen bestimmten Betrag oder Bitcoins zu überweisen, um das Passwort zur Entschlüsselung zu erhalten.

Es existieren noch Dutzende weitere Beispiele, deren Aufzählung den Rahmen dieses Artikels sprengen würde.

Die Tatbestände im StGB

Die klassischen «IT-Delikte» im StGB sind die unbefugte Datenbeschaffung (Art. 143 StGB), das unbefugte Eindringen in ein Datenverarbeitungssystem (Art. 143bis StGB), die Datenbeschädigung (Art. 144bis StGB) und der betrügerische Missbrauch einer Datenverarbeitungsanlage (Art. 147 StGB).

Unbefugte Datenbeschaffung

Nach Art. 143 Abs. 1 StGB macht sich strafbar, wer in der Absicht, sich oder einen anderen unrechtmässig zu bereichern, sich oder einem anderen elektronisch oder in vergleichbarer Weise gespeicherte oder übermittelte Daten beschafft, die nicht für ihn bestimmt und gegen seinen unbefugten Zugriff besonders gesichert sind.

Mit Daten sind Informationen gemeint, die von einer Datenverarbeitungsanlage (Computer, Tablet, Handy etc.) durch entsprechende Programme entgegengenommen, automatisch bearbeitet und wieder abgegeben werden.

Unter den Begriff in *vergleichbarer Weise gespeicherte oder übermittelte Daten* fallen z.B. die optische Speicherung mittels Lasertechnik auf CD. Damit soll der Tatbestand auch mit der elektronischen Methode vergleichbare technische Verfahren erfassen.

Die Daten müssen gegen den *unbefugten Zugriff* des Täters besonders geschützt sein, wie dies z.B. bei Zugangscodes, Verschlüsselung etc. der Fall ist. Wenn jemand einfach seinen PC offen lässt und ein Dritter sich so Zugang zu Daten verschafft, macht sich Letzterer nicht strafbar.

Die tatbestandmässige Handlung besteht darin, wenn der Täter eine Art Gewahrsam der Daten erhält (wie z.B. Kopieren auf CD/USB-Stick) bzw. er mit den Daten «arbeitet» (z.B. Einlesen mit eigener Einrichtung). Blosse Kenntnisnahme genügt jedoch nicht.

Die Tat wird von Amts wegen verfolgt (Offizialdelikt). Eine unbefugte Datenbeschaffung zum Nachteil eines Angehörigen oder Familiengenossen wird nur auf Antrag verfolgt.

Eindringen in ein Datenverarbeitungssystem

Dieser Tatbestand ist in Art. 143bis StGB festgehalten. Er will Datenverarbeitungssysteme (wie z.B. PCs, Laptops wohl auch Tablets und Handys) – nicht aber die darin gespeicherten Daten – schützen.

Nach Abs. 1 der Bestimmung macht sich strafbar, wer unbefugterweise in ein solches System eindringt. Damit der Tatbestand erfüllt wird, muss der Täter auf dem Weg einer Datenübertragungseinrichtung eindringen. Die Bestrafung erfolgt auf Antrag.

Gemäss Abs. 2 macht sich strafbar, wer Zugangscodes, Daten oder Programme in Verkehr bringt oder zugänglich macht, von denen er weiss oder annehmen muss, dass sie für ein unbefugtes Eindringen in ein Datenverarbeitungssysten verwendet werden sollen. Es handelt sich dabei um ein Offizialdelikt.

Datenbeschädigung

Der Tatbestand von Art. 144bis Abs. 1 StGB bezweckt den Schutz von Daten. Tathandlung ist das Verändern, Löschen oder Unbrauchbarmachen (z.B. durch unbefugte Verschlüsselung) von Daten. Es handelt sich um ein Antragsdelikt, wobei bei grossem Schaden (üblicherweise ab CHF 10 000.–) die Tat von Amts wegen verfolgt wird.

Nach Abs. 2 macht sich strafbar, wer Programme herstellt, einführt oder in Verkehr bringt, anpreist, anbietet oder sonst wie zugänglich macht, von denen er weiss oder an-

nehmen muss, dass sie für die illegale Datenbeschädigung verwendet werden sollen. Es handelt sich dabei um ein Offizialdelikt.

Betrügerischer Missbrauch einer Datenverarbeitungsanlage

Art. 147 StGB ergänzt den bekannten Straftatbestand des Betrugs (Art. 146 StGB) insofern, als dass auch eine Verschiebung von Vermögenswerten durch Manipulation an oder mit Daten strafbar ist, ohne dass ein Mensch irregeführt werden muss, wie es beim klassischen Betrug nötig ist. Die tatbestandmässige Handlung liegt in der Einwirkung auf einen Datenverarbeitungs- oder -übermittlungsvorgang durch Missbräuche wie eine unrichtige, unvollständige oder unbefugte Verwendung von Daten. Mit der Tatbestandsvariante «Einwirkung in vergleichbarer Weise» sollen technisch noch nicht bekannte Missbräuche erfasst werden, aber auch Manipulationen an Hardware.

Gefordert wird eine Vermögensverschiebung (z.B. Belastung eines Kontos) durch eine oben erwähnte Missbrauchshandlung.

Es handelt sich um ein Offizialdelikt. Handlungen zum Nachteil eines Angehörigen oder Familiengenossen werden hingegen nur auf Antrag verfolgt.

Weitere Delikte

Da die heutige Technik als gängiges Kommunikationsmittel verwendet wird, kommen folglich auch sämtliche Tatbestände zum Tragen, bei denen die entsprechenden Äusserungen strafrechtlich relevant sind. So kann z.B. eine Erpressung (Art. 156 StGB), Drohung (Art. 180 StGB), Nötigung (Art. 181 StGB), Ehrverletzung (Art. 173 ff. StGB) usw. über E-Mail, Chat, SMS, Social Media etc. erfolgen. Auch der Tatbestand des Betrugs (Art. 146 StGB) kommt infrage, so z.B. beim Einsatz von Rogueware, wo falsche Antivirenprogramme das Opfer warnen, dass sein Computer infiziert sei und eine zusätzliche Software gekauft werden müsse. Zudem kann mit den fraglichen Delikten auch der Tatbestand der Geldwäscherei (Art. 305bis StGB) erfüllt werden.

Schliesslich stehen auch die Sexualdelikte im Vordergrund. Dabei können die Tatbestände der sexuellen Belästigung (Art. 198 StGB) – wobei es sich hierbei um eine Übertretung und ein Antragsdelikt handelt – und der sexuellen Handlungen mit Kindern (Art. 187 StGB) vorliegen.

Zuletzt ist auch der Tatbestand der verbotenen Pornografie (Art. 197 StGB) zu erwähnen. In letzter Zeit konnte in der Presse entnommen werden, wonach vermehrt Personen wegen des Versendens vermeintlicher «Jux-Videos» per Handy, die sexuelle Handlungen mit Kindern, Tieren oder Gewalttätigkeiten enthielten, Ärger mit der Justiz bekommen hätten und bestraft wurden.

Cybercrime ist ein vielschichtiger Begriff. Genauso vielfältig sind die infrage kommenden Straftatbestände.

AUTOR

Fatih Aslantas, lic. iur., LL.M., Rechtsanwalt ist Partner in der Anwaltskanzlei Forrer Lenherr Bögli & Partner Rechtsanwälte mit Büros in Weinfelden (TG) und Rickenbach b. Wil (TG). Er berät vornehmlich KMU im Wirtschaftsrecht und ist darüber hinaus auch als Strafverteidiger tätig.