



Cybercrime im weiteren Sinne: Internetbetrug stellt nahezu die Hälfte aller Cybercrime-Anzeigen 2021 dar.

Erneuter Anstieg von Cybercrime

Die Zahl der Cybercrime-Delikte stieg 2021 um 28,6 Prozent. Durch die Covid-19-Pandemie wurden Phishing, Malspam und Ransomware begünstigt. Die Aufklärungsquote wurde auf 36,9 Prozent gesteigert.

Die Zahl der Cybercrime-Delikte steigt Jahr für Jahr an. Ob durch Hacking, Datenbeschädigung, Betrugsdelikte, Drogenhandel im Darknet oder Online-Kindesmissbrauch sowie Cybergrooming oder Cybermobbing – die Delikte sind vielfältig und durch die Digitalisierung werden innerhalb kurzer Zeit mit wenig Aufwand viele Opfer erreicht. Für die Polizei stellen vor allem der Internetbetrug, Angriffe mit Schadsoftware und Erpressungsversuche große Herausforderungen dar.

Anzeigen. Laut Cybercrime-Report des Bundeskriminalamts stieg 2021 die Zahl der angezeigten Cybercrime-Fälle innerhalb eines Jahres um 28,6 Prozent von 35.915 im Jahr 2020 auf 46.179 Anzeigen. Die Aufklärungsquote wurde um 3,4 Prozentpunkte auf 36,9 Prozent angehoben. 2021 wurden 5.000 Delikte mehr von der Polizei aufgeklärt.

Cybercrime im engeren Sinne. Das Bundeskriminalamt unterteilt Cybercrime in zwei große Bereiche: Cybercrime im engeren Sinne und im weiteren Sinne. Unter Ersterem werden Angriffe auf Daten oder Computersysteme verstanden, die unter der Verwendung der Informations- und Kommunikationstechnik (IKT) stattfinden. Darunter fallen Straftaten, die sich gegen Netzwerke oder gegen Geräte, Dienste oder Daten in diesen Netzwerken richten, wie etwa Datenbeschädigung, Hacking oder DDoS-Attacken (Distributed Denial of Service). Im Vergleich zum Vorjahr wurden hier 19,9 Prozent mehr angezeigte Straftaten verzeichnet (2021: 15.484).

Die häufigste Deliktsform war, wie im Vorjahr auch, der betrügerische Datenverarbeitungsmissbrauch mit 12.701 angezeigten Fällen. Um 52,5 Prozent stieg die Zahl der Anzeigen wegen

Missbrauchs von Computerprogrammen und Zugangsdaten, darunter sind sämtliche Vorbereitungshandlungen für Cybercrime-Straftaten subsumiert.

Cybercrime im weiteren Sinne. Darunter werden Straftaten zusammengefasst, bei denen die IKT als Tatmittel eingesetzt wird, worunter auch die steigende Anzahl an Internetbetrugsdelikten fällt. 2021 erreichte der Internetbetrug mit 22.440 angezeigten Fällen einen neuerlichen Höchststand und stellt nahezu die Hälfte aller Cybercrime-Anzeigen dar (2020: 18.780). Doch auch die sonstige Kriminalität im Internet stieg deutlich an, was auf die Zunahme an Massenerpressungs-E-Mails und die Infizierung mit Ransomware zurückzuführen ist (2020: 4.221, 2021: 8.255). Gestiegen ist auch die Zahl der gefährlichen Drohungen und beharrlichen Verfolgungen sowie Suchtmitteldelikte



Cybercrime im engeren Sinne: Der betrügerische Datenverarbeitungsmissbrauch war die häufigste Deliktsform.

im Internet. Auch der Online-Kindesmissbrauch hat zugenommen. Wurden 2020 noch 1.702 Fälle registriert, kamen 2021 1.921 Fälle zur Anzeige. Hier konnte jedoch die Aufklärungsquote um 2,6 Prozentpunkte im Vergleich zum Vorjahr gesteigert werden.

Covid-19 und die Auswirkungen.

Auch im zweiten Pandemiejahr stieg aufgrund des veränderten Einkaufsverhaltens im Internet die Zahl der Internetbetrügereien stark an. Mit Malspam, Phishing oder Ransomware wurde in Aussendungen von Fake-Mails oder SMS mitgeteilt, dass der Verbleib einer angeblichen Pakete-Lieferung per Link nachverfolgt werden könnte. Wurde der

Link oder die Datei angehängt geöffnet, wurde jedoch eine Schadsoftware am Zielgerät installiert.

Prävention und Eigenverantwortung.

Prävention ist ein großer Eckpfeiler, wenn es darum geht, effektiv gegen Cybercrime vorzugehen. In ganz Österreich sind deshalb Präventionsbedienstete der Polizei im Einsatz und sind bei Beratungen in den Polizeiinspektionen, durch Vorträge bei Organisationen, Unternehmen, Gemeinden oder bei Elternabenden in Schulen und Kindergärten aktiv. Da es bei neu auftretenden Modi Operandi gilt, die Bevölkerung möglichst schnell davor zu warnen, informiert das Bundeskriminalamt bei Be-

kanntwerden neuer Deliktsformen auf den unterschiedlichsten Kanälen.

Neue Melde-Möglichkeit. Es gibt die Möglichkeit, Cybercrime auf der Homepage des Bundeskriminalamtes zu melden (<https://bundeskriminalamt.at/mdst/cc.aspx>). Dadurch wird eine zusätzliche Möglichkeit geboten, Hinweise und Sachverhalte rasch und unkompliziert an die Cyber-Spezialistinnen zu übermitteln. Durch diese Neuerung ist es möglich, Trends und Entwicklungen rascher zu erkennen und zu reagieren. Wer ein Cybercrime-Delikt meldet, erhält eine Eingangsbestätigung. Die Meldung selbst ersetzt keine Anzeige bei der Polizei. *Romana Tofan*

DIGITALE BEWEISSICHERUNG

Hasskommentare sichern

Der Umgangston im Internet wird rauer und durch das vermeintliche Pseudonym fällt bei einigen Userinnen und Usern die Hemmschwelle. Doch sie bedenken dabei oftmals nicht, dass sie mit Hasskommentaren oder Cybermobbing nicht nur die Grenzen der Netiquette überschreiten, sondern sich auch strafbar machen.

Hass im Netz ist keine Seltenheit und betrifft viele Userinnen und User. Um rechtliche Schritte einleiten zu können, muss alles gesichert werden. Von Postings sollten Screenshots angefertigt werden, wobei besonders

wichtig ist, dass das Datum darauf erkennbar ist. Dabei gilt es, den ganzen Thread zu dokumentieren. Das kann bei Postings mit vielen Kommentaren sehr aufwendig sein, weshalb das Startup *NetzBeweis* eine Lösung zur Verfügung stellt.

Beweismittelsicherung. *NetzBeweis* hilft Userinnen und Usern bei der Sicherung der Beweise. Hierfür bietet das Startup zwei Lösungen an: Für die Privatnutzung kostenlos über ein Webformular und für die professionelle Nutzung, etwa durch Rechtsanwältinnen und Rechtsanwälte, kostenpflichtig über die Browser Extension. Die Use-

rin oder der User kopieren den Link der zu sichernden Seite und geben ihn sowie eine E-Mail-Adresse im Webformular ein. *NetzBeweis* erstellt nun ein unveränderbares PDF, das eine elektronische Signatur und Datum aufweist.

Gesichert werden können öffentlich zugängliche Webseiten. Mit der Browser Extension können zusätzlich auch nicht öffentliche Unterhaltungen und Chats, wie etwa in *WhatsApp* oder *Facebook-Messenger-Chats* gesichert werden. Durch die Browser-Integration können die Webseiten zudem schnell und unkompliziert mit einem Klick über die Toolbar gesichert werden.

www.netzbeweis.com