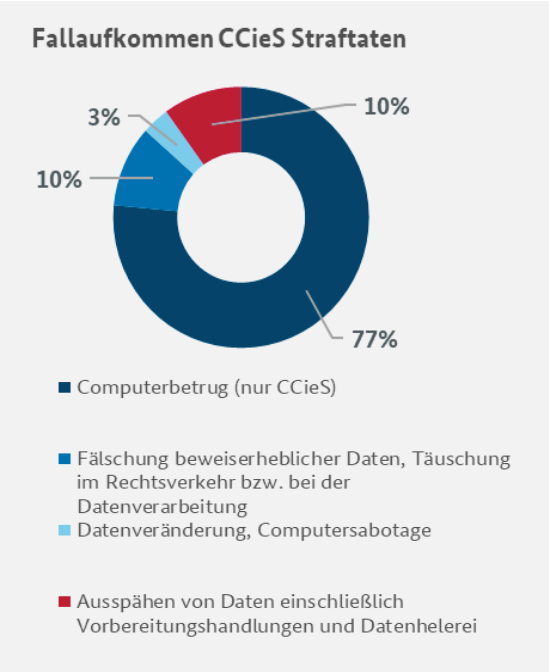
Bundeskriminalamt

BKA

FACTSHEET

Cybercrime 2020

FALLAUFKOMMEN – PKS 2020



- Die Anzahl erfasster Cyberstraftaten (Cybercrime im engeren Sinne; CCieS) ist in den letzten Jahren stetig angestiegen; so auch 2020 um 7,92 % (2020: 108.474; 2019: 100.514).
- Die Aufklärungsquote lag mit 32,6 % weiterhin auf niedrigem Niveau. Nur rund ein Drittel der angezeigten Straftaten wurde aufgeklärt.
- Die Zahl der ermittelten Tatverdächtigen stieg dagegen um 9,5 % auf 24.717 (2019: 22.574).
- Im Phänomenbereich Cybercrime ist von einem überdurchschnittlich großen Dunkelfeld auszugehen, da Straftaten hier besonders häufig nicht angezeigt werden.
- Kriminalität verlagert sich zunehmend in den digitalen Raum: 320.323 Delikte wurden 2020 unter Nutzung des Internets als Tatmittel begangen (+8,7 %; 2019: 294.665).

BEDEUTENDE PHÄNOMENBEREICHE DER CYBERCRIME

UNDERGROUND ECONOMY

- Bei der Underground Economy handelt es sich um ein international vernetztes, organisiertes, kriminelles Konstrukt, über das überwiegend illegale finanzielle Ziele bedient werden.
- Der Großteil der illegalen Marktplätze wird bestimmt durch Angebot und Nachfrage.
- Beliebteste Handelsware bleiben digitale Identitäten jeder Art – Account-Daten, Kreditkartendaten, Passwörter etc.

MAIL-SPAM UND PHISHING

- Gestohlene digitale Identitäten sind häufig Ausgangspunkt weiterer Straftaten. Um diese zu erlangen nutzen Cyberkriminelle häufig Spam- und Phishing-Mails.
- Das durchschnittliche Mail-Spam-Aufkommen ist 2020 um 17 % gestiegen (Quelle: BSI).
- Als Narrativ derartiger E-Mails diente 2020 insbesondere die Corona-Pandemie – die Täter nutzten damit das Informationsbedürfnis und die Ängste der Bevölkerung aus.

MALWARE

- Der Einsatz von Malware ist elementarer Bestandteil der CCieS – kaum eine Straftat wird ohne Malware oder missbräuchlich eingesetzte Tools begangen.
- Es kommen verschiedene Malware-Familien zur Anwendung, die jeweils unterschiedliche Funktionalitäten aufweisen (u.a. Downloader, Information-Stealer, Krypto-Miner).
- 2020 wurden ca. 1,15 Mrd. Malwarevarianten identifiziert (Quelle: AV Test), davon 137,59 Mio. neue.

RANSOMWARE

- Die Bedrohungslage durch Ransomware stieg auch 2020 weiter an. Von allen Modi Operandi im Bereich Cybercrime besitzt Ransomware das höchste Schadenspotenzial.
- Beliebte Ziele waren wirtschaftlich starke Unternehmen, Kritische Infrastrukturen und die öffentliche Verwaltung.
- Eine Infektion mit Ransomware und die Verschlüsselung von Systemen kann für Unternehmen zu massiven und kostenintensiven Geschäfts- bzw. Funktionsunterbrechungen führen und damit existenzbedrohend sein.
- Opfersysteme werden nicht mehr nur verschlüsselt, sondern parallel auch ausgespäht, um den Opfern zusätzlich mit einer möglichen Veröffentlichung von Daten drohen zu können. Dieser Modus Operandi gewinnt zunehmend an Bedeutung.
- Cyberkriminelle nutzen Ransomware organisiert und arbeitsteilig; in der Underground Economy hat sich das „Ransomware-as-a-Service“-Modell etabliert.

DDOS

- Die Anzahl an DDoS-Angriffen, insbesondere gegen Lernplattformen, Impfportale und VPN-Server, steigt weiter an. Auch die Intensität von DDoS-Angriffen nimmt zu.
- Weltweit konnten 2020 50 Mio. DDoS-Angriffe registriert werden. Das entspricht etwa 137.000 Attacken pro Tag (Quelle: Link 11/AWS). Die Corona-Pandemie spielt hierbei auch eine Rolle. Seit ihrem Beginn wurde eine Zunahme solcher Angriffe um 98 % verzeichnet.

CYBERCRIME IN ZEITEN VON CORONA

- Durch die in Folge der Pandemie stark voranschreitende Digitalisierung aller Lebensbereiche ergeben sich mehr Tatgelegenheiten für Cyberkriminelle.
- Die Täter sind flexibel und haben sich schnell angepasst, nutzen z. B. die Corona-Pandemie als Narrativ und wendet dieses auf bewährte Modi Operandi wie Spam und Phishing an.
- Vermehrt sind Angriffe auf Unternehmen und öffentliche Einrichtungen festzustellen, die für die Bekämpfung der Corona-Pandemie relevant sind. Im Fokus der Täter steht insbesondere auch die gesamte Impfstoff-Lieferkette, da ein Ausfall nur eines Unternehmens hier erhebliche Auswirkungen hätte.

GESAMTBEWERTUNG/AUSBLICK

- Cyberkriminelle sind global organisiert und agieren zunehmend professionell. Die Grenzen zwischen profitorientierten und staatlich gesteuerten Gruppierungen verschwimmen.
- Das Cybercrime-as-a-Service-Modell steigert nicht nur das informationstechnische Level durchgeführter Cyber-Straftaten, sondern eröffnet auch wenig technik-affinen Tätern den Zugang zu Cybercrime und neuen Tatgelegenheiten.
- Im Zielspektrum (professioneller) Cybertäter stehen vor allem ihnen finanziell lukrativ erscheinende Opfer aus dem Bereich der Wirtschaft. Ransomware- und DDoS-Angriffe stellen hierbei eine existentielle Bedrohung für die Wirtschaft dar.
- Die von Cyberangriffen ausgehende Gefahr ist weiterhin auf hohem Niveau, die Intensität verzeichneter Angriffe steigt stark an. Angesichts dieser Entwicklungen ist davon auszugehen, dass Cybercrime auch 2021 weiter an Relevanz gewinnen wird.
- Nur ein gemeinsames Vorgehen aller Sicherheitsbehörden, der Wirtschaft, der Wissenschaft und der Politik wird es ermöglichen, die zunehmenden Gefahren der Cybercrime abwehren und Tatverdächtige identifizieren und der Strafverfolgung zuführen zu können.