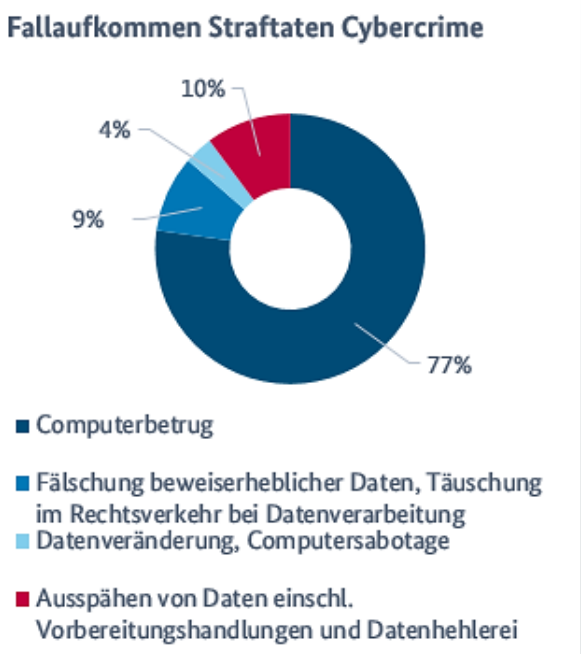
Bundeskriminalamt

BKA

FACTSHEET

Cybercrime 2021

FALLAUFKOMMEN - PKS 2021



- Die Anzahl erfasster Cyberstraftaten ist in den letzten Jahren stetig angestiegen; so auch im 2021 um 12,18% (2021: 146.363, 2020: 130.477).
- Die Aufklärungsquote lag mit 29,3% weiterhin auf einem niedrigen Niveau. Nur rund ein Drittel der angezeigten Straftaten wurden aufgeklärt.
- Im Phänomenbereich Cybercrime ist von einem überdurchschnittlich großen Dunkelfeld auszugehen, da Straftaten hier besonders häufig nicht angezeigt werden.

BEDEUTENDE PHÄNOMENBEREICHE DER CYBERCRIME

Underground Economy (UE)

- Das Angebot der UE bildet die Grundlage vieler Straftaten im Cyber-Bereich.
- Neben Cybercrime-as-a-Service-Angeboten gewannen besonders Initial Access Broker und gefälschte Covid19-Impfzertifikate an Relevanz.

Data Leaks

- Auf einschlägigen Foren und Marktplätzen der Underground Economy werden Daten, die zuvor durch einen unberechtigten Zugriff erlangt wurden, zum Kauf angeboten.
- Das Angebot umfasst Anmeldedaten, Zahlungsdaten, personenbezogene Daten etc., welche dann als „Rohstoff“ für weitere kriminelle Aktionen gehandelt werden.
- Für 2021 wurden ca. 184,65 Mio. kompromittierte Nutzerkonten erfasst. (Quelle: Hasso-Plattner-Institut)

Eintrittsvektoren - Phishing & IT-Schwachstellen/Exploits

- Klassisches Phishing gehörte auch 2021 zu den Haupteintrittsvektoren für Schadsoftware.
- Der Finanzsektor war 2021 weltweit am stärksten von Phishing betroffen. (Quelle: Anti-Phishing Working Group)
- Die Anzahl an identifizierten Phishing-Webseiten ist seit der Hochphase der Corona-Pandemie sprunghaft auf ein neues Niveau angestiegen und nimmt kontinuierlich weiter zu.
- Durch die Ausnutzung einer IT-Schwachstelle können sich Cyberkriminelle Zugänge zu Systemen verschaffen.
- 54% der in der UE verkauften Exploits wurden innerhalb der letzten zwei Jahre veröffentlicht. (Quelle: Trend Micro)

Schadprogramme - Malware & Ransomware

- Malware ist das primäre Werkzeug zur Begehung von Cyberstraftaten.
- Ransomware, Remote Access-Tools (RAT) und Info-Stealer stellen die bedeutendsten Malware-Varianten im Jahr 2021 dar.
- Das Bedrohungspotential durch Ransomware ist im Jahr 2021 nochmals deutlich angestiegen. Sie bleibt die Cyber-Bedrohung mit dem höchsten Schadenspotential.
- Ransomware verursachte einen jährlichen Schaden von ca. 24,3 Mrd. Euro. 2019 betrug diese Zahl noch 5,3 Mrd. Euro. (Quelle: Bitkom e.V.)
- Im internationalen Vergleich ist Deutschland überdurchschnittlich häufig von Ransomware-Angriffen betroffen.
- Die sog. Double Extortion, bei der Opfersysteme nicht nur verschlüsselt werden, sondern zusätzlich mit der Veröffentlichung von Daten gedroht wird, hat sich inzwischen als Standard-Modus-Operandi etabliert.

Distributed Denial of Service (DDoS)

- DDoS-Angriffe nehmen in ihrer Intensität und Komplexität weiter zu.
- 2021 kam es zu 41% mehr DDoS-Angriffen als im Vorjahr. (Quelle: Link11)
- Pro Monat wurden durchschnittlich 2335 DDoS-Angriffe registriert. (Quelle: Deutsche Telekom AG)

Bundeskriminalamt

BKA

ZIELE

- Grundsätzlich kann jede natürliche Person und jedes Unternehmen oder jede Einrichtung Ziel bzw. Opfer von Cybercrime werden. Bei Unternehmen ist dies unabhängig von der Unternehmensgröße und Branche.
- Neben Cyberangriffen auf unterschiedlichste Branchen war das Jahr 2021 u.a. geprägt von Angriffen auf KRITIS und Ziele in der öffentlichen Verwaltung.
- Die Anzahl sog. Supply-Chain-Angriffe mit nationalen und internationalen Auswirkungen ist spürbar angestiegen. Ihr enormes Bedrohungspotential entfaltet sich besonders durch die große Reichweite der Angriffe.

TÄTER

- Der Übergang zwischen finanziell und politisch motivierten Cybercrime-Gruppierungen ist hinsichtlich ihrer angestiegenen Professionalisierung und Anpassungsfähigkeit fließend. Es ist davon auszugehen, dass alle Arten von Gruppierungen über annähernd dasselbe Gefährdungspotenzial, Know-How und vergleichbare Ressourcen verfügen.

SCHÄDEN DURCH CYBERCRIME

- Cybercrime gehört zu den Phänomenbereichen mit dem höchsten Schadenspotenzial in Deutschland.
- Die Cybercrime-Schäden in Deutschland beliefen sich im Jahr 2021 auf 223,5 Mrd. Euro und haben sich damit seit 2019 mehr als verdoppelt. (Quelle: Bitkom e.V.)
- Cyber-Angriffe können vielfach zu existenzbedrohenden Notlagen führen, insbesondere für Unternehmen. Der längerfristige Ausfall staatlicher Dienstleistung kann auch spürbare Auswirkungen für die Bevölkerung mit sich bringen.

GESAMTBEWERTUNG/AUSBLICK

- Die Verzahnung internationaler Lieferketten sowie die fortschreitende Digitalisierung, u.a. auch durch die Corona-Pandemie, schafft eine Vielzahl neuer Tatgelegenheiten für Cyberkriminelle.
- Mit steigender Professionalität der Täter steigt die Anzahl erfolgreicher Angriffe und damit auch die Höhe des verursachten Schadens sowie die spürbaren Auswirkungen auf das alltägliche Leben der Bevölkerung.
- Insbesondere der Angriffskrieg Russlands gegen die Ukraine und dabei eingesetzte hybride Angriffsformen sowie Aktivitäten beteiligter Cyberakteure verdeutlichen die Auswirkungen aller Arten von Cyberangriffen, die auch über Ländergrenzen hinweg reichen.
- Eine enge und vertrauenswürdige Kooperation zwischen staatlichen Behörden und privaten Unternehmen ist die Grundvoraussetzung für eine Implementierung effektiver Maßnahmen zur Eindämmung der Cybercrime.