



Offensive Security

20.10.2025



Vorstellungsrunde

Für welches Unternehmen arbeiten Sie und hat Ihr Unternehmen eine Cybersicherheitsabteilung / einen CISO?

Warum haben Sie sich für Grundlagen der Cybersicherheit entschieden?

Welche praktische Erfahrung mit Cybersicherheit haben Sie bereits?

*Was sind Ihre **Erwartungen** an den Kurs?*



Einführung

20.10.2025



“Underground Economy”: Cybercrime-as-a-Service (CaaS)

Kriminelle Dienstleistungen und Werkzeuge werden über das Internet (z.B. Darknet, Telegram, zugangsbeschränkte Foren) angeboten und verkauft (Kryptowährung):

- Kriminelle bieten ihre Fähigkeiten, Tools oder Infrastruktur gegen Bezahlung an.
- Käufer müssen keine tiefen technischen Kenntnisse haben.
- CaaS senkt die Einstiegshürde für Cyberkriminalität erheblich.

Foren & Messenger-Server

- Digitale Treffpunkte für Austausch und Kontaktaufnahme
- „Eintrittstor“ in die Szene

Bulletproof Hosting & Proxyprovider

- Robuste Infrastruktur, die schwer abschaltbar ist
- VPNs zur Verschleierung

Marktplätze

- Automatisierte Shops für Zugangsdaten und illegale Güter
- Ähnlich wie Amazon

Malwareentwicklung & Coding

- Maßgeschneiderte Schadsoftware
- Je nach Bedarf und Budget

Crypting & Obfuscation

- Tarnung und Verschlüsselung von Malware
- Spezialisierte Dienstleister

Counter-Antivirus-Services (CAV)

- Prüfung der Malware auf Erkennbarkeit
- z.B. Antivirenprogramme

Malware Delivery & Infection on Demand

- Verbreitung der Malware
- z.B. via Phishing, Malspam oder Drive-by

Drops, Mules & Cashout

- Geldabhebung durch reale Personen
- hohes Risiko für Täter

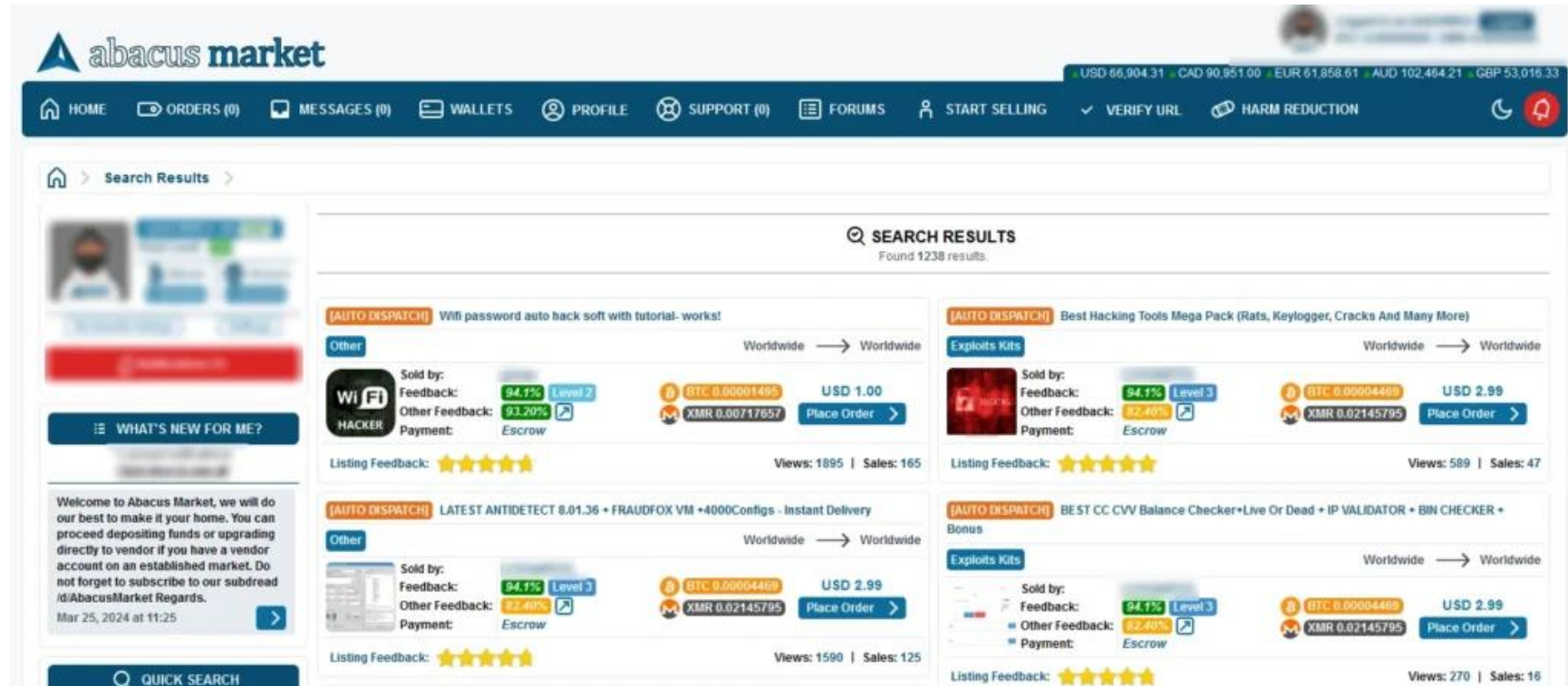
Exchanger (digitale Geldwäsche)

- Umwandlung und Verschleierung krimineller Einnahmen
- „sauberes“ Geld

BJA - Lageprodukte aus dem Bereich Cybercrime - Die Underground Economy



Beispiel: Abacus Market



Estimated transaction volume: \$15 million

Cryptocurrencies accepted: Bitcoin (BTC), Monero (XMR)

Focus: narcotics, counterfeit items, hacking tools, and stolen data

[The 10 Biggest Dark Web Markets – Most Active Illegal Marketplaces in 2025](#)



Beispiel: Russian Market



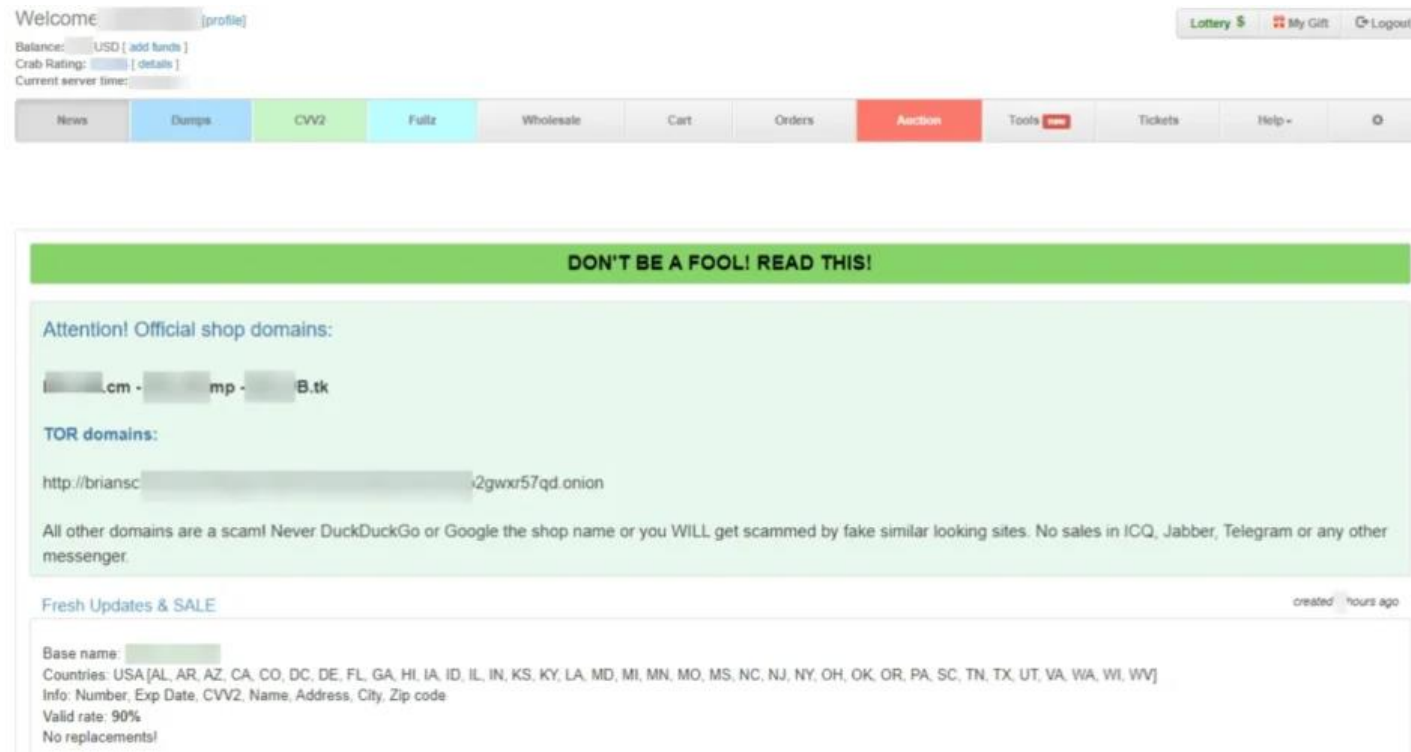
Transaction methods: Bitcoin, Litecoin, Ethereum

Focus: CVVs, RDP credentials, stealer logs, and bank info

The 10 Biggest Dark Web Markets – Most Active Illegal Marketplaces in 2025



Beispiel: BriansClub



One of the oldest (2014) dark web markets for stolen credit cards, fullz (complete identity kits), and dumps

Accepted currencies: USDT, Dash, Monero

Focus: Financial fraud, carding, identity theft

[The 10 Biggest Dark Web Markets – Most Active Illegal Marketplaces in 2025](#)



Unternehmerische Verteidigung - Offense vs. Defense Security

Offense Security

Das Ziel der offensiven Sicherheit besteht darin, reale Angriffe zu simulieren, um die Sicherheitslage eines Unternehmens zu testen:

Wer testet?

- White Hat Hacker / Ethical Hacker
- „Red Teams“

Was sind die Herausforderungen?

- Spezialisten werden benötigt (kostenintensiv)
- Rechtliche Situation muss geklärt werden

Welche Tools verwendet wie beispielsweise:

- **Kali Linux** – hunderte Tools für Penetrationstests
- **Metasploit** Framework – Plattform zum Entwickeln und Ausführen von Exploits gegen bekannte Schwachstellen
- **Wireshark** – Netzwerk-Sniffer zur Analyse von Netzwerkpaketen
- **Cobalt Strike** – Kommerzielles Red-Team-Tool für Post-Exploitation und Command & Control
- **Burp Suite** – Web-Security-Testing-Tool zur Analyse und Manipulation von HTTP/S-Verkehr
- **Nmap** – Netzwerkscanner zur Erkennung von offenen Ports und Diensten.

Defense Security

Das Ziel der defensiven Sicherheit besteht darin, Systeme, Netzwerke und Daten vor Angriffen zu schützen und Sicherheitsvorfälle frühzeitig zu erkennen und zu verhindern:

Wer schützt?

- Security Operations Center (SOC)
- „Blue Teams“
- IT-Sicherheitsbeauftragte
- IT-Teams (z.B. Administratoren)

Was sind die Herausforderungen?

- Angriffsflächen sind vielfältig und dynamisch
- Erkennung und Reaktion müssen in Echtzeit erfolgen
- Hohe Anforderungen an Monitoring und Analyse

Welche Tools werden beispielsweise verwendet:

- **Firewall** – Filtert Netzwerkverkehr basierend auf definierten Regeln
- **SIEM** (z. B. Splunk, MS Sentinel) – Zentralisiert und analysiert Logdaten zur Erkennung von Bedrohungen
- **EDR** (z. B. CrowdStrike, Trellix) – Überwacht Endgeräte auf verdächtige Aktivitäten
- **IDS/IPS** (z. B. Snort, Suricata) – Erkennt und verhindert Angriffe im Netzwerk
- **Antivirus / Anti-Malware** – Erkennt und entfernt bekannte Schadsoftware
- **Patch-Management-Tools** – Halten Systeme aktuell/schließen Sicherheitslücken
- **Vulnerability Scanner** (z.B. Qualys, Nessus) – Automatisierte Schwachstellenanalyse zur Identifikation und Priorisierung von Sicherheitslücken



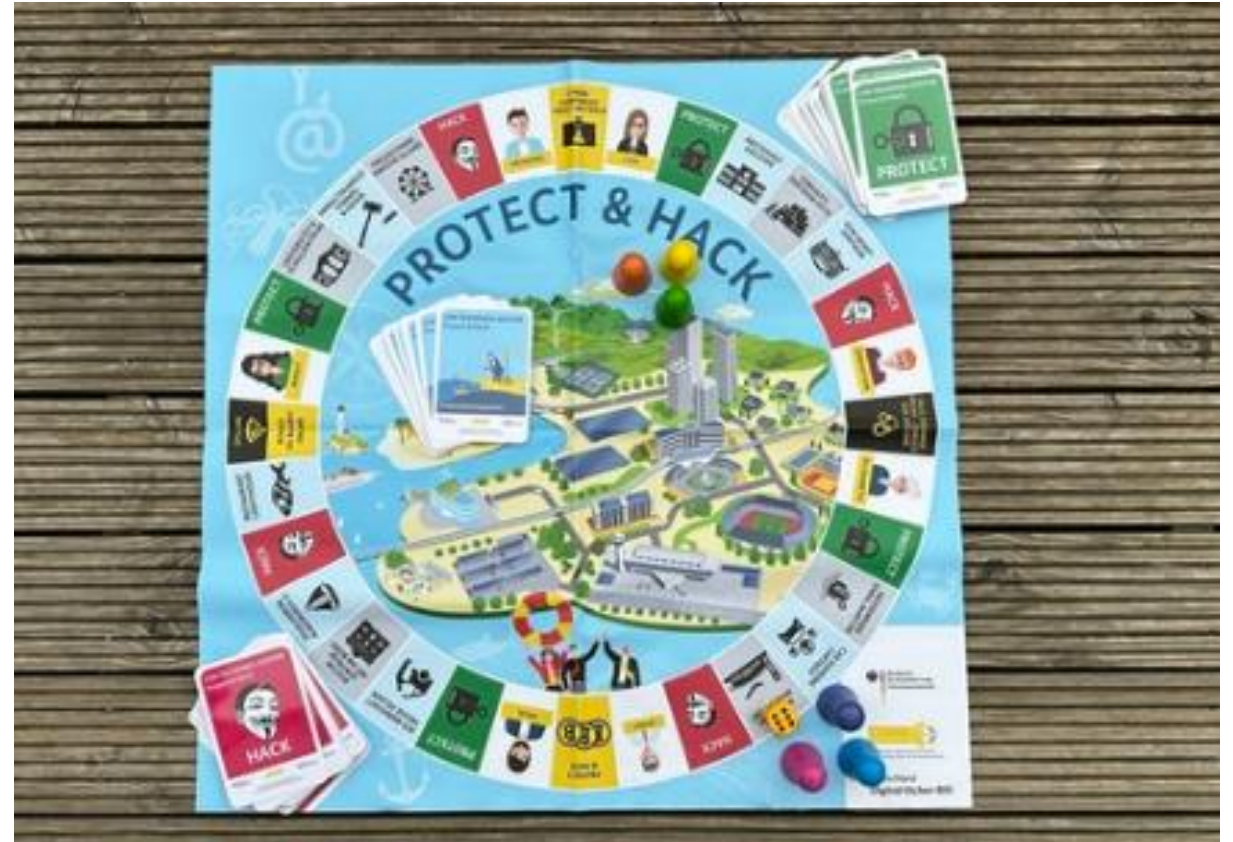
Gruppenarbeit 1: Protect & Hack - 45 min

20.10.2025



Gruppenarbeit 1: Brettspiel Protect & Hack

- Finden Sie sich in 6 Gruppen mit je 5 Studierenden zusammen.
- Lesen Sie die Spielanleitung
- Spielen Sie das Spiel ca. **45 min.**



Gruppenarbeit 2: Angriffsmetho- den - 25 min

20.10.2025

Gruppe 1: DoS/DDoS (Denial of Service / Distributed Denial of Service)

Kernfragen:

- Was ist der Unterschied zwischen einem DoS- und einem DDoS-Angriff?
- Welche Arten von DDoS-Angriffen gibt es (z. B. Volumen-, Protokoll-, Applikationsangriffe)?
- Was ist ein Botnetz und welche Rolle spielt es bei DDoS-Angriffen?
- Welche Beispiele für bekannte Angriffe gab es in den letzten Jahren?



Gruppe 2: Malware & Ransomware

Kernfragen:

- Was versteht man unter Malware? Welche Arten gibt es?
- Wie verbreitet sich Malware typischerweise?
- Welche Rolle spielen Exploits und Schwachstellen bei der Verbreitung von Malware?
- Welche bekannten Ransomware-Angriffe gab es in den letzten Jahren?
- Sollte man Lösegeld zahlen, wenn wichtige Daten verschlüsselt wurden?



Gruppe 3: Social Engineering & Phishing (inkl. Business E-Mail Compromise)

Kernfragen:

- Welche psychologischen Prinzipien nutzen Angreifer beim Social Engineering?
- Was ist Phishing und wie hängt es mit Social Engineering zusammen?
- Welche verschiedenen Arten von Phishing gibt es (z. B. Spear Phishing, Whaling, Smishing, Vishing)?
- Welche bekannten Social-Engineering-Angriffe gab es in den letzten Jahren?



Gruppe 4: Passwort Attacken & Brute Force Attacken

Kernfragen:

- Was versteht man unter einer Passwort-Attacke?
- Was ist ein Brute-Force-Angriff und wie funktioniert er?
- Welche anderen Arten von Passwort-Angriffen gibt es (z. B. Dictionary Attack, Credential Stuffing, Rainbow Tables)?
- Wie unterscheiden sich Brute-Force- und Dictionary-Angriffe technisch?
- Wie funktionieren Passkeys?



Gruppe 5: Schwachstellenausnutzung

Kernfragen:

- Was versteht man unter einer Schwachstelle in der IT-Sicherheit?
- Was ist der Unterschied zwischen einer bekannten und einer Zero-Day-Schwachstelle?
- Welche Rolle spielen CVEs (Common Vulnerabilities and Exposures) bei der Klassifizierung von Schwachstellen?
- Wobei handelt es sich bei Bug-Bounty-Programmen?
- Erläutere zwei bekannte Schwachstellen aus der Vergangenheit



Gruppe 6: Angriffe auf Webanwendungen

Kernfragen:

- Warum sind Webanwendungen ein beliebtes Ziel für Angreifer?
- Welche typischen Schwachstellen gibt es in Webanwendungen?
- Was ist ein SQL-Injection-Angriff und wie funktioniert er?
- Was versteht man unter Cross-Site Scripting (XSS)?
- Was ist ein Remote Code Execution (RCE) Angriff?
- Welche Beispiele aus der Praxis existieren?



Arbeitsblatt: Cyber Kill Chain – 10 min

20.10.2025



Cyber Kill Chain

Was ist eine Advances Persistent Threat (APT)?

Wie gehen Angreifer im laut Cyber Kill Chain vor?

Welche bekannten APT-Gruppen gibt es?



Übung: Moniker Link – 20 min

20.10.2025



Exploitation Basics

1. Erstellen Sie einen kostenlosen Account bei TryHackMe (THM)
2. Schreiben Sie sich für Cyber Security 101 ein
3. Absolvieren Sie das Modul “Moniker Link” in den Exploitation Basics



<https://tryhackme.com>



Arbeitsblatt: Hacking Tools – 10 min

20.10.2025



Gruppenarbeit 3: Hacker- paragraph - 20 min

20.10.2025

Der “Hackerparagraph” – 202c Strafgesetzbuch (StGB)

§ 202 Verletzung des Briefgeheimnisses

(1) Wer unbefugt

1. einen verschlossenen Brief oder ein anderes verschlossenes Schriftstück, die nicht zu seiner Kenntnis bestimmt sind, öffnet oder
2. sich vom Inhalt eines solchen Schriftstücks ohne Öffnung des Verschlusses unter Anwendung technischer Mittel Kenntnis verschafft, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, wenn die Tat nicht in § 206 mit Strafe bedroht ist.

(2) Ebenso wird bestraft, wer sich unbefugt vom Inhalt eines Schriftstücks, das nicht zu seiner Kenntnis bestimmt und durch ein verschlossenes Behältnis gegen Kenntnisnahme besonders gesichert ist, Kenntnis verschafft, nachdem er dazu das Behältnis geöffnet hat.

(3) Einem Schriftstück im Sinne der Absätze 1 und 2 steht eine Abbildung gleich.

§ 202a Ausspähen von Daten

(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.



Der “Hackerparagraph” – 202c Strafgesetzbuch (StGB)

§ 202b Abfangen von Daten

Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

§ 202c Vorbereiten des Ausspähens und Abfangens von Daten

(1) Wer eine Straftat nach § 202a oder § 202b **vorbereitet**, indem er

1. **Passwörter oder sonstige Sicherungscodes**, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder
2. **Computerprogramme**, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) § 149 Abs. 2 und 3 gilt entsprechend.



Der “Hackerparagraph” – 202c Strafgesetzbuch (StGB)

§ 202d Datenhehlerei

(1) Wer **Daten** (§ 202a Absatz 2), die **nicht allgemein zugänglich** sind und die ein anderer durch eine rechtswidrige Tat erlangt hat, sich oder einem anderen **verschafft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, um sich oder einen Dritten zu bereichern oder einen anderen zu schädigen**, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Die Strafe darf nicht schwerer sein als die für die Vortat angedrohte Strafe.

(3) Absatz 1 gilt nicht für Handlungen, die ausschließlich der **Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten** dienen. Dazu gehören insbesondere

1. solche Handlungen von **Amtsträgern oder deren Beauftragten**, mit denen Daten ausschließlich der Verwertung in einem Besteuerungsverfahren, einem Strafverfahren oder einem Ordnungswidrigkeitenverfahren zugeführt werden sollen, sowie
2. solche **beruflichen Handlungen** der in § 53 Absatz 1 Satz 1 Nummer 5 der Strafprozessordnung genannten Personen, mit denen Daten entgegengenommen, ausgewertet oder veröffentlicht werden.



Gruppenarbeit 3: Bekannte Urteile zum “Hackerparagraphen”

Geben Sie den Studierenden eine Zusammenfassung folgender Urteile:

Gruppe 1: **BVerfG, Beschluss vom 18.05.2009 - 2 BvR 2233/07**

Gruppe 2: **AG Berlin-Tiergarten, 16.01.2017 - 327 Ds 44/16**

Gruppe 3: **Modern-Solution-Prozess / Hendrik Heinle (2023-2025)**

Gruppe 4: **Fall der Sicherheitsforscherin Lillith Wittmann (2021)**

Gruppe 5: **BGH, 13.05.2020 - 5 StR 614/19**

Gruppe 6: **BGH, Urteil vom 21.07.2015 – 1 StR 16/15**



Arbeitsblatt: Schwachstellen – 10 min

20.10.2025

