Deutsche Stiftung für Recht und Informatik

STRAFBARKEIT VON WHITE-HAT-HACKING IN DEUTSCHLAND UND EUROPA

Alexander Weiss / Johannes Zwerschke, LL.M.
Piltz Legal (Berlin)

Herbstakademie 2024

Ethical / White-Hat-Hacking

Abgrenzung White- / Grey- / Black-Hat-Hacker

- Keine verbindliche Terminologie
- Abgrenzung i.d.R. anhand der Ziele & Methoden

Ethical / White-Hat-Hacker

- Tätigkeit: Penetrationstests und andere Testmethoden
- Ziel: Überprüfung der Sicherheit von IT-Systemen

Rechtliche Differenzierung?

- Auch White-Hat-Hacking strafrechtlich relevant
- Beispiel: Aktuelles Verfahren vor dem AG Jülich (17 Cs-230 Js 99/21-55/23) / LG Aachen (60 Qs 16/23)

Verfahren vor dem AG Jülich / LG Aachen

Sachverhalt

- Software für ein Warenwirtschaftssystem
- Datensätze von bis zu 700.000 Endkunden auf dem Server
- Auslesen des Passworts im Quellcode mittels eines Decompilers; dadurch Zugang zu Kundendaten
- Weitergabe von Informationen über die Schwachstelle an einen Blogbetreiber
- Information auch an das Unternehmen mit Fristsetzung

Verfahren

- Strafbefehl der StA Köln
- Abgelehnt vom AG Jülich da kein hinreichender Tatverdacht
- Sofortige Beschwerde der StA Köln beim LG Aachen (erfolgreich)
- Verurteilung durch LG Jülich (Geldstrafe i.H.v. 3.500 EUR)

§ 202a StGB: Rechtliche Erwägungen

§ 202a StGB: Rechtliche Erwägungen

Datenbegriff

- Informationen, die in einer für eine Datenverarbeitungsanlage erkennbaren Form codiert sind
- Weite Auslegung des Datenbegriffs
- Passwort oder die erlangten Daten?

„Nicht für den Täter bestimmt“

- Die Daten sollen „nach dem Willen des Berechtigten nicht in den Herrschaftsbereich des Täters gelangen“
- Also: ohne Zugangserlaubnis
- Ob Daten allgemein zugänglich, ist irrelevant

§ 202a StGB: Rechtliche Erwägungen

Besondere Sicherung

- Vorkehrungen, die den Zugriff ausschließen oder nicht unerheblich erschweren
- Mechanische Schließeinrichtungen, technische Vorkehrungen etc.
- Nicht: Vorkehrungen, die anderen Zwecken dienen
- Folge: Passwortschutz nicht automatisch besondere Sicherung gegen unberechtigten Zugang
- Mangelnde Sicherung schließt die Strafbarkeit aus

§ 202a StGB: Rechtliche Erwägungen

Zugangsverschaffung durch Überwindung der Zugangssicherung

- „Durchbrechung des Schutzes“
- Abstrakt-generelle Betrachtungsweise
- Spezialkenntnisse des Täters nicht berücksichtigungsfähig
- Stellt das Auslesen des Passworts nach Dekompilierung eine Überwindung der Zugangssicherung dar?
  - AG Jülich*: Nein, da Dekompilierung mit gängigem Hilfsprogramm für jedermann möglich
  - LG Aachen: Ja, da Daten nicht für jedermann abgreifbar, sondern hier nur wegen besonderer Kenntnisse

* gemeint ist das Strafbefehlsverfahren vor dem AG Jülich und der Beschluss vom 10.05.2023 – 17 Cs-230 Js 99/21-55/23

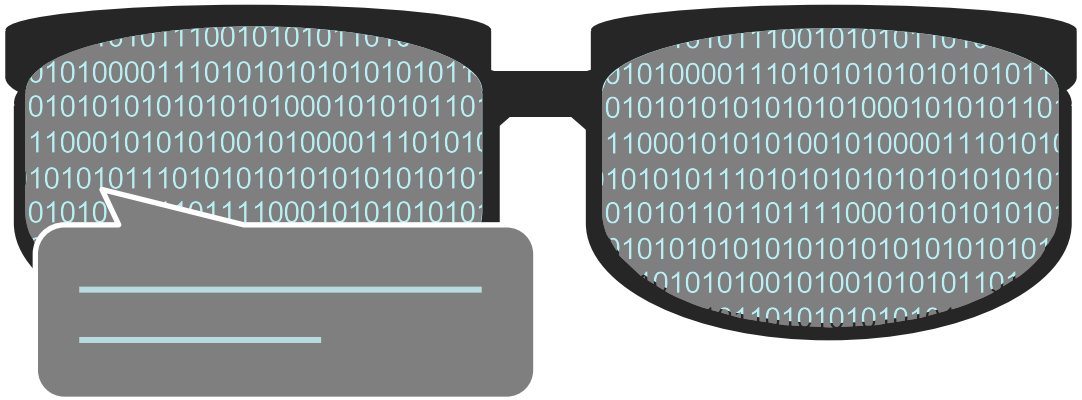
Unbefugtheit

- Nicht durch Gesetz oder Einwilligung gerechtfertigt
- Nachträgliches Einverständnis reicht nicht aus

§ 202a StGB: Rechtliche Erwägungen

Subjektiver Tatbestand

- Bedingter Vorsatz reicht
- Irrige Annahme der Berechtigung führt zu § 17 StGB
- Also: auch bei einem White-Hat-Hacker Vorsatz i.d.R. unproblematisch



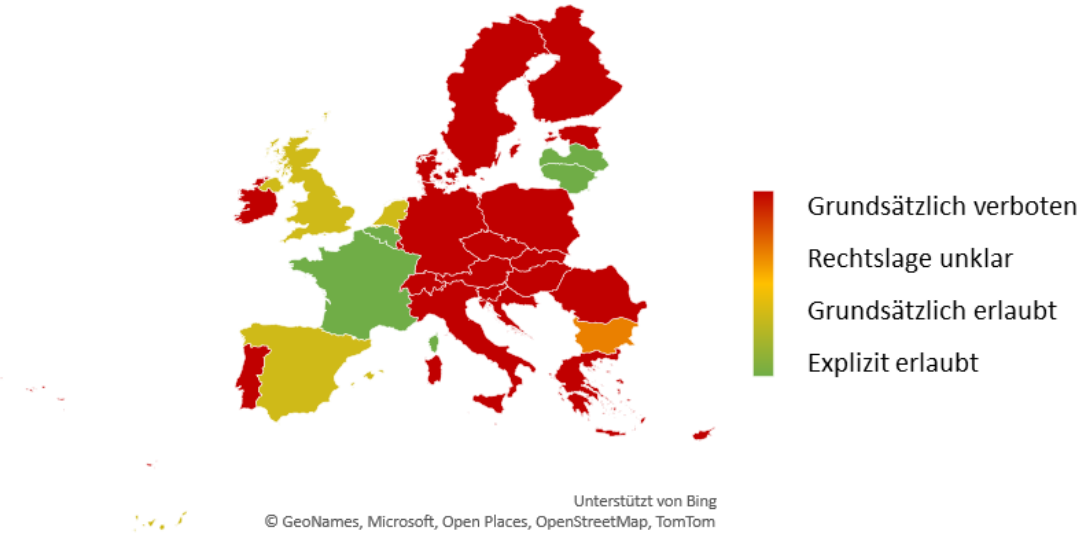
§ 202a StGB: Rechtliche Erwägungen

Ausschluss der Strafbarkeit nach § 34 StGB?

- Dauergefahr aufgrund von Sicherheitslücken
- Problem: Eintritt eines Schadens nicht immer ernstlich zu befürchten
- Unter Umständen kommen auch mildere Mittel in Betracht
- Interessenabwägung mit dem Rechtsgut der Integrität der IT-Systeme
- Kenntnis der Notstandslage vorausgesetzt
- Problem: Suche nach Schwachstellen vs. konkrete Kenntnis
- Folge: Rechtfertigender Notstand nicht per se eine Rechtfertigung für White-Hat-Hacker

Rechtslage in Europa

- Gemischtes Bild bzgl. Strafbarkeit von White-Hat-Hacking
- In vielen Staaten CVD-Policies in Planung
- CVD-Policies auch im CRA erwähnt
- Ähnliche Empfehlung in der NIS-2-Richtlinie
- Aber: nur unverbindlich



Rechtslage in Europa

Belgien

- Art. 49 Abs. 2 Klokkenluiderswet:
- *„…Unbeschadet der Anwendung des Gesetzes vom 28. November 2022 über den Schutz von Personen, die Verstöße gegen das Unionsrecht oder das nationale Recht melden, die bei einer juristischen Person des Privatsektors festgestellt wurden,* ***kann jede natürliche oder juristische Person dem nationalen CSIRT das Vorhandensein einer potenziellen Schwachstelle im Sinne von Artikel 6, 34° melden.*** *Diese Bestimmung berührt auch nicht die gesetzlichen Bestimmungen über den Schutz von Personen, die Verstöße gegen das Unionsrecht oder das nationale Recht melden, die bei einer Rechtsperson des öffentlichen Sektors festgestellt wurden. …“*

Frankreich

- Gesetzliche Ausnahmeregelung zum Art. 40 Code de Procedure Penale
- Also: „Absehen von der Verfolgung“
- Voraussetzungen:
  - Handeln im guten Glauben („bonne foi“)
  - Meldung ausschließlich an die Nationale Agentur für Sicherheit von Informationssystemen ANSSI

Rechtslage in Europa

Lettland

- Voraussetzung für Strafbarkeit: substantieller Schaden (ab 2.500 / 5.000 EUR)
- Keine einheitliche CVD-Policy
- Unternehmen und öffentliche Stellen dürfen aber eigene Policies haben

Litauen

- Hacking straflos, wenn diese Kriterien erfüllt:
  - Wahrung der Integrität des Systems
  - Keine exzessiven Maßnahmen
  - Meldung
  - Vertraulichkeit

Rechtslage in Europa

Niederlande

- StA *kann* von der Verfolgung absehen
- Berücksichtigt werden folgende Aspekte:
  - Handelt der Hacker im Interesse der Gesellschaft?
  - Sind die eingesetzten Mittel verhältnismäßig?
  - Gab es mildere Mittel?
- Brute-Force-Angriffe; unterlassene Meldung oder zu langes Warten vor der Meldung führen ggf. zur Strafbarkeit

UK

- Öffentliche Stellen und Unternehmen des Privatsektors haben eigene CVD-Policies
- National Cyber Security Centre (NCSC) stellt ein Vulnerability Disclosure Toolkit sowie Guidelines für Reporting zur Verfügung

Fazit

- Rechtlich fragmentiertes und unklares Bild in Europa
- Strafrechtliche Verfolgung bleibt in Deutschland ein Risiko
- Aber: Argumentationsansätze für Straflosigkeit vorhanden
- Lösung auf Rechtfertigungsebene in DE eher schwer denkbar, Anpassung des Tatbestands von § 202a StGB am rechtssichersten
- Einwilligung des Systemeigentümers derzeit sichere Lösung
- Reformbedarf – auch durch Bundesregierung erkannt