Deutsche Stiftung für Recht und Informatik

Vom Hörsaal in den Gerichtssaal

IT-Sicherheitsforschung als rechtliches Risiko

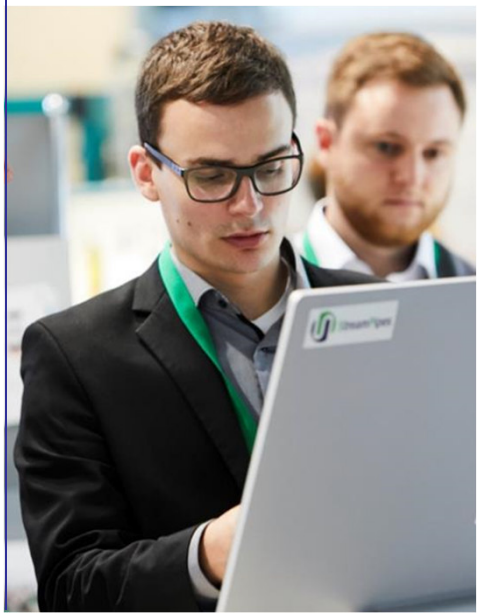
Dr. Manuela Wagner, Daniel Vonderau
FZI Forschungszentrum Informatik

Herbstakademie 2020

Fahrplan

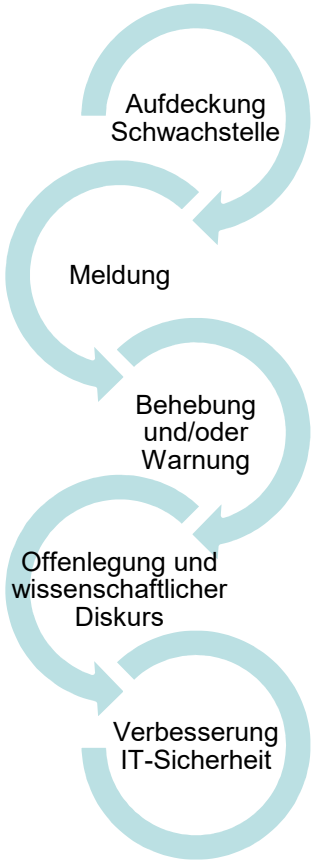
1. Einleitung
2. Überblick über die Rechtslage
3. Mitigationsmöglichkeiten
4. Reformvorschläge
5. Fazit

Einleitung



IT-Sicherheitsforschung als wesentlicher Beitrag für die Sicherheitspraxis

- Forscherinnen
  - untersuchen u.a. Produkte und Systeme auf Sicherheitslücken und konzeptionelle Sicherheitsmängel,
  - melden Funde den Produkt-/Systemverantwortlichen,
  - informieren die Öffentlichkeit zum Schutz der Produktnutzenden,
  - veröffentlichen Erkenntnisse im wissenschaftlichen Fachdialog,
  - erforschen/entwickeln neue Schutzkonzepte



Problem der rechtlichen Legitimation

- Rechtliche Einordnung der Forschungstätigkeit
  - Haftungsrisiken:
    - Verletzung von Urheberrechten bei der Untersuchung von Computerprogrammen
    - Veröffentlichung sensibler Information
  - Strafbarkeitsrisiken
    - Ausspähen / Abfangen von Daten
    - Datenveränderung / Computersabotage
- Wann wird der Graubereich zum verbotenen Tun?

Forschungstätigkeit

- Forscherinnen analysieren Computerprogramme:
  - Dabei **vervielfältigen** sie das Programm und übertragen es in Testumgebungen (z.B. sog. Code Emulation)
  - **Übersetzen** Maschinencode in menschlich verständliche Sprache (sog. Disassemblieren bzw. Dekompilieren)
  - **Umgehen** technische (Kopier-)Schutzmaßnahmen
- Forscherinnen „hacken“ Systeme:
  - **Überwinden** Zugangssicherungen und **verschaffen** sich **Zugang** zu Daten
  - Untersuchen **elektromagnetische Abstrahlung** einer Datenverarbeitungsanlage
  - Analysieren öffentliche/nichtöffentliche **Datenübermittlungen**
  - **Unterdrücken** oder **Verändern** Daten

Forschung und Urheberrecht

- Computerprogramme i.d.R. schutzfähig („kleine Münze“)
- Vervielfältigen, Übersetzen u.a. Umarbeitungen, Verbreitung und öffentliche Wiedergabe zustimmungsbedürftig
  - § 69d erlaubt **Fehlerberichtigung:** Suche nach einem unbekannten Fehler im Wege einer Analyse umfasst?
  - § 69d Abs. 3 UrhG erlaubt lediglich passive Formen des **Beobachtens, Untersuchens und Testens** von geschützten Programmen (nicht Reverse Engineering)
  - **Dekompilieren** nach § 69e UrhG gesperrt?
  - Verweis auf Lizenzierungsmöglichkeit geht ins Leere
  - Dagegen: Hardwaretests können auf § 11 Nr. 2 PatG sowie die Erlaubnis des Reverse Engineerings in § 3 Abs. 1 Nr. 2 GeschGehG gestützt werden

Forschung und Strafrecht

- § § 202a ff., 303a f. StGB schützen sog. Datenverfügungsberechtigen
- IT-Strafrecht differenziert aktuell nicht immer nach verfolgten Absichten
- Forschungsprivilegierung wie in § 201a Abs. 4 StGB oder aus der DSGVO fehlt
  - Rückgriff auf Gesetzesbegründung, die zum einen „beschwichtigt“ aber auch davon ausgeht, dass „ethische Hackerinnen“ über eine Einwilligung / Einverständnis der Berechtigten verfügen müssten
  - Umkehrschluss Verbot proaktiver Tests?

Folgen für redliche, wissenschaftlichen Forschung

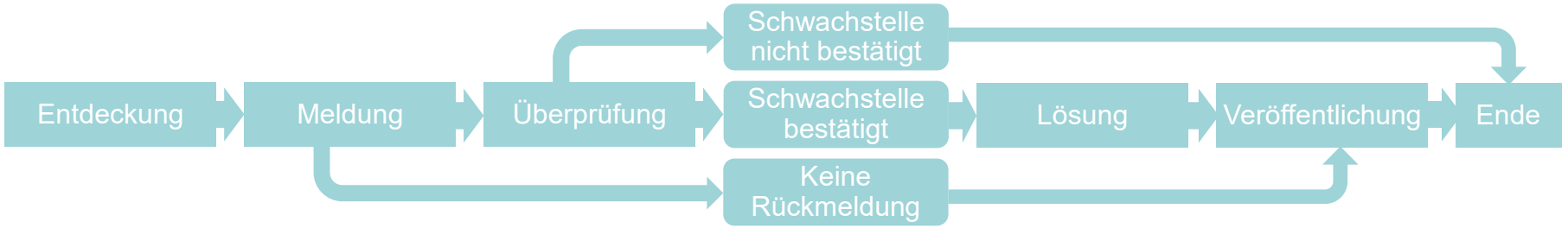
- Feststellung der Rechtswidrigkeit eines Forschungsvorhabens kann zu Abbruch des Vorhabens führen
  - Wissenschaftliche Redlichkeit geht über die Einhaltung rechtlicher Verpflichtungen hinaus und umfasst ebenfalls die Verpflichtung, bei der jeweiligen Tätigkeit auftretende Risiken zu erkennen und zu bewerten
  - Forschungseinrichtungen sollen als Kompensat für staatliche Fremdkontrolle Organe bereit stellen, die Anhaltspunkten der Gefährdung verfassungsrechtlich geschützter Güter anderer nachgehen und Maßnahmen ergreifen können

Mitigationsmöglichkeiten

- **Compliance Prozesse**
  - Vorgelagertes Prüfverfahren einrichten
    - Prozessschritte definieren, bevor ein Forschungsvorhaben beginnen darf
    - Risikomatrix für Bewertung von Haftungs- und Strafbarkeitsrisiken
  - Expertinnen integrieren
    - Auswertung rechtlicher Risiken und technischer Möglichkeiten
  - Flankierend: Verankerung in Richtlinien und Policys
    - Veröffentlichung einer Disclosure Policy um Transparenz und Nachvollziehbarkeit der Prozesse sicherzustellen

Mitigationsmöglichkeiten

- **Coordinated bzw. Responsible Disclosure Policy**
  - Verschiedene Disclosure Modelle (Full, Non, Limited, Coordinated/Responsible) mit unterschiedlichen Ergebnissen



  - Diametrale Interessen der Beteiligten? Gemeinsame Ziel: von Sicherheitslücken ausgehende Risiken zu verringern sowie Schadens- und Kostenminimierung
  - Coordinated Vulnerability Disclosure (CVD) als Mittelweg für den größtmöglichen Interessenausgleich aller Beteiligten
  - Über weitere Verbreitung und Standardisierung kann Akzeptanz steigen: verankert im europäischen Standard EN 303 645 für IoT (aus Anbietersicht: ISO/IEC 30111, ISO/IEC 29147:2018)

Mitigationsmöglichkeiten

- **Orientierung an Leitprinzipien**
  - Bisher keine Kasuistik zur IT-Sicherheitsforschung (Ausnahme § 202c StGB, „Hackerparagraph“)
  - Kein Vorgehen abseits der Einwilligung in Deutschland bekannt
  - Parameter für „Ethisches Hacken“ in den Niederlanden als Vorbild:
    - Öffentliches Interesse
    - Verhältnismäßigkeit
    - Subsidiarität
  - Parameter für Offenlegung: CVD-Prozess

Reformvorschläge

- **Gestaltung der Rechtslage**
  - Gemengelage unterschiedlicher Grundrechtspositionen zu beachten (v.a. Produktverantwortliche, Produktnutzenden, Forschenden)
  - Schaffung eines Rechtfertigungsgrundes
    - Im Rahmen digitaler Souveränität diskutiert, Rechtslage vergleichbar zu medizinischem Heileingriff?
  - Anpassung des Rechtsrahmens
    - Erlaubnis des Reverse Engineerings in § § 69a ff. UrhG, Beschränkung der § § 202a ff. StGB anhand der Intention
    - Eine an § 7a BSIG angelehnte Regelung unter Beachtung des EU-Rechts

Fazit und Ausblick

- **Unabhängige IT-Sicherheitsforschung**
  - ist notwendig, um ein hohes Sicherheitsniveau zu gewährleisten
  - Forscherinnen sollten nicht aus Unsicherheit von Forschung abgehalten werden
  - Sicherheitsanalysen sollten nicht allein staatlichen Stellen überlassen werden
  - Mitigationsmöglichkeiten existieren und sollten angewandt werden
  - Benötigt einen klaren Rechtsrahmen, um Haftungs- und Strafbarkeitsrisiken zu minimieren

Vielen Dank!

Kontakt

FZI Forschungszentrum Informatik

Dr. Manuela Wagner

Daniel Vonderau

Haid-und-Neu-Str. 10-14
76131 Karlsruhe

E-Mail: vonderau/wagner@fzi.de
Web: www.fzi.de