Darknet verstehen – Technik, Risiko, Gesellschaft, Recht

- Michael Brickmann · DIH · 04.02.2026

- Theorie + kontrollierte Labor-Demonstration (legal, whitelisted)
- Quizzes, Fallstudien, Checklisten

Agenda (4 Stunden)

- 1) Begriffe & Mythen
- 2) Technik: Tor & Onion Services
- 3) Labor-Demo (kontrolliert)
- 4) Risiken & Ökonomie
- 5) Politik: Repression, Shutdowns
- 6) Whistleblowing & Information Sharing
- 7) Recht/DSGVO & Abschluss

Regeln (Compliance & Safety)

- Keine Schritt-für-Schritt-Anleitungen zu illegalen Handlungen
- Keine Links/Marktplätze/illegalen Inhalte
- Labor: Whitelist/Bookmarks-only, keine Suchmaschinen
- Keine Accounts, keine personenbezogenen Eingaben, keine Downloads
- Bei unerwarteten Inhalten: sofort stoppen → Reset

Begriffe & Einordnung

Surface Web / Deep Web / Darknet

- Surface Web: indexiert
- Deep Web: nicht indexiert (alltäglich)
- Darknet: absichtlich verborgen, spezieller Zugang

Mythencheck

- „Alles illegal“ – falsch
- „Tor macht unsichtbar“ – falsch
- Technik ≠ Handlung

Warum Begriffe wichtig sind

- Fehlentscheidungen vermeiden
- Risikokompetenz statt Sensationslogik
- Politische Dimension verstehen

Technik: Tor & Onion Routing

Tor als Overlay-Netzwerk

- Tor läuft über dem Internet
- Relays/Verzeichnisse/Client
- Ziel: Kommunikationsbeziehungen verschleiern

Onion Routing (Modell)

- Mehrere Stationen (Nodes)
- Mehrere Verschlüsselungsschichten
- Jede Station kennt nur Teilinformationen

Onion Services

- Dienste nur im Tor-Netz
- Kein klassischer Exit notwendig
- Legitime Use-Cases möglich (z. B. Quellenschutz)

Grenzen der Anonymität

- Threat Model entscheidend
- Fingerprinting/Endpunkte
- Verhalten & OPSEC (nur Konzept)

Messbarkeit & Zensurindikatoren

- Tor-Metriken: Schätzwerte
- Anomalien als Hinweis
- Kein Beweis, aber Signal

Labor-Demonstration (kontrolliert)

Labor-Setup

- Virtuelle Maschinen
- Laborrechner
- Restriktive Firewall
- Snapshot/Reset
- Downloads deaktiviert

Labor-Regeln

- Whitelist/Bookmarks-only
- Keine Suchmaschinen
- Keine Accounts
- Abbruchregel

Beobachtungsaufgabe

- Ladezeit/Performance – Wie performant ist das Darknet
- Usability – Finde ich Informationen leicht
- Vertrauenssignale – Wie vertrauenswürdig sind die Angebote
- Risikoindikatoren

- Beispiel: 21 Million Club

Reflexion

- Was ist anders als erwartet?
- Welche Vertrauenssignale fehlen?
- Welche Risiken bleiben trotz Legalität?

Risiken & Ökonomie

Threat Modeling

- Schutzgüter
- Akteure
- Angriffswege
- Folgen

Typische Risiken

- Malware
- Betrug
- Desinformation
- Recht/Compliance

Ökonomie: Marktlogik

- Geringe Rechtsdurchsetzung
- Reputation als Ersatz
- Betrug strukturell wahrscheinlich

Leak-Ökonomie

- Zugangsdaten/Erpressung
- Reputationsschäden
- Incident Response statt Neugier

Politik & nicht-demokratische Staaten

Digitale Repression

- Zensur
- Überwachung
- Manipulation
- Einschüchterung

Tool-Blocking

- Umgehungstools werden blockiert
- OONI Messdaten/Reports : https://explorer.ooni.org/
- Zugang als Machtfrage

OONI

Open Observatory of Network Interference

Global community measuring Internet censorship since 2012

Internet Shutdowns

- Extremmaßnahme
- Auswirkungen auf Bildung/Wirtschaft/Gesundheit
- Dokumentierte Häufigkeit

Warum Tor wichtig sein kann

- Quellenschutz
- Zugang zu unabhängigen Informationen
- Schutz vor Repression

Whistleblowing & Information Sharing

Whistleblowing – Definition

- Meldung im öffentlichen Interesse
- Abgrenzung zu Hacking/Leaking
- Schutz Dritter

EU-Richtlinie 2019/1937

- Mindeststandards
- Schutz vor Vergeltung
- Sichere Meldekanäle
- Österreich: HinweisgeberInnenschutzgesetz (HSG), gültig seit Februar 2023

Kernpunkte der Richtlinie:

- Schutzziel: Whistleblower sollen vor beruflichen Repressalien wie Kündigung, Degradierung oder Diskriminierung geschützt werden.
- Pflicht für Unternehmen: Firmen ab 50 Mitarbeitern sowie Behörden und Gemeinden (ab 10.000 Einwohnern) müssen interne Meldekanäle einrichten.
- Anwendungsbereich: Die Richtlinie umfasst Verstöße in Bereichen wie öffentliches Beschaffungswesen, Finanzdienstleistungen, Produktsicherheit, Umweltschutz und Datenschutz.
- Meldewege: Hinweisgeber können zwischen internen Kanälen und externen Meldestellen (staatliche Behörden) wählen.

SecureDrop (Beispiel)

- Anonyme Einreichungen
- Onion-Service als Kanal
- Technik + Prozess

Information Sharing (IT)

- Vorfallberichte/IOCs/Lessons Learned
- Governance: Zweckbindung, Minimierung
- Need-to-know

Abwägungsmatrix

- Öffentliches Interesse
- Authentizität
- Datenschutzrisiko
- Eskalation

Recht/DSGVO & Abschluss

DSGVO-nahe Praxis

- Leak-Hinweis: nicht klicken
- Dokumentieren
- Melden (IT-Security/DSB)
- Need-to-know

Fallstudien (Transfer)

- Dump-Link
- Anonyme Quelle
- Unerwarteter Inhalt im Labor

Post-Quiz

- Transferfragen
- Prozesskompetenz
- Reflexion

Takeaways

- Technik ≠ Handlung
- Risiko & Prozess
- Kontext verstehen
- Professionell reagieren

Quellen & Weiterführendes

- Freedom House
- OONI
- Access Now
- OHCHR
- UN Report
- SecureDrop
- Tor Metrics

Quiz 1 (Begriffe) – Fragen

- 1) Deep Web = Darknet?
- 2) Tor illegal?
- 3) Onion Service?
- 4) Risikoindikator?
- 5) Shutdown?

Quiz 1 – Lösungen

- 1) Nein
- 2) Nein (Handlung entscheidet)
- 3) Dienst nur im Tor
- 4) Downloadaufforderung
- 5) Internetabschaltung

Abschluss & Feedback

- Was nehme ich mit?
- Welche offenen Fragen?
- Feedback (1 Minute)