DIGITALE SELBSTVERTEIDIGUNG: ANONYMES SURFEN MIT TOR

1 WO SIND DIE PROBLEME?

- Das Internet ist nicht anonym.
- Um den Inhalt einer Webseite zustellen zu können, bekommt diese bei jedem Aufruf die IP-Adresse, die eindeutig einem Anschluss-Inhaber zugeordnet ist.
- Auch Dritte, deren Inhalte auf einer Seite eingebunden werden (Google, Facebook etc.), bekommen diese Information automatisch.
- Behörden können sich – heute oder in Zukunft – Zugang zu diesen Daten verschaffen, nicht nur, um konkrete Straftaten zu verfolgen, sondern auch, um sehr unspezifische „Gefährdungen“ zu untersuchen.

2 WAS KÖNNEN WIR TUN?

- Tor (ursprünglich „The Onion Router“)
  - Anfragen werden nicht direkt an Webseite geschickt, sondern über drei Zwischenstationen.
  - Die Anfragen und zugehörige Antworten werden schichtweise verschlüsselt – daher „Onion“, also „Zwiebel“.
  - Die erste Zwischenstation („Entry-Knoten“) sieht zwar, von wem eine Anfrage kommt, aber nicht, wohin sie geht, da sie noch mit den nächsten beiden Schichten verschlüsselt ist.
  - Die letzte Zwischenstation („Exit-Knoten“) sieht zwar die Anfrage im Klartext, aber nicht, woher sie kommt, da sie ausschließlich mit der mittleren Zwischenstation kommuniziert.
- *Tor Browser Bundle* für alle gängigen Betriebssysteme verfügbar
  - angepasste Version von Mozilla Firefox
  - einige Hilfsprogramme
  - Nutzung von Tor „mit einem Klick“

3 WAS BLEIBT AN PROBLEMEN?

- Surfen über Tor-Netzwerk ist *sehr* langsam.
- Exit-Knoten kann aus aufgerufenen Webseiten (eigenes Facebook-Profil o. ä.) eventuell Informationen herleiten.
  ⇒ Vorsicht bei personalisierten Seiten
- Theoretisch ist Angreifer möglich, der *sowohl* Entry- *als auch* Exit-Knoten kontrolliert.
  ⇒ geeignete Auswahl und häufiger Wechsel der Zwischenstationen wichtig

PIRATEN INFORMIEREN