REGISTRIERUNG BEI DER RTR; DIE ZULÄSSIGKEIT STATISTISCHER AUSWERTUNGEN

4.12.2015: Schutz der Privatsphäre im Internet

JOHANNES KEPLER
UNIVERSITÄT LINZ

INSTITUTE
OF NETWORKS
AND SECURITY

TOR UND DAS TKG

- Unterliegt der Betrieb eines TOR-Knotens dem TKG?
- Wenn ja, dann insb:
  - Meldepflicht (§ 15)
    - Jede Änderung/Einstellung ist ebenfalls zu melden
  - Sicherheitsmaßnahmen nach Stand der Technik (§ 16a, 95, 95a)
    - Inkl Meldung der Maßnahmen an die Regulierungsbehörde
  - AGBs sind verpflichtend zu erlassen (§ 25)
  - Aufsichtsrecht durch Regulierungsbehörde (§ 86)
  - Kommunikationsgeheimnis und Datenschutz (§ 92 f)
  - Vorratsdatenspeicherung → Sofern wieder eingeführt
- Ziemlicher Aufwand; für Private kaum tragbar
- Die JKU (das Institut) meldete und erhielt wunschgemäß einen negativen Feststellungsbescheid

WANN UNTERLIEGT MAN DEM TKG?

- UA als Betreiber eines öffentlichen Kommunikationsnetzes oder eines öffentlichen Kommunikationsdienstes
- Öffentlich: Hier nicht zweifelhaft
  - Jeder weltweit kann den TOR-Knoten benützen; außer an Entry-Nodes ist eine Benutzerprüfung unmöglich (=anonym!)
  - Client-Programm: Gratis & für jeden verfügbar
- Kommunikationsnetz (§ 3 Z 4,11) = Übertragungssysteme und ggf **Vermittlungs-einrichtungen** zur elektronische Übertragung von Signalen, unabhängig von der Art der übertragenen Informationen
- Kommunikationsdienst (§ 3 Z 3, 9) = Gewerbliche Dienstleistung, die ganz oder überwiegend in der Übertragung von Signalen über Kommunikationsnetze besteht; aber keine Inhaltsanbieter oder Dienste mit redaktioneller Kontrolle

TELEKOMMUNIKATIONS-DIENST/-NETZ

KOMMUNIKATIONSDIENST: GEWERBLICHE DIENSTLEISTUNG?

- Selbständig, planmäßig, nach außen gerichtet, regelmäßig etc.
- Aber: Kein Gewinn, noch nicht einmal Einnahmen!
  - Auch keine Werbung auf Webseiten, ersetzen im Datenstrom…
- Finanzierung erfolgt durch Universität: Geräte und Personal
  - Reicht das aus?
  - ErläutRV: Dienste ohne ökonomischen Hintergrund (zB von Universitäten betriebene Datenbanken) fallen heraus
  - ErläutRV: Auch unentgeltliche Angebote fallen darunter, wenn sie im Endeffekt den Unternehmenswert steigern sollen
- Universität: Steigerungen des (zB wissenschaftlichen) „Wertes“ können kaum darauf zurückgeführt werden, nicht einmal indirekt
  - Gegenargument: Gleiche Dienste gibt es auch kommerziell!

KOMMUNIKATIONSDIENST: SIGNALÜBERTRAGUNG?

- Übertragung findet hier zwischen zwei Netzwerkanschlüssen statt
  - Entfernung: Knapp 5 cm ☺ (bzw 2 VLANs eines Abschlusses)
- Was passiert hier: Geht es um den Transport der Daten oder um eine inhaltliche Bearbeitung?
  - Hauptzweck ist die Anonymisierung → Bearbeitung
- ABER:
  - China: Zensur verhindert Kommunikation; mittels TOR geht es
  - Abgegrenztes großes Gebiet, Benutzerzahl nicht unerheblich
  - Verbindung von „Internet mit Zensur und eingeschränkt“ zu „Allgemeines Internet“ → Übertragung zwischen zwei Netzen!
    - Das ist auch nicht bloß ein unabsichtlicher Nebeneffekt…
- Zumindest ein Anteil an Signalübertragung erfolgt

KOMMUNIKATIONSDIENST: ERGEBNIS (RTR-BESCHEID)

- Dienst besteht nicht überwiegend in der Übertragung von Signalen über Kommunikationsnetze
  - Gewisse Übertragung wurde daher anscheinend anerkannt!
- Der Netzzugang wird nicht von der JKU angeboten
  - Nutzer des Dienstes sind keine „Teilnehmer“ nach § 3 Z 19 TKG
  - Kritik: „Teilnehmer“ sind nicht erforderlich!
    - Nutzer des Dienstes haben keinen Vertrag mit der JKU, sind also tatsächlich keine Teilnehmer
    - Auch teleologisch können „Teilnehmer“ nicht erforderlich sein
  - Allgemein jedoch meist richtig: Man muss schon im Internet sein, um TOR nützen zu können, daher kein „Zugang“ zum Netz sondern etwas „im“ Netz!
    - Auch hier wieder das Problem China/Iran/…: „Neues“ Internet!

KOMMUNIKATIONSNETZ: ÖRTLICHE VERTEILUNG

- RTR: Mindestens ein Netzwerksknoten und zwei Verbindungen zu anderen Netzen
  - Ein Knoten → Der Tor-Exit-Node
  - Zwei Verbindungen: Eingang und Ausgang
  - Andere Netze: Es ist in beiden Fällen dasselbe Netz
    - Kommunikation ist grundsätzlich möglich; evtl weigert sich eine Seite daran teilzunehmen
    - Jemand unterbricht die Verbindung (zB Zensur) → Siehe vorher!
- Auch teleologisch begründbar: Geographische Ausdehnung ist der Sinn und Zweck
  - Zusammenschaltung, Leitungsrechte, Mitbenutzung etc.
  - Es gibt kein „Servicegebiet“, da die gesamte Welt „Kunde“ ist

KOMMUNIKATIONSNETZ: VERBINDUNGEN ZU TEILNEHMERN?

- RTR: Verbindung zu einem Netz und Verbindungen zu Teilnehmern reichen auch aus (=Mobilfunk)
  - Es wird aber kein Zugang zu einem Netz eröffnet: Wer Tor nutzen will, muss schon im Internet sein (siehe aber sogleich)
  - Hauptproblem: Keine Teilnehmer (Legaldef. in § 3 Z 19 TKG)
    - Erfordert einen Vertrag → Weder kennen wir die Tor-Nutzer noch haben wir einen (anonymen) Vertrag mit ihnen (zB per AGBs)
- Weitere Schwierigkeit: Das Ziel ist (iA) auch vorher schon erreichbar, da beide im Internet sind
  - Ziel ist nicht das „erreichbar machen“ (Dissidenten?) sondern die „inhaltliche Bearbeitung“, dh die Anonymisierung

KOMMUNIKATIONSNETZ: HIDDEN SERVICES

- Diese Dienste sind ausschließlich über Tor erreichbar
  - Zur Verwaltung manchmal auch anders, dies ist aber nicht öffentlich möglich und nicht öffentlich bekannt
- Verbindung “Internet” mit “Darkweb”
  - Letzteres ist zwar klein, aber ein echtes separates Netz
- Vorläufiges Ergebnis: Tor-Knoten als Verbindung zweier Netze
- ABER: Ein Knoten alleine erlaubt keinen Zugriff
  - Es wird eine vollständige Kaskade (3 Knoten) benötigt
    - Directory-Server nicht: Diese dienen nur dem Auffinden, nicht der Kommunikation (evtl wegen techn. Umsetzung zu bezweifeln)
  - Daher erst Meldepflicht, wenn alle drei Typen betrieben werden – sonst nicht einmal theoretisch möglich

KOMMUNIKATIONSNETZ: TEILNEHMERANSCHLUSS?

- Kein „Betreiben“ eines Kommunikationsnetz, wenn die Verbindung zu anderen öffentlichen Kommunikationsnetzen ausschließlich über einen Teilnehmeranschluss erfolgt (§ 3 Z 4)
  - ZB große Nebenstellenanlagen
- „Anschluss“ des Tor-Knotens: Ethernet + IP
  - Andere Varianten existieren ebenfalls in der Praxis (zB WLAN), aber vielfach ist das exakt der Teilnehmeranschluss
  - Wichtig: „Teilnehmer“ bedeutet hier „Endkunde“, zb auch ein Unternehmen das einen Internetanschluss benötigt.
    - Muss nicht das Verbindungsende sein: ZB Ruf-Weiterleitung
  - Nicht aber ISPs: Mehrere Anschlüsse sowie zusätzliche Protokolle (zB BGP), andere Vergabe von IP-Adressen (mehrere/große Blöcke), regelmäßige Durchleitung

KOMMUNIKATIONSNETZ: ERGEBNIS (RTR-BESCHEID)

- Keine räumliche Signalübertragung, da beide Anschlüsse am selben Ort und mit dem selben Netz verbunden sind
  - Gedankliche Voraussetzung: „Trennung“ vom restlichen Universitätsnetz
    - Institute besitzen keine Rechtspersönlichkeit, nur die JKU
    - Sonstige Angebote der Uni könnten ein Kommunikationsdienst sein
    - Das Uni-Netz ist evtl mehrfach verbunden (Aconet-Ring)
    - Sonst vollständig getrennt: Keine gemeinsamen Nutzer, keine integrierte Verwaltung etc.
- Kein Kommunikationsnetz, da darüber kein Kommunikationsdienst erbracht wird
  - Nur eingeschränkt richtig: Wir machen das nicht, allgemein kann das schon erfolgen (wir wissen nicht wer die Knoten wofür nutzt; muss nicht dieselbe Person sein)!

ÜBERTRAGBARKEIT AUF DRITTE?

- Gilt das Ergebnis („TKG nicht anwendbar“) auch für ISP/Private?
  - Keine räumliche Signalübertragung? JA
    - ISP: Setzt voraus, dass der Tor-Knoten separat betrieben wird und nicht in das „normale“ Netz integriert ist
  - Kein Kommunikationsdienst, da die Anonymisierung im Vordergrund steht? JA
  - Kein neuer Netzzugang? JA
- Ergebnis: Kein Problem, sofern nicht „Besonderheiten“ erfolgen, zB Modem-Einwahl in einen Entry-Knoten
  - Dann ist aber die Besonderheit der Auslöser
- Hängt daher nicht von „Forschungsprojekt“ oder „Universität“ ab!

ACHTUNG: Vertrag mit ISP → Serverbetrieb evtl verboten!

STATISTISCHE AUSWERTUNGEN

STATISTISCHE AUSWERTUNGEN: PLAN UND RECHTLICHE ASPEKTE

- Geplant ist, statistische Daten über die Nutzung des Exit-Nodes zu sammeln und auszuwerten
- Wichtig: Keine Chance zur De-Anonymisierung (nicht einmal eine Erleichterung!), aber trotzdem nützliche Daten erheben…
- Grundlegende Regeln:
  - Keine Sammlung am Eingang, nur am Ausgang
    - Wenn nur eine Seite, dann ist alleine mit diesen Daten keine De-Anonymisierung möglich bzw wird nicht erleichtert
    - Dritte (=Daten aus weiteren Quellen) → Zusätzlich verallgemeinert
  - Keine Untersuchung des Kommunikationsinhalts
    - Vollautomatisch wäre zwar möglich, ist aber nicht hilfreich, da für Verfeinerung/Analyse ein manueller Einblick nötig wäre
    - Einzige Möglichkeit: Signaturprüfung nach externen Quellen
  - Weitere Einschränkungen (zB zu wenige Datensätze)

WELCHE DATEN WERDEN ERHOBEN?

- Ziel-IP-Adresse: Welche Server werden kontaktiert?
  - Aber: Dies ist viel zu individuell; Rückschlüsse wären möglich
  - Daher Verallgemeinerung nach zwei Punkten:
    - Umsetzung auf Autonome Systeme → zB Google (=Firmen), aber auch große Provider
    - Ziel-Land mittels (lokaler!) GeoIP-Auflösung
- Ziel-Port: Welche Dienste werden verwendet?
  - Nur Dienste einer „interessanten“ Liste werden gespeichert
  - Alles andere wird zu „Rest“ aggregiert
  - Basierend auf Port wird „Verschlüsselt: Ja/Nein/Beides“ zugeordnet (leider nicht eindeutig; würde Inhaltsanalyse erfordern)
- Datenmenge: Eingehend und Ausgehend; Bytes und Anzahl
- Abgelehnte Verbindungen (RST, nicht inhaltliche Verweigerung)

WAS SOLL DAMIT UNTERSUCHT WERDEN (1)

- Welche Dienste (im Sinne von Betreibern) werden genutzt?
  - Aufgrund der Verallgemeinerung kann dies nur bei sehr großen Diensten und dort nur pauschal beurteilt werden!
- Wo stehen die kontaktierten Server? Gibt es spezielle geographische „Hotspots“?
  - Lässt uU Rückschlüsse auf die Nutzer zu (Ort/Interessen)
- Welche Dienste (im Sinne von Protokollen) werden genutzt?
  - Web, Chat, SSH, …
- Wie viele Fehler gibt es, dh wie oft wird eine Verbindung überhaupt abgelehnt?
  - Eine Überprüfung ob dies im „öffentlichen“ Internet ebenfalls erfolgt wäre zwar theoretisch möglich, würde aber eine Verarbeitung der konkreten Adresse bedeuten!

WAS SOLL DAMIT UNTERSUCHT WERDEN (2)

- Wie ist die Symmetrie der Verbindung?
  - Mehr Upload oder mehr Download? Vergleich mit “normaler” Nutzung des Internets möglich.
- Zeitlicher Verlauf der Nutzung: Hinsichtlich Protokollen wie auch kontaktierten Servern (lässt evtl Rückschlüsse auf Quellen zu!)
  - Wo ist gerade „Internet-Nutzungszeit“ bei Last-Spitzen?
- Welcher Datenanteil ist verschlüsselt?
  - Nur grob (basierend auf Ports=Protokollen) → Wie „sicher“ wird das Tor-Netzwerk verwendet?

Generell: Mehr wäre möglich, würde aber Gefahren für Nutzer bedeuten oder ist rechtlich heikel (Inhalts-Analyse)!

STATISTISCHE UNTERSUCHUNG: RECHTLICHE BEWERTUNG

- Personenbezogene Daten liegen vor → Datenschutzgesetz
  - Zumindest während der Verbindung sind es die IP-Adressen
- Ausnahme nach § 47 DSG: Wissenschaft und Statistik
  - Hier relevant: Legaler Datenbesitz und anonymes Ergebnis
  - Anonymität der Ergebnisse ist gegeben
  - Ob die Statistik „wissenschaftlich“ sein muss, ist umstritten
    - Viele Kommentare sagen ja, doch steht im Text für „historische, statistische oder wissenschaftliche Zwecke“
    - Auch teleologisch unklar: Ist das Ergebnis anonym, kommt es auf Vorgehensweise bzw „Nützlichkeit“ des Ergebnisses nicht an
  - Legaler Besitz: Daten wurden zur „Bearbeitung“ übergeben
    - Dies wäre hinsichtlich des (dekodierten) Inhalts zweifelhaft!
- Zusätzlich: Für uns sind die Daten nur indirekt personenbezogen

AUSBLICK

- Sofern ein Serverbetrieb erlaubt ist, darf in Österreich an einem Internet-Anschluss ein Tor-Knoten betrieben werden
  - Achtung auf die Datenmenge
  - Sperren der eigenen IP-Adresse oder Beschwerden sind jedoch selbst zu verantworten/bearbeiten und dürfen nicht einfach ignoriert werden
- Statistische Auswertungen sind möglich, sofern besondere Einschränkungen beachtet werden
  - Derzeit noch keine Ergebnisse; Betrieb hat erst begonnen
  - Besondere Schwierigkeit: Keine Kenntnisnahme des Inhalts zur Verbesserung oder Überprüfung der Statistik
    - „Blindflug“ mit Vermutungen, die auf Überlegungen basieren

JOHANNES KEPLER
UNIVERSITÄT LINZ

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

JOHANNES KEPLER
UNIVERSITÄT LINZ
Altenberger Straße 69
4040 Linz, Österreich
www.jku.at