Unter Beobachtung

Staatstrojaner, Polizeiaufgabengesetz, Quellen-Telekommunikationsüberwachung, ...

Themen/Termine

- <u>08.10.2021, 18:00 Uhr: Was dürfen die?</u>
  - Überblick über die Gesetze/Regelungen, die digitale Überwachung möglich machen
- <u>15.10.2021, 18:00 Uhr: Was können die?</u>
  - Ein Versuch einer Einschätzung, wie real die Bedrohung durch digitale Überwachung ist
- <u>22.10.2021, 18:00 Uhr: Was können wir tun?</u>
  - Einführungsworkshop: Wie können wir digitale Kommunikation sicherer gestalten?

Eine kurze Bitte...

- Bitte schaltet, wenn ihr nicht sprecht, eure Mikrofone stumm.
- Ob ihr die Kameras an oder aus macht, ist euch überlassen (Kamera aus ist gut für Klima und Privatsphäre)
- Postet Fragen & Kommentare gerne in den Chat, wir werden immer wieder danach schauen und sie im Laufe der Zeit beantworten.

DISCLAIMER

Wir sind keine (Rechts-)Expert*innen!

Wenn ihr etwas besser wisst, klärt uns gerne auf!

Ziele der Veranstaltung

- Wir wollen aufklären
- Sensibilisierung für das Thema
- Erarbeitung, welche Maßnahmen sinnvoll sein können
- Vernetzung
- Skillsharing
- Langfristige Arbeit an dem Thema

Heutiges Thema

Was dürfen die?

- Einblick in neuere Gesetze und deren Konsequenzen schaffen

Der Schwerpunkt der Reihe liegt allgemein auf digitaler Überwachung -> andere Gesetze zu staatlicher Repression, wie etwa zum Thema Pfefferspray, werden nicht behandelt

Allgemein

Überwachungsgesetze bieten Sicherheit! Wirklich?

Überwachungsgesetze sollten nicht isoliert betrachtet werden, sondern in ihrer Gesamtheit. Nur so wird das tatsächliche Ausmaß der Eingriffe in die Persönlichkeitsrechte und damit der digitalen Selbstbestimmung deutlich.

Dazu später mehr!

Telekommunikationsgesetz (TKG)

22.04.2021: Novellierung beschlossen

Inhaltliche Überwachung unterliegt Bundes- und Landesgesetzen. TKG regelt die technische Umsetzung + Ermächtigung der Bundesregierung die TKÜV zu erlassen

Das Wichtigste, was für uns relevant ist?

- Marktortprinzip für Messenger (Unternehmen unterliegen dem Recht des Landes, in dem sie Tätig sind)
- Vorratsdatenspeicherung bleibt im Gesetz
- Bestandsdatenauskunft
- Mailanbieter ab 100.000 Vertragspartner*innen sind verpflichtende Schnittstelle für behördliche Datenabrufe (zuvor wurde gefordert, dass Teilnehmer*innen gezählt werden. Dies hätte zur Folge, auch kleine Dienste betroffen wären, wenn die einzelnen Vertragspartner*innen in mehreren Gruppen aktiv sind, oder mehrere Mail-Adr. haben)

Im neuen TKG finden sich also wieder verfassungsrechtlich zumindest umstrittene Neuerungen!

Quelle: https://netzpolitik.org/2021/recht-auf-lahmes-internet-was-das-neue-telekommunikationsgesetz-bedeutet/
https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Broschueren/INFO5.pdf?__blob=publicationFile&v=17

Quellen-Telekommu...WAS?

Typen von Überwachung digitaler Endgeräte

1. Telekommunikationsüberwachung
2. Quellen-Telekommunikationsüberwachung
3. Quellen-Telekommunikationsüberwachung “plus”
4. Online-Durchsuchung

Typen von Überwachung digitaler Endgeräte

1. Telekommunikationsüberwachung
2. **Quellen-Telekommunikationsüberwachung**
3. **Quellen-Telekommunikationsüberwachung “plus”**
4. **Online-Durchsuchung**

Quellen-Telekommunikationsüberwachung

- ”Kleiner Staatstrojaner”, d.h. es darf nur laufende Kommunikation mitgelesen/gehört werden.
- Privatsphäre der Betroffenen wird immens angegriffen;
- Für das Eindringen in die Geräte Betroffener sind in der Regel Sicherheitslücken notwendig.
- Die rechtliche Basis findet sich in der StPO, sowie in den entsprechenden PolG der Länder.

Quelle: polizeigesetze-stoppen.de; inzwischen OFFLINE, nur noch über das Internet archive abrufbar;

Quellen-Telekommunikationsüberwachung “plus”

- Wie Quellen-TKÜ;

  <u>Einziger Unterschied:</u>

- Hier darf der gesamte Kommunikationsverlauf gelesen werden, auch rückwirkend.

Online-Durchsuchung

- Geräte werden digital durchsucht.
- Daten darauf werden sichergestellt.
- In der Regel durch Einsatz von Schadsoftware die über Sicherheitslücken aufgespielt wird.
- ALLE Inhalte des Geräts können eingesehen werden! >> Immenser Eingriff in Privatsphäre
- Interessenkonflikt zwischen der Nutzung der Sicherheitslücken und staatlichen Verpflichtung, möglichst sichere Systeme zu gewährleisten.
- Grundlage ist die StPO sowie die entsprechenden PolG der Länder
- Begriff ist irreführend, weil eben keine punktuelle Durchsuchung, sondern über längeren Zeitraum

Quelle: polizeigesetze-stoppen.de; inzwischen OFFLINE, nur noch über das Internet archive abrufbar;

Staatstrojaner im Einsatz

- RCIS (BKA)
- FinSpy (FinFisher)
- Pegasus (NSO Group)
- Candiru (s/t)
- ...

Foto: https://securelist.com/finspy-unseen-findings/104322/

Wie kommt der Fisch auf mein Gerät?

<u>physischer Zugriff:</u>

z.b. Gerät offen liegen lassen, oder vorgetäuschter Techniker*innenbesuch, oder heimlicher Zutritt zu Wohnung

<u>digitaler Zugriff:</u>

Trojaner wird durch eine Sicherheitslücke oder durch Phishing aufgespielt.

Neuerdings: Mitwirkungspflicht der Telekommunikationisanbieter!

Heimliches Betretungsrecht der Wohnung

- Betretungsrecht der Wohnung ohne Wissen der Betroffenen Person haben der Bundesverfassungsschutz sowie alle LandesVS-Behörden, ebenso wie der MAD und der BND.

- In einigen Bundesländern (Bayern,Hessen, Sachsen Mecklenburg-Vorpommern) hat dieses Recht auch die Polizei, jedoch mit Einschränkungen

- Der Entwurf des Bundespolizeigesetzes wurde jüngst vom Bundesrat abgelehnt.

Quellen: https://freiheitsrechte.org/polg-mv/, https://www.bundestag.de/resource/blob/670140/af12ed40fb30d3bfda6f00bd362fb54a/WD-3-213-19-pdf-data.pdf
https://www.zeit.de/politik/deutschland/2021-06/staatstrojaner-bundesrat-verfassungsschutzgesetz-union-spd-ueberwachung-kommunikation-reform

Mitwirkungspflicht der Internet-Provider

- Internet-Anbieter, sowie mit dem neuen VS-Gesetz auch Anbieter von klassischer Telekommunikation, Email-Provider, Messengerdienste und VoiP, sollen Datenströme an Geheimdienste umleiten.
- Dadurch sollen die Geheimdienste bei der Installation von Schadsoftware unterstützt werden.

Quellen: https://netzpolitik.org/2020/staatstrojaner-provider-sollen-internetverkehr-umleiten-damit-geheimdienste-hacken-koennen/ , https://netzpolitik.org/2020/mit-diesem-gesetz-bekommen-alle-geheimdienste-staatstrojaner/ ,

Probleme beim Einsatz der Trojaner

- Sicherheitrisiko für die gesamte Gesellschaft wird in Kauf genommen, damit in 3 Fällen abgeschnorchelt werden kann
- Notwendigkeit ist nicht gegeben, ist aber zwingendes Kriterium für Grundrechtseingriffe
- Sind gesetzlich nicht kontrollierbar und intransparent.
- Technisch/Rechtlicher Fallstrick: vermutlich lässt sich zwischen den drei Trojanern (QTKÜ, QTKÜ+, Online-Durchsuchung) keine Trennlinie ziehen.

https://netzpolitik.org/2021/bundespolizeigesetz-grosse-koalition-einigt-sich-auf-staatstrojaner-einsatz-schon-vor-straftaten/

Ein Beispiel

- Inzwischen ist es verboten, Propagandamittel von Organisationen zu verbreiten, die auf der “EU-Terrorliste” stehen.
- Nach der Novelle des StGB können nun hierfür Telekommunikations- und Quellenkommunikationsüberwachung verwendet werden.
- Dies ist kurzfristig ausgeweitet worden auf sogenannte Feindeslisten.

Quelle: https://netzpolitik.org/2021/ausweitung-bei-staatstrojanern-kollateralschaeden-im-prozessrecht/

Ein Beispiel

- Die Ausweitung auf die Terrorliste bedeutet, dass auch bei nicht-verbotenen Organisationen nun eine QTKÜ möglich ist.
- Durch diese Gesetzesänderung kann nun potentiell die Verbreitung von “Propagandamitteln” genügen für eine QTKÜ
- Lichtblick: Verdacht reicht hier nicht aus.

Quelle: https://netzpolitik.org/2021/ausweitung-bei-staatstrojanern-kollateralschaeden-im-prozessrecht/

ABER

2019 wurde die Quellen-Telekommunikationsüberwachung insgesamt 31 mal richterlich angeordnet und in drei Fällen tatsächlich angewandt.

Das bedeutet im Umkehrschluss, dass ein enormes Sicherheitsrisiko ALLER in Kauf genommen wird, für den Ermittlungserfolg bei ein paar wenigen Fällen.

Gleichzeitig sinkt dadurch das kollektive Vertrauen in die digitale Infrastruktur.

Zudem wird Straftatbereich, in dem die Technik eingesetzt werden darf, permanent erweitert, und immer neue Behörden bekommen erweiterte Befugnisse.

Quelle: https://netzpolitik.org/2021/justizstatistik-2019-polizei-nutzt-staatstrojaner-vor-allem-bei-erpressung-und-drogen/

Vorratsdatenspeicherung

Erfasst werden sollen Verbindungsdaten -> wer, wo, wie, mit wem. Konkrete Inhalte von z.B. Nachrichten nicht.

Was können Verbindungsdaten sein?

- Welche **Messagingdienste** benutzt wurden
- Wann Nachrichten gesendet wurden
- Wann **Anrufe** getätigt wurden, mit wem, wie lange und wie oft
- Wann über welche Plattform **Videotelefonie** getätigt wurde, mit wem und wie lange

Vorratsdatenspeicherung

- **Bewegungsprofile** einer Person via Apps über Funkdaten oder GPS
- Auskunft über **Internetverhalten** (IP-Vorratsdatenspeicherung)
- **Metadaten** von Kommunikation
- Auf **internationaler Ebene**: Fluggastdaten, Fingerabdrücke, Zahlungsverkehr
- Aber auch Verkehrsdaten via Smart Cars, Daten vom Smart TV und Smart Home, automatisch generierte SMS für Ärzt*innentermine

Die Vorgaben betreffen Anbieter*innen, die entsprechende Daten auf gesetzlichen Beschluss erfassen und zur Verwertung bereitstellen müssen.

Vorratsdatenspeicherung: Kritik

- Unvereinbarkeit mit Menschenrechten
- Kosten-Nutzen-Rechnung unzureichend (Untersuchungen haben gezeigt, dass kaum Erfolge bei der Strafverfolgung zu verzeichnen sind. Die Kosten sind demgegenüber nicht gerechtfertigt)
- Online-Aktivitäten im Ausland bleiben unberührt (z.B. über ausländische Server)
- Alle sind verdächtig = Vertrauensverlust in der Bevölkerung
- Trennung von Verbindungsdaten und Inhalten kaum möglich
- Verbindungsdaten sind ebenso aussagekräftig
- Datensammlungen sind hochsensibel und könnten gehackt werden
- Problematisch bei bestimmten Berufsausübungen (z.B. Journalist*innen können nicht mehr vertrauensvoll mit ihren Quellen sprechen)

Vorratsdatenspeicherung: Historie

April 1996
Mindestspeicherfristen für Telekommunikationsdaten

Februar 2005
Neuer Beschluss über anlasslose Speicherung

Mai 2006
Europäische „Richtlinie über die Vorratsspeicherung von Daten“ tritt in Kraft

März 2010
Deutsches Bundesverfassungsgericht erklärt die Vorratsdatenspeicherung für verfassungswidrig

April 2014
Oberverwaltungsgericht NRW erklärt neue Vorratsdatenspeicherung für europarechtswidrig

Dezember 2015
Neue Vorratsdatenspeicherung wird in Deutschland verkündet

Juni 2017
EuGH befindet die bisherige Verratsdatenspeicherung als verfassungswidrig

Juni 2017
Bundesnetzargentur setzt geplante Vorratsdatenspeicherung vorläufig aus

Vorratsdatenspeicherung: Aktuell

Der **2015** vorgestellte Gesetzentwurf für die **Vorratsdatenspeicherung**, der **2017** in Kraft treten sollte, wurde kurz vor der offiziellen Anwendung auf Eis gelegt. Im **April 2018** bestätigte das Verwaltungsgericht Köln erneut, dass die Vorratsdatenspeicherung gegen das **Europarecht** verstoße. In Deutschland wird die Methode also nach wie vor **nicht angewendet**. Der deutsche Entwurf zur Vorratsdatenspeicherung liegt aktuell allerdings wieder vor dem EuGH.

<u>Oktober 2020</u>
Das EuGh stellt erneut fest, dass eine allg. und unterschiedslose Speicherungs- und Weiterleitungspflicht von Verkehrs- und Standortdaten mit dem Unionsrecht unvereinbar ist (Artikel 7, 8 und 11 der Grundrechtecharta)

https://www.bussgeldkatalog.org/vorratsdatenspeicherung/ https://www.br.de/radio/bayern2/inhalt/spezial/vorratsdatenspeicherung-geschichte-100.html
https://netzpolitik.org/2021/vorratsdatenspeicherung-und-taeglich-gruesst-das-murmeltier/

IT-Sicherheitsgesetz: Zweck

Beschlossen im April 2021

- Schutz von kritischer Infrastruktur (Entsorgung, Gesundheit, Energie usw.) + kritische Komponenten
- Regelungen für den Ausbau von 5G (Huawei)
- Mehr Verbraucher*innenschutz (Cybersicherheit)
- Stärkung Bundesamt für Sicherheit und Informationstechnik (BSI)

Quelle:
https://www.datenschutz-praxis.de/allgemein/trotz-massiver-kritik-bundestag-verabschiedet-it-sicherheitsgesetz-2-0/

IT-Sicherheitsgesetz: Funktionsweise

- BSI greift in Systeme ein und bereinigt diese
- Scant nach Sicherheitslücken, muss diese jedoch nicht mitteilen (das bedeutet, dass Sicherheitslücken offen gehalten werden und so zur Gefahr von Verbraucher*innen werden können)
- Beschränkung auf KRITIS-Bereiche
- Protokolldaten + Bestandsdatenauskünfte
- Mit Hilfe des TKG können Interaktionen abgefangen werden

Im Gesetz sind viele Bereiche nicht klar definiert

https://www.bitkom.org/sites/default/files/2020-12/201211_sn_bitkom_it-sicherheitsgesetz_2.0.pdf

IT-Sicherheitsgesetz: Kritik

- Stärkung des BSI kann zu “Ersatznachrichtendienst” führen, da eine enge Kooperation zum Bundesinnenministerium inkl. Geheimdiensten besteht
- Keine Mitteilung von Sicherheitslücken
- Unzureichende Festlegung auf Schutzziele
- Wenig zielgerichtet Regulierung
- Scans bieten Potenzial, Dienste und Programme zu stören oder deren Ausführung zu verhindern

Quellen:
https://www.golem.de/news/it-sicherheitsgesetz-2-0-bundestag-ignoriert-it-sicherheitsexperten-2104-155974.html
https://www.bitkom.org/sites/default/files/2020-12/201211_sn_bitkom_it-sicherheitsgesetz_2.0.pdf
https://www.security-insider.de/kritik-zur-anhoerung-des-it-sicherheitsgesetzes-20-a-1003864/

Warum also?

- Technik entwickelt sich rasant; gab es vor einigen Jahren noch nur zwei nennenswerte Trojaner, so werden nun immer mehr bekannt
- Sukzessive wird der digitale Raum poliziert. Die Gesetze werden immer restriktiver, der Zugriff immer unverblümter. Der Druck auf EU-Ebene nimmt ebenfalls zu.
- Die Themen frühzeitig erkennen, die Auswirkungen begreifen, und sich rechtzeitig wehren!

Exkurs: digitale Überwachung ohne private Endgeräte

- Biometrische Überwachung
  - Fingerabdruck im Personalausweis
    - seit 02.08.2021
    - Klage dagegen läuft
  - Gesichtserkennung:
    - PimEyes, ClearView AI, etc…
    - UN + EU fordert Moratorium der Technologie
    - Behörden ermitteln gegen die Unternehmen
  - Retina-Scan
- Videoüberwachung

Wer die Klagen gegen den Fingerabdruck, die Vorratsdatenspeicherung, … unterstützen will, kann u.a. an https://digitalcourage.de/spenden

Ausblick

Sicherheit? Mit Sicherheit nicht!

- Straftaten werden nicht verhindert, lediglich können Daten bei der Aufklärung helfen ➡
- Aber: Studie von 2011 vom Max-Planck-Institut Vorratsdatenspeicherung kaum Einfluss auf Aufklärungsquote
- Gesichtserkennung fehlerhaft und diskriminierend

Quellen: https://netzpolitik.org/2021/vorratsdatenspeicherung-und-taeglich-gruesst-das-murmeltier/
https://netzpolitik.org/2018/diskriminierende-gesichtserkennung-ich-sehe-was-was-du-nicht-bist/

Ausblick: Wie weit geht das Alles?

Erinnerung: Überwachungsgesetze sollten nicht isoliert betrachtet werden, sondern in ihrer Gesamtheit.

2005 Urteil Bundesverfassungsgericht ➡ Grundrechtrelevante Überwachungsmaßnahmen dürfen nicht einzeln betrachtet werden

Max-Planck-Institut ➡ Überwachungsbarometer zur objektiven Einschätzung der Überwachungslast

Auch Überwachungsgesamtrechnung (Auflistung aller Überwachungsgesetze) genannt soll zukünftig als Entscheidungsgrundlage für neue Gesetze und Reformen dienen

Andere Konzepte sind für eine Freiheitsbestandsanalyse (hier wird vorgeschlagen Grundgesetze dahingehend zu prüfen, welche noch nicht durch Überwachungsgesetze ausgeübt werden können

Quellen: https://shop.freiheit.org/#!/Publikation/1025
https://netzpolitik.org/2021/ueberwachungsgesamtrechnung-mehr-als-die-summe-der-einzelteile/
https://www.fiff.de/publikationen/fiff-kommunikation/fk-jhrg-2019/fk-2019-4/fk-4-19-p37.pdf