Digitale Unversehrtheit

- Wie sicher ist „sicher“? -

- Vortrag [Kurzfassung] -

Wolfgang Meyer
Sicherheit – Privatsphäre – Wahlfreiheit – Verbraucherbildung
https://wmcivis.de

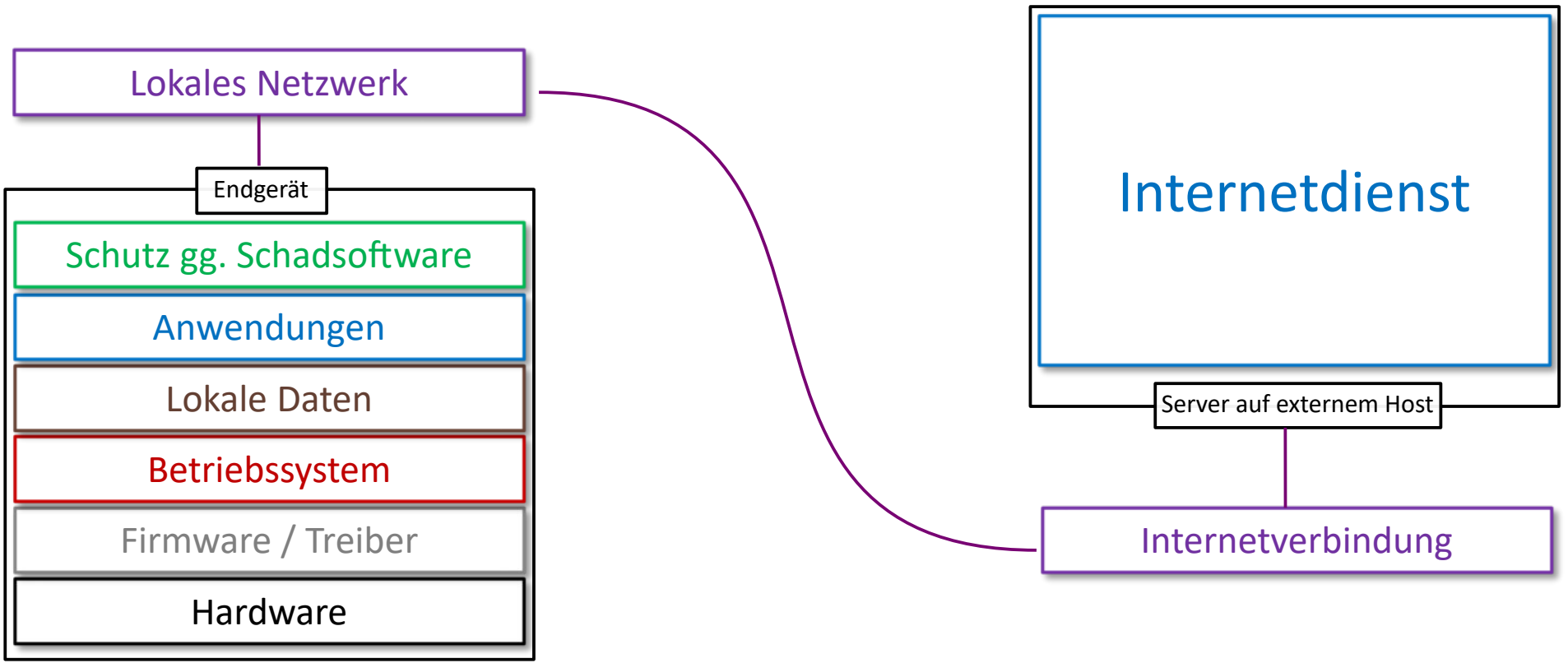
„Sicherheit“ in der digitalen Welt?

- Viele Menschen verbinden „digitale Sicherheit“ vor allem mit der vermeintlichen Sicherheit einzelner Produkte oder Technologien – etwa eines modernen Smartphones, eines bestimmten Betriebssystems oder eines bekannten Messengers. Dadurch entsteht leicht der Eindruck, Sicherheit lasse sich durch die Wahl „der richtigen Technik“ erreichen.
- Aussagen wie „Apple ist sicher“, „Linux ist sicher“ oder „Signal ist sicher“ vereinfachen die Wirklichkeit stark. Tatsächlich gibt es kein Gerät, kein Betriebssystem und keinen Internetdienst, der Menschen für sich allein zuverlässig und dauerhaft schützen könnte.
- Sicherheit kann daher nicht allein durch den Kauf oder die Nutzung bestimmter Technik erreicht werden. Technische Schutzmaßnahmen sind wichtig, sie reichen aber nicht aus, um Manipulation, Überwachung, Datenmissbrauch oder menschliche Fehlentscheidungen zu verhindern.
- „Sicherheit“ betrifft nicht nur Computer und Programme, sondern ebenso Menschen, gesellschaftliche Entwicklungen, wirtschaftliche Abhängigkeiten und politische Rahmenbedingungen. Angriffe zielen heute oft weniger auf Technik als auf menschliches Verhalten und gesellschaftliche Schwachstellen.
- Ein technisch gut geschütztes Gerät kann deshalb trotzdem Teil unsicherer oder manipulativer Strukturen sein – etwa dann, wenn Nutzer durch Desinformation, psychologische Einflussnahme oder digitale Abhängigkeiten beeinflusst werden.

„Sicherheit“ als fortwährender Prozess

- Statt nur von „digitaler Sicherheit“ zu sprechen, kann der Begriff „Digitale Unversehrtheit“ verwendet werden. Gemeint ist damit die Fähigkeit, sich in einer digitalen Welt möglichst wirksam gegen unterschiedliche Gefahren zu schützen und Angriffen widerstandsfähig zu begegnen.
- Digitale Unversehrtheit bedeutet nicht, dass es keine Angriffe mehr gibt. Vielmehr geht es darum, Risiken zu erkennen, Schäden zu begrenzen und trotz ständiger Bedrohungen handlungsfähig zu bleiben.
- Die Gefahren reichen heute weit über klassische Hackerangriffe hinaus. Dazu gehören unter anderem Datenmissbrauch, Manipulation, Desinformation, psychologische Einflussnahme, Einschränkungen von Wahlfreiheit sowie das gezielte Herbeiführen menschlicher Fehlentscheidungen.
- Ein einmal eingerichteter Schutz genügt nicht dauerhaft. Die digitale Welt verändert sich ständig – ebenso die Methoden von Unternehmen, politischen Akteuren, Kriminellen oder extremistischen Gruppen, die Einfluss auf Menschen nehmen wollen.
- Der Schutz der eigenen Digitalen Unversehrtheit muss deshalb als fortlaufender Kreislauf verstanden werden: Entwicklungen wahrnehmen, Risiken einordnen, Entscheidungen treffen und das eigene Verhalten sowie Schutzmaßnahmen immer wieder an neue Gegebenheiten anpassen.

Wesentliche Komponenten moderner IT



Wesentliche Komponenten moderner IT

Lokale Komponenten haben keinen Einfluss und bieten keine Kontrolle über Sicherheit der Internetdienste!

Endgerät

Aktuelles Betriebssystem, Sicherheitsupdates; aktuelle Firmware; Sabotageschutz; Apps aus sicheren Quellen, Updates installiert; sicheres lokales Netz

Unsichere Diensteanbieter

Unsichere Dienste

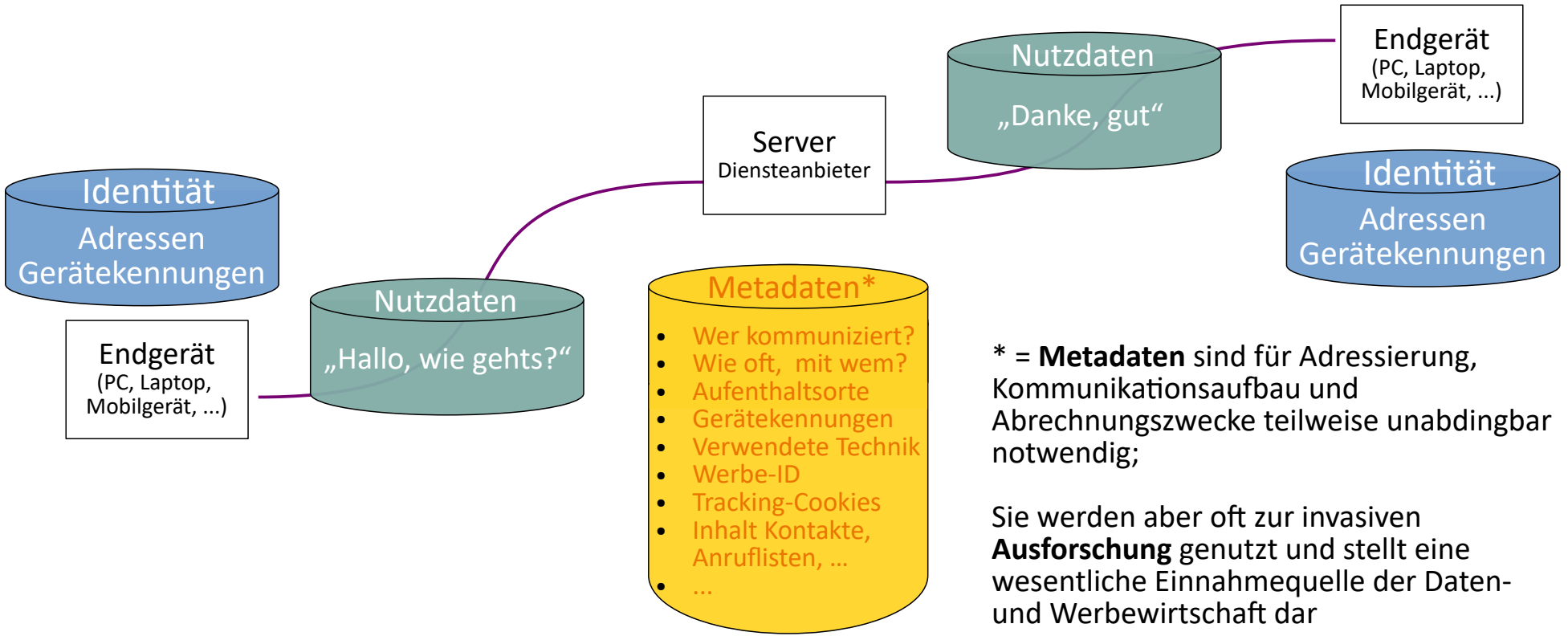
Internetdienst

Identität
Adressen
Gerätekennungen
Nutzdaten
Metadaten

Server auf externem Host

Angriffe auf Internetdienste

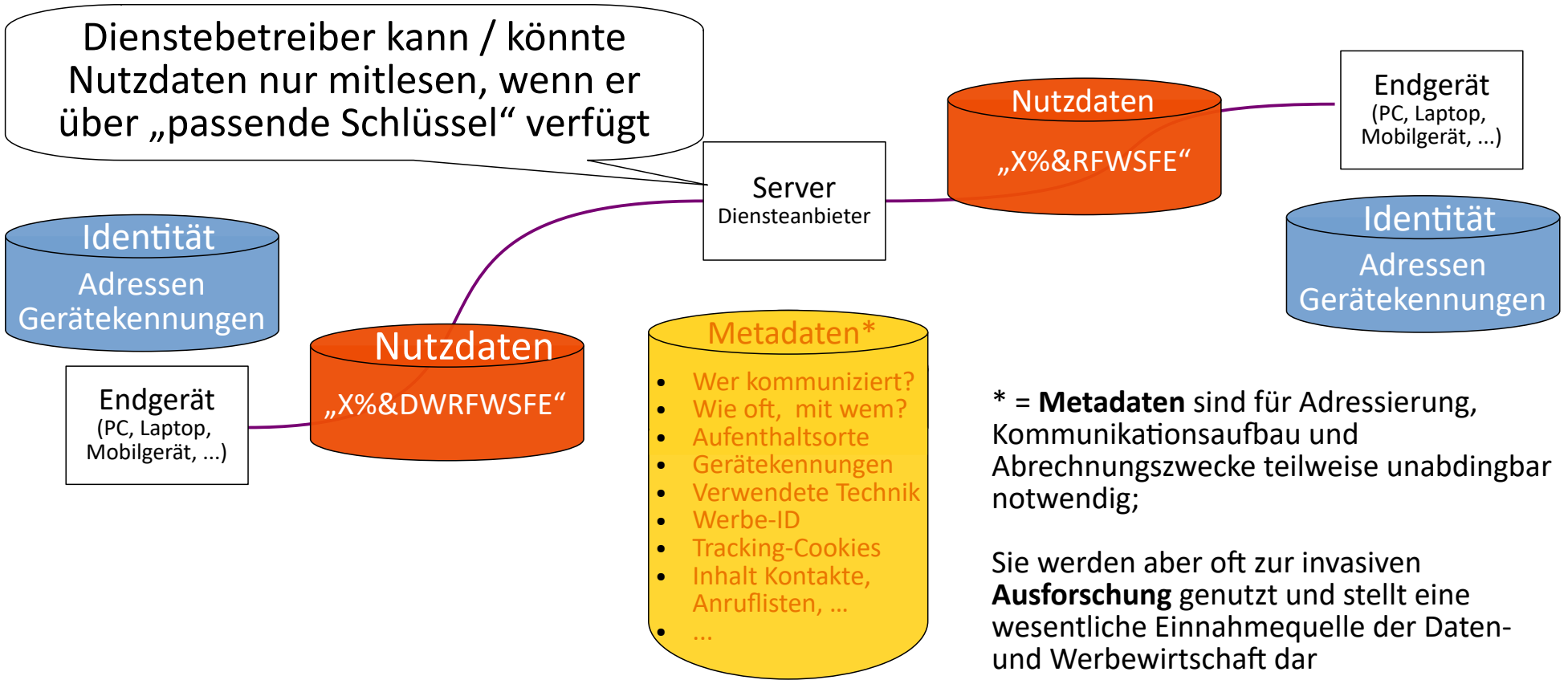
Daten bei der Nutzung von Internetdiensten



* = **Metadaten** sind für Adressierung, Kommunikationsaufbau und Abrechnungszwecke teilweise unabdingbar notwendig;

Sie werden aber oft zur invasiven **Ausforschung** genutzt und stellt eine wesentliche Einnahmequelle der Daten- und Werbewirtschaft dar

Ende-zu-Ende-Verschlüsselung - Schutzwirkung?



* = **Metadaten** sind für Adressierung, Kommunikationsaufbau und Abrechnungszwecke teilweise unabdingbar notwendig;

Sie werden aber oft zur invasiven **Ausforschung** genutzt und stellt eine wesentliche Einnahmequelle der Daten- und Werbewirtschaft dar

Schutzgüter Digitale Unversehrtheit

(IT-)Sicherheit

Technik, Daten, …

Verfügbarkeit, Integrität, Vertraulichkeit

Schutz der Privatsphäre

Rechtlicher Schutz bei der Verarbeitung personenbezogener Daten

Datenschutz (Privacy[engl.])/ Informationsfreiheit, ...

Digitale Souveränität[IT-Nutzer]

Wahlfreiheit bei der Nutzung von IT-Geräten, -Anwendungen und -Diensten

Einhaltung von Rechtsordnung und **gesellschaftlicher Zusammenhalt** in der digitalen Welt

z. B. Schutz / wirksame Maßnahmen gegen Hass und Hetze, Verführung / Ausbeutung Minderjähriger, betrügerische Anzeigen, Werbung und politische Einflussnahme, Deepfakes, ...

Wie sicher ist „sicher“? – Hardware / Firmware

- Es gibt in der Technik nie eine vollständige (100%) Sicherheit; es verbleiben immer Unwägbarkeiten
- Herstellerseitige Systemsoftware (Firmware / Treiber) kann bereits schädliche Komponenten enthalten
- Besondere Vorsicht ist bei Hardware aus unsicheren Herkunftsstaaten geboten; das deutsche Bundeskriminalamt registrierte bereits im Jahr 2023 bei ausländischen Cyberangriffen einen Zuwachs von rund 28 % gegenüber dem Vorjahr; die meisten dieser Angriffe stammten aus Russland oder China
- Auch einzelne Hardwarehersteller aus vermeintlich sicheren Staaten können, entgegen vollmundiger Versprechen, keine hundertprozentige Sicherheit gewährleisten
- Es besteht vielmehr die große Gefahr, sich in trügerischer Sicherheit zu wiegen

Wie sicher ist „sicher“? - Sabotageschutz*

- Schutz gegen Computerviren, „Trojanische Pferde“ oder „Netzwerkwürmer“ ist heute oft bereits Teil der mit Betriebssystemen ausgelieferten Systemsoftware; manche kostenlose „Antivirensoftware“ forscht Daten auf den installierten Systemen aus
- Dieser technische Schutz erstreckt sich nicht auf Schäden durch vor Betrug, Deepfakes, Phishing u. ä., weil diese Taten nicht auf die Technik, sondern auf die Wahrnehmung, die Täuschung oder das Handeln von Menschen abzielen
- Klassische „Computerviren“ funktionieren nicht auf Geräten unter den Betriebssystemen Android oder Apple iOS / iPadOS; „Antivirensoftware“ ist dort ebenfalls nicht (sinnvoll) lauffähig
- „Trojanische Pferde“ sind dagegen durchaus weit verbreitet und können immense Schäden verursachen; ein gewisser technischer Schutz ist teils in der Systemsoftware von Mobilgeräte enthalten (z. B. Android PlayProtect), größeren Schutz bietet aber das verantwortliche Verhalten der Nutzer bei der Installation von Software
- Auch einzelne Hardwarehersteller aus vermeintlich sicheren Staaten können, entgegen vollmundiger Versprechen, keine hundertprozentige Sicherheit gewährleisten
- Es besteht vielmehr die große Gefahr, sich in trügerischer Sicherheit zu wiegen

* = andere Begriffe. „Malware“, „Schutz gegen Schadsoftware“

Schutz der Privatsphäre

- Wer erreichbar ist, kann gezielt angegriffen werden - E-Mail-Adressen und Telefonnummern ermöglichen Phishing, Schockanrufe, Messenger-Betrug, personalisierte Fake-Nachrichten oder Spam-Kampagnen
- Wissen über Gewohnheiten erleichtert Manipulation - regelmäßige Aufenthaltsorte, Tagesabläufe, Urlaubszeiten oder Einkaufsgewohnheiten helfen bei Betrug, Einbruchsplanung oder glaubwürdigen Täuschungsversuchen
- Das soziale Umfeld wird zum Angriffspunkt - Familienmitglieder, Vereine, Kollegenkreise oder Nachbarschaften liefern Vertrauensbeziehungen für Social Engineering („Bekannter empfiehlt“, „angeblich vom Verein“, „Kollege braucht Hilfe“)
- Fotos, Videos und Beiträge liefern verwertbare Informationen - Gesichter, Stimmen, Wohnorte, Fahrzeuge, Namensschilder, Hobbys oder technische Geräte ermöglichen Identitätsmissbrauch, Deepfakes oder Sicherheitsfragen zu erraten
- Je mehr über Menschen bekannt ist, desto leichter werden gezielte Angriffe - aus vielen kleinen Einzelinformationen entstehen vollständige Persönlichkeits- und Beziehungsprofile; wer wenig über mich weiß, kann mich schwerer täuschen, manipulieren oder unter Druck setzen

Markante Fälle von Datenmissbrauch ...*

2018 – Cambridge-Analytica-Skandal

- 87 Millionen ...

2018–2019 – Massenabgriff über Facebook-Kontaktimport / Suchfunktionen

- ... **Telefonnummern** und Profilen ...

2021 – Veröffentlichung eines Facebook-Datensatzes mit 533 Millionen Nutzern

- … **Telefonnummer**

2022 – Datensatz mit rund 400 Millionen **WhatsApp**-Telefonnummern

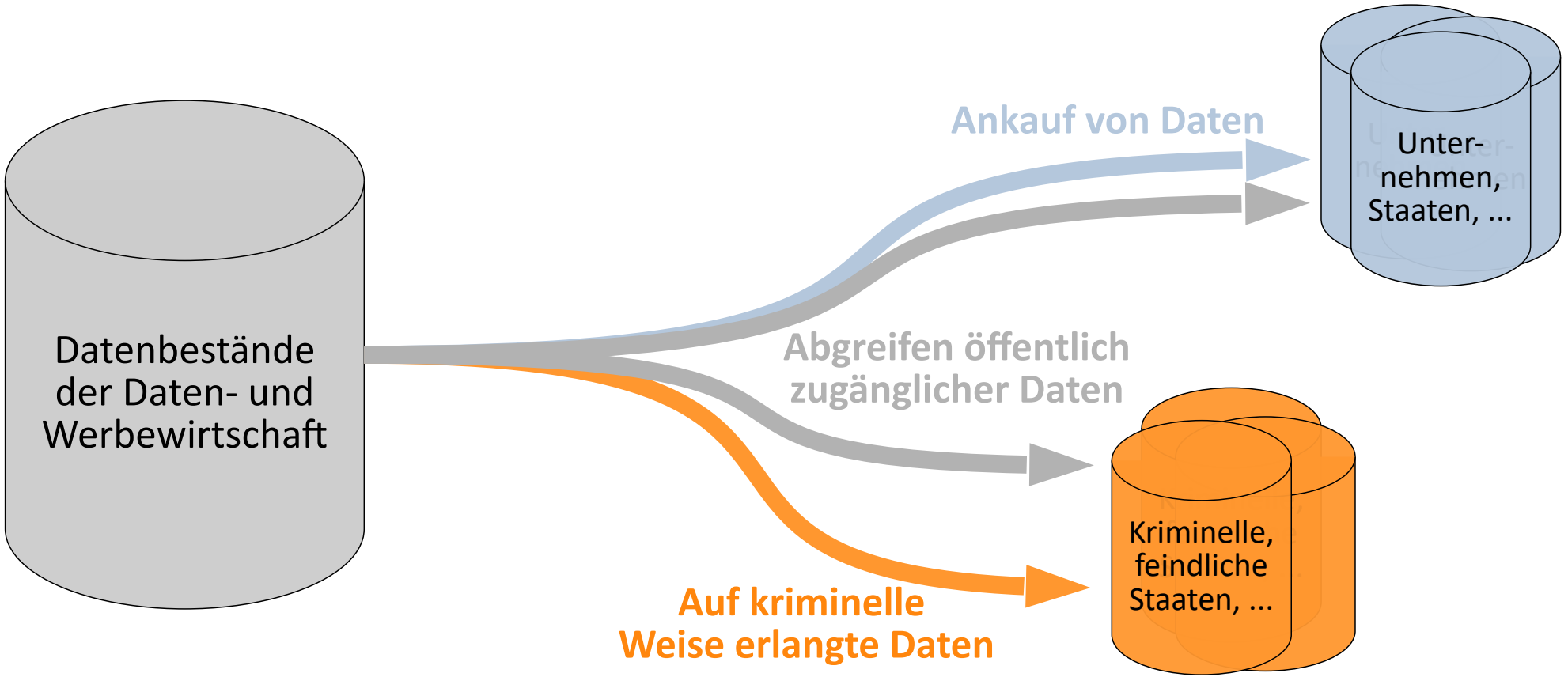
- ... und anschließend in Hackerforen zum Verkauf angeboten

2025 – „WhatsScraping“-Forschungsprojekt (Wien) – 3,5 Milliarden **WhatsApp**-Profilinformationen

- ... **Telefonnummern** ...

* = durch, teilweise automatisiertes, Abgreifen öffentlich zugänglicher Daten

Nutzniesser von Datenhandel / -Missbrauch



Empfehlung!

WDR-Dokumentation

Hirschhausen und die Deepfake-Mafia

ARD-Mediathek

https://www.ardmediathek.de/

… einzelne Aussagen aus dem Video ...

- … und was ja verrückt ist, dass Meta Platform, Inc. ein sehr bewusstes Interesse daran hat, genau solche Inhalte auszuspielen …
- … machte nach eigenen Schätzungen allein 2024 16 Mrd. Dollar, also 10% ihres Umsatzes, mit bewusstem Betrug ...
- ... wenn wir jetzt nicht handeln, steht die liberale Demokratie vor dem Haus
- … weil die Europäische Union Angst vor den USA hat

Deepfakes – Relativierung der Wirklichkeit*

- Deepfakes machen nicht nur Lügen möglich, sondern untergraben die Grundlage, auf der Wahrheit überhaupt noch erkannt werden kann.
- Bilder, Stimmen und Videos können heute glaubhaft synthetisch erzeugt werden - was sichtbar ist, ist keineswegs zwangsläufig real.
- Mittels Technik kann immer mehr Information erzeugt werden, zugleich sinkt deren Verlässlichkeit.
- Informationen werden zunehmend weniger danach bewertet, ob sie zutreffen, sondern ob sie in bestehende Erwartungs- und Deutungsmuster passen.
- Die Folge ist eine Entwicklung hin zu „Unsicherheit als Normalzustand“, in der die Unterscheidung zwischen authentisch und manipuliert dauerhaft fragiler wird.

Quelle: „Die Realität hat ein Echtheitsproblem“ 09.05.26 Julia Engels bei Telepolis

Gezielte Reiz und Informationsüberlastung*

- Die Geschwindigkeit digitaler Kommunikation überholt zunehmend die Möglichkeiten deren verlässlicher Überprüfung.
- Deepfakes können insbesondere in Zeiten hohen Zeitdrucks – etwa vor Wahlen oder während internationaler Krisen – Wirkung entfalten, bevor ihre Fälschung nachweisbar ist.
- Selbst eindeutig identifizierte Manipulationen verlieren ihre gesellschaftliche und politische Wirkung häufig nicht vollständig.
- Die massenhafte Überflutung des Informationsraums mit widersprüchlichen, emotionalisierenden oder irreführenden Inhalten erschwert Orientierung und öffentliche Verständigung.
- Deepfakes wirken damit nicht nur als Werkzeug der Desinformation, sondern als Verstärker von Vertrauensverlust, Polarisierung und gesellschaftlicher Desorientierung.

* = „Flood the zone with shit“ – wird dem früheren Trump-Berater Steve Bannnon zugeschrieben

Digitale Souveränität / Wahlfreiheit - Problem

- Abhängigkeit von US-amerikanischer Regierungspolitik
- Abhängigkeit von wenigen Anbietern - Kaum echte Alternativen. Vorgaben der Anbieter müssen akzeptiert werden.
- Erschwerter Anbieterwechsel - Daten, Kontakte oder Käufe bleiben an Plattformen gebunden.
- Weniger Datenschutz - Datensammlung und Profilbildung oft kaum vermeidbar.
- Zusätzliche Kosten und Einschränkungen - Proprietäre Formate und fehlende Kompatibilität erzeugen neue Kosten.
- Kontrolle durch große Plattformen - Wenige Unternehmen bestimmen Zugänge, Anwendungen und Kommunikationswege

Digitale Souveränität / Wahlfreiheit gewinnen

- Alternativen nutzen: Andere Geräte, Betriebssysteme, Anwendungen und Dienste wählen → weniger Abhängigkeit von einzelnen Konzernen
- Offene Formate verwenden: Dateien exportierbar speichern → leichter Wechsel zu anderen Programmen und Diensten
- Eigene Daten selbst sichern: Backups, Passwortmanager und Zwei-Faktor-Anmeldung nutzen → mehr Kontrolle über Zugänge und Daten
- Datensparsame Dienste bevorzugen: Anbieter wählen, die weniger Daten sammeln und transparenter arbeiten
- Bewusst entscheiden: Browser, Messenger oder Suchmaschine gezielt auswählen → mehr Wahlfreiheit und Selbstbestimmung

Wenn Sie mehr wissen wollen ...

vhs KARLSRUHE

Wie sicher ist „sicher“? – Sicherheit in der digitalen Welt

Was Sie wirklich wissen sollten; Kurzvortrag

Sicherheit in der digitalen Welt bedeutet mehr als nur starke Passwörter oder eine gute Verschlüsselung. Der Schutz der Privatsphäre und die digitale Souveränität tragen ebenfalls zur digitalen Unversehrtheit bei – gerade angesichts der marktbeherrschenden Digitalkonzerne.

Viele Schutzversprechen erweisen sich bei genauerem Hinsehen als trügerisch, wie z. B. die viel beworbene Ende-zu-Ende-Verschlüsselung, die nicht vor der Auswertung von Metadaten oder rechtlichen Risiken durch das Fehlverhalten von Diensteanbietern oder Gesprächspartnern schützt. Hinzu kommt die gezielte Irreführung durch manipulative Gestaltungsstrategien, die Nutzer zu Entscheidungen drängen, die nicht in ihrem Interesse liegen (sogenannte „Dark Pattern“).

Der Vortrag gibt einen Überblick über aktuelle Risiken für die digitale Selbstbestimmung und zeigt Auswege auf.

Kursnummer: 262-67054

kostenlos

Start: Sa. 11.07.2026 15:45 Uhr

Ende: Sa. 11.07.2026 17:00 Uhr

1 Termin / 1.67 Ustd.