

Skript Vortrag Datenschutz vs. Bequemlichkeit

Adrian Scheibe & Camillo Ballandt

12. Mai 2023

Inhaltsverzeichnis

1 Einführung	1
1.1 Auftreten von Datenschutz	1
1.2 Definitionen	1
1.3 Wichtigkeit von Datenschutz	1
2 Aktuelle Problempunkte	1
2.1 Softwaretelemetrie	1
2.2 Online-Tracking	2
2.3 Verwendung der Daten	2
3 Lösungsansätze	2
3.1 Open-Source-Software	2
3.2 Anonyme Telemetrie	2
3.3 Monopole vermeiden	2
3.4 Datenschutz im Browser	2
3.5 Staatliche Regulierung	3
4 Diskussion	3
5 Fazit	3

1 Einführung

1.1 Auftreten von Datenschutz

Analog

- Mündliche Informationsweitergabe
- Briefgeheimnis
- Unantastbarkeit der Wohnung

Digital

- Geheimer Informationsaustausch
- Sichere Datenspeicher

1.2 Definitionen

Definition 1.1 (Daten) *Daten sind eine wieder interpretierbare Darstellung von Information in formalisierter Art, geeignet zur Kommunikation, Interpretation oder Verarbeitung.*“

Definition 1.2 (Telemetrie) *Sammeln von Rohdaten innerhalb einer Anwendung, die im Hintergrund an den Entwickler übertragen werden.*

1.3 Wichtigkeit von Datenschutz

- Gesetzlich verankert (DSGVO)
 - Privatsphäre
 - Anonymität
 - Selbstbestimmung
- Argument: „Ich habe nichts zu verbergen.“
- Ungerechtfertigter Profit aus personenbezogenen Daten
 - Veränderung/Verkürzung von Daten
 - Änderung persönliche Einstellungen

2 Aktuelle Problempunkte

2.1 Softwaretelemetrie

Arten

- Mit/ohne personenbezogenen Daten
- Opt-in/opt-out (Mit Zustimmung/Mit Widerspruch)
- Programmebene
- Betriebssystem-Ebene (z.B. Windows-Nutzungsdaten, Problemlösung)

2.2 Online-Tracking

- Cookies für z.B. Anmelde- oder Einstellungsdaten
- Cross-Site Tracking für Erstellung eines „Nutzerprofils“
- Suchmaschine (Werbezwecke, Vorschlagsverbesserung, Umfragen)
- Soziale Netzwerke (Maximale Zeit in Netzwerk)
- Online-Shopping (Vorschläge, Preisanpassung)

2.3 Verwendung der Daten

- Werbevorschläge
- KI-Training
- Verhaltensforschung/Umfragen
- Erstellung Identitätsprofil
- Verkauf auf „Datenbörse“ (⇒ Riesige Industriebranche)

Sind personenbezogene Daten sicher?

- Nein
- Selbst Firmen mit Datenschutzziel nutzen personenbezogene Daten (Bsp. Apple)

3 Lösungsansätze

3.1 Open-Source-Software

Open-Source → quelloffen

- Code frei einsehbar, ausführbar, modifizierbar

Vorteile

- Code wird von vielen unabhängigen Akteuren geprüft
- Höhere Sicherheit/Datenschutz
- Kann kopiert und selbst weiterentwickelt werden

Nachteile

- Jeder kann Daten einsehen und Schwachstellen erkennen
- Erschwerte Monetarisierung

Beispiele für Open-Source-Software (OSS)

- Betriebssysteme: BSD, Linux (Android)
- Professionelle Anwendungen: OBS, VLC, Chromium
- Office Suite: Libreoffice, Onlyoffice (siehe Lernsax)
- Programmiersprachen: Python, Java, C
- Serverbetriebssystem (Linux sehr verbreitet)
- Für fast jeden Einsatzzweck

3.2 Anonyme Telemetrie

- Telemetrie für Debugging, Weiterentwicklung nützlich
- ohne personenbezogene Daten (nur generische Informationen)
- Nur mit Zustimmung (opt-in)
- Besseres Image für Betreiber

3.3 Monopole vermeiden

- Fast jeder Browser basiert auf Chromium (großer Einfluss von Google)
- Windows dominiert bei Desktop-Betriebssystemen
- Weitere Beispiele (Messenger: WhatsApp, Suchmaschine: Google)

3.4 Datenschutz im Browser

- Extension (Werbeblocker, https, kein JavaScript)
- Sichere Proxy oder DNS-Resolver
- VPN
 - Potenzielles Risiko (Datenverkehr von Betreiber kontrolliert, Vertrauen notwendig)
 - Oft Datenlecks, langsam

- Tor-Netzwerk
 - Bester Datenschutz (Exit-Nodes wunder Punkt)
 - Sehr langsam, begrenzt

3.5 Staatliche Regulierung

- Gesetzliche, verbindliche Rahmenbedingungen
- Bsp. DSGVO (Zustimmung für Cookies notwendig)
- Oft zu geringe Strafen für Nichteinhalten (z.B. Google)
- Staat hat Interessen abseits von Datenschutz (z.B. Überwachung)

4 Diskussion

1. Soll der Staat weitere Gesetze zum Datenschutz einführen?

Pro	Kontra
	Derzeitige Gesetze verbessern
	Nur internationale Gesetze sinnvoll

2. Sollten die Algorithmen sozialer Netzwerke und / oder KIModelle offengelegt werden müssen?

Pro	Kontra
Experten können Algorithmen beurteilen	Schwer zu verstehen

Welche Datenschutzoptionen sind sinnvoller als andere?

Sinnvoll	Schwächer
VPNs (bequem, sicher)	Tor (langsam)
Weniger Internet nutzen	

Können Open-Source-Programme (wie Libreoffice) die proprietären Standards (wie Word) ersetzen?

Pro	Kontra
Für Standardfunktionen ausreichend	Unkenntnis bei breiter Masse
kostenfrei	Vorteile nicht einfach ersichtlich
	Weniger komfortabel

Individuelle Ansprüche sind entscheidend

5 Fazit

- Komplette Privatsphäre in heutiger digitalisierter Gesellschaft nicht (mehr) gewährleistet
- Schon immer Kampf Privatsphäre vs. Komfort/Sicherheit
- Daten als Machtinstrument
- Gute Anonymität jedoch mit wenig Aufwand möglich
- Aufklärung/Aufmerksamkeit für Thema stärken
- Privatsphäre ist auch für Menschen, die „nichts zu verstecken haben“