



datenschutzkonformes Webtracking?

Dr. Stefan Schleipfer

Datenschutzkonformes Webtracking

Bedeutet nach weitverbreiteter Ansicht:

- IP-Adressen nur verkürzt speichern
- über Verwendung von Cookies unterrichten (oder Einwilligung?)
- über Verwendung von Fingerprints unterrichten (oder Einwilligung?)
- Widerspruchsrecht, Unterrichtungspflichten

Im Mittelpunkt der Betrachtung: technische Details wie:
IP-Adressen, Cookies und Fingerprints

Datenschutzkonformes Webtracking

Im Mittelpunkt der Betrachtung: IP-Adressen

- „Ist die IP-Adresse ein personenbezogenes Datum?“ nach weit verbreiteter Ansicht grundlegendste Frage im Internet-Datenschutz
- intensive Beschäftigung mit IP-Adressen in Literatur und bei den Aufsichtsbehörden
- einige Gerichtsurteile, aktuell: 28.10.2014: BGH fragt EuGH

Im Mittelpunkt der Betrachtung: Cookies

- seit Ende der 90er-Jahre intensiv diskutiert
- Art. 5 Abs. 3 der ePrivacy-Richtlinie 2009 („Cookie-Richtlinie“), dazu bereits 4 Stellungnahmen der Art.-29-Gruppe

Im Mittelpunkt der Betrachtung: Fingerprints

- Diskussion um Personenbezug und Zulässigkeit

Datenschutzkonformes Webtracking

Im Mittelpunkt der Betrachtung: IP-Adresse, Cookies und Fingerprints

- sind nur technische Details im Webtracking
- Sind dies diejenigen Komponenten, die die Rechte der Nutzer beim Thema Webtracking / Nutzungsprofile am meisten in Gefahr bringen?

Im Folgenden untersucht:

- Was ist datenschutzkonformes Webtracking?
- Gefahren für Verletzung dieser Anforderungen, insbes. Rollen von IP-Adressen, Cookies und Fingerprints dabei



Datenschutzkonformes Webtracking

In Deutschland: Telemediengesetz (TMG)

- enthält allgemeine Bestimmungen zu Nutzungsprofilen

Daraus ableitbar allgemeine Regeln:

- Welche Daten dürfen in Nutzungsprofilen gespeichert werden?
Antwort gilt auch für IP-Adressen, Cookie-Inhalte und Fingerprints.
- Welche Auswertungen / Verarbeitungen sind auf Nutzungsprofilen zulässig?
- Wozu dürfen die Auswertungen verwendet werden?

Zentrale TMG-Bestimmung zu Nutzungsprofilen §

§ 15 Abs. 3 Satz 1 TMG:

- „Der Diensteanbieter darf für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien Nutzungsprofile bei Verwendung von Pseudonymen erstellen, sofern der Nutzer dem nicht widerspricht.“

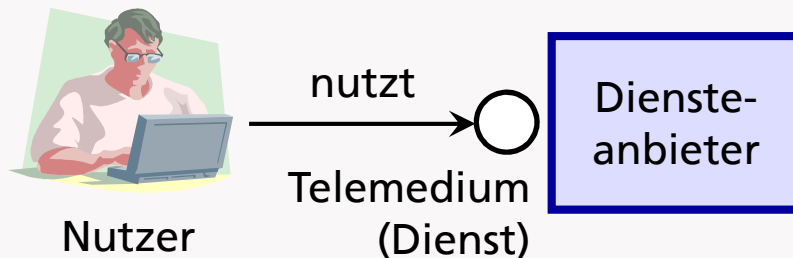
Zentrale TMG-Bestimmung zu Nutzungsprofilen §

§ 15 Abs. 3 Satz 1 TMG:

- „Der **Diensteanbieter** darf für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der **Telemedien** Nutzungsprofile bei Verwendung von Pseudonymen erstellen, sofern der **Nutzer** dem nicht widerspricht.“

Grundlegend für die DS-Bestimmungen im TMG:

- Anbieter-Nutzer-Verhältnis:



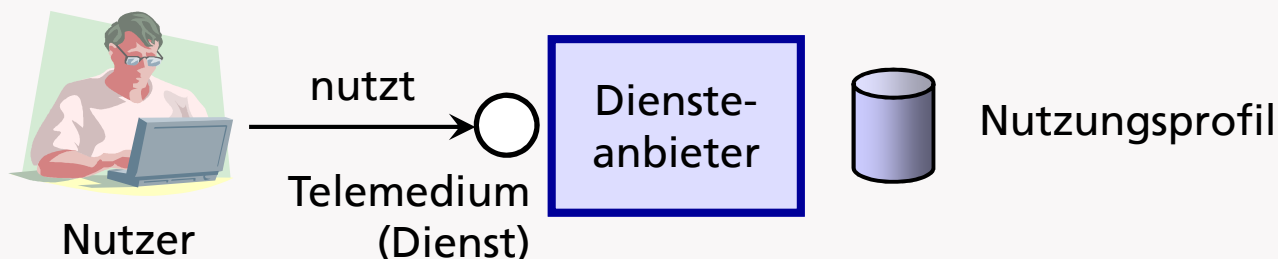
Zentrale TMG-Bestimmung zu Nutzungsprofilen §

§ 15 Abs. 3 Satz 1 TMG:

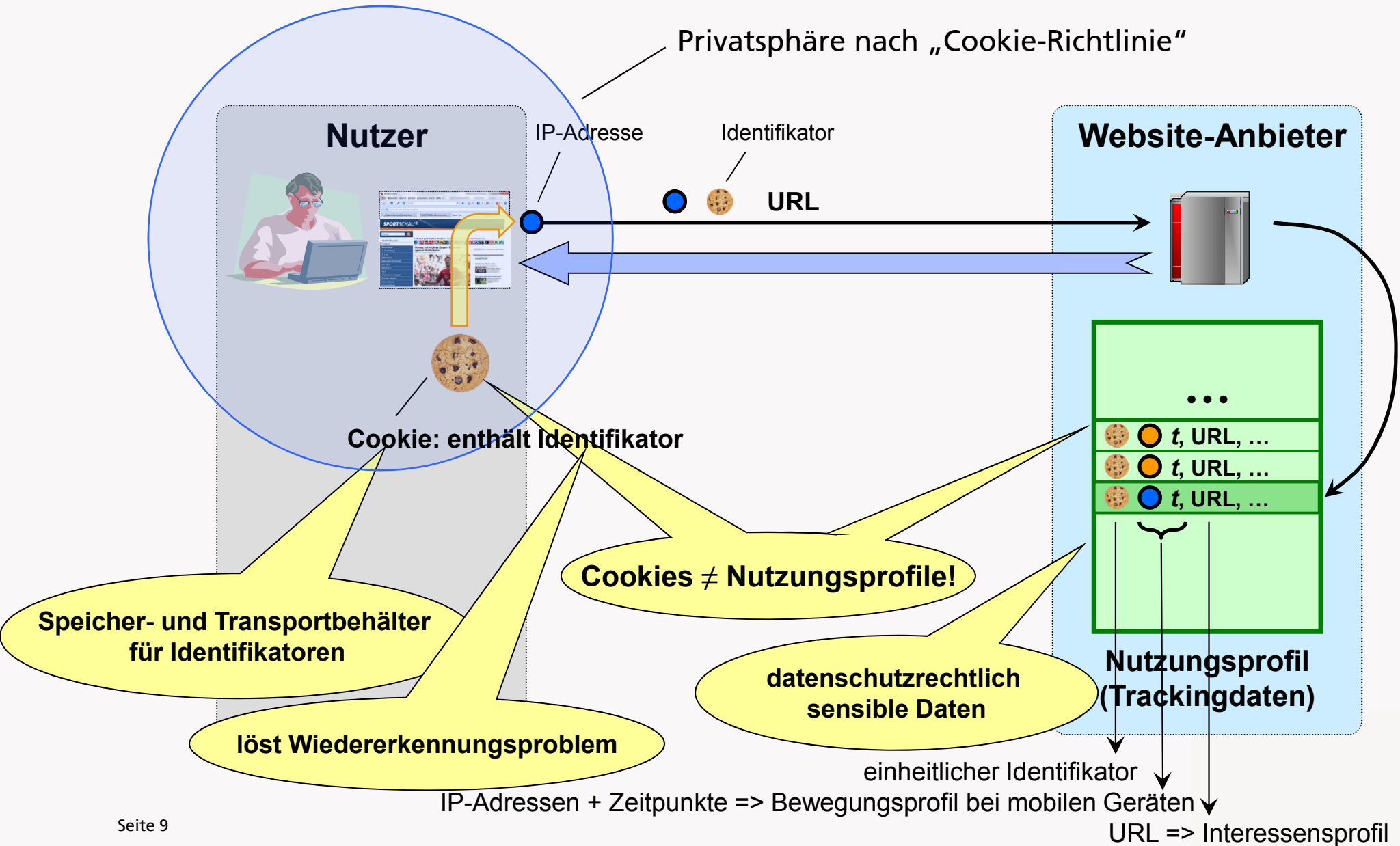
- „Der Diensteanbieter darf für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien **Nutzungsprofile** bei Verwendung von Pseudonymen erstellen, sofern der Nutzer dem nicht widerspricht.“

Nutzungsprofil:

- aufgezeichnete und ausgewertete Protokolldaten über die Inanspruchnahme eines Dienstes („Telemedium“) des Diensteanbieters durch einen Nutzer



Nutzungsprofile technisch (lokale)





Rechte der Nutzer

hängen entscheidend ab nicht vom Umgang mit Cookies:

- nur technische Lösung des Wiedererkennungsproblems

sondern vom Umgang mit Nutzungsprofilen:

- in Nutzungsprofilen nur anonyme / pseudonyme oder auch personenbezogene Daten gespeichert?
- Auswertungen: statistisch – individuell?
- Nutzungsprofile der Person zugeordnet und mit personenbezogenen Daten verknüpft?
- Nutzungsprofile an Dritte übermittelt?

Zentrale TMG-Bestimmung zu Nutzungsprofilen §

§ 15 Abs. 3 Satz 1 TMG:

- „Der Diensteanbieter darf für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien Nutzungsprofile bei Verwendung von **Pseudonymen** erstellen, sofern der Nutzer dem nicht widerspricht.“



Pseudonym

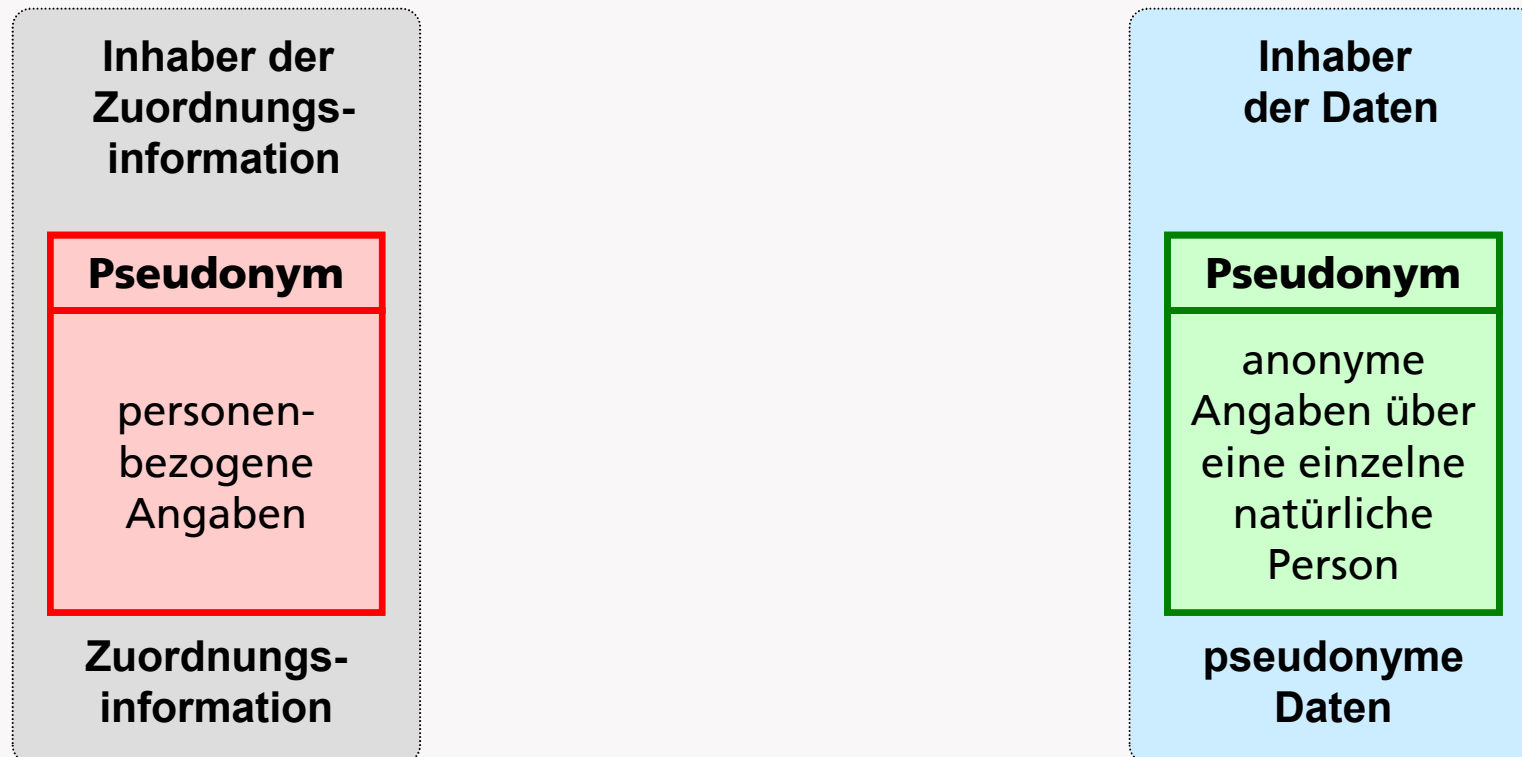
Begriffe:

- Pseudonym: in BDSG+TMG nicht definiert
- pseudonyme Daten: in BDSG+TMG nicht definiert
- BDSG 2001 definiert Pseudonymisieren = Vorgang, der aus personenbezogenen Daten pseudonyme Daten macht:
Passt nicht: Nutzungsprofile sind von vorn herein pseudonym zu erstellen!
- TMG setzt Begriff „Pseudonym“ als bekannt voraus



Pseudonyme Daten

Kennzeichnende Eigenschaft: Funktionstrennung



Zusammenführung weiter möglich, u.U. auch zulässig (über Pseudonym)



Pseudonym

Kennzeichnende Eigenschaften:

- Kennzeichen einer einzelnen natürlichen Person
- Inhaber der Daten kann Pseudonym nicht der Person zuordnen.
Pseudonym ist für ihn anonym (Anforderung!).
- Inhaber der Zuordnungsinformation kann Pseudonym der Person zuordnen.
Pseudonym ist für ihn personenbezogen.



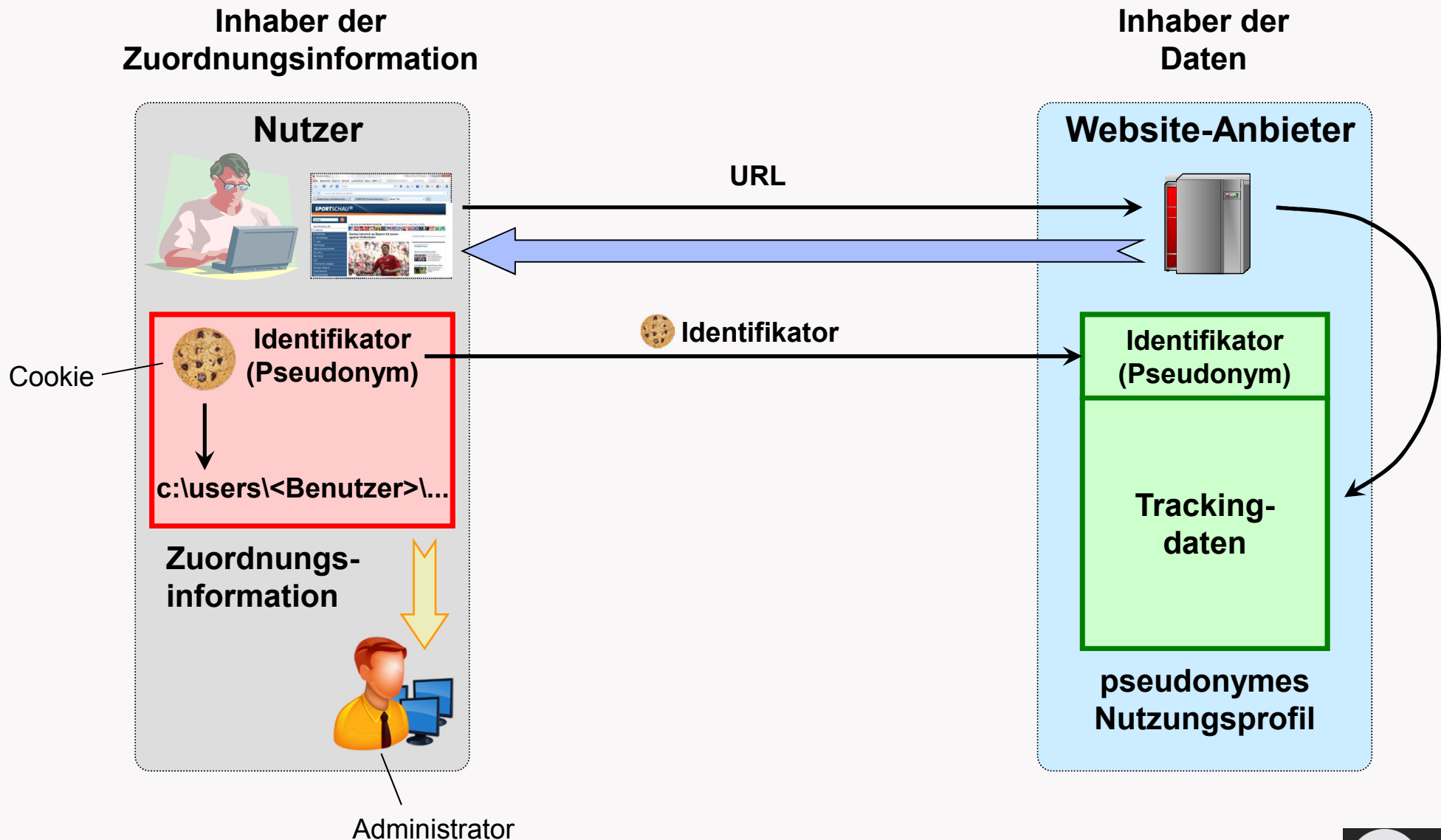
Pseudonyme Daten

Daten mit Funktionstrennung:

- Identifiziert durch Pseudonym
- Dateninhaber hat die Daten, aber nicht die Zuordnungsinformation.
=> kann die Daten nicht der Person zuordnen.
=> pseudonyme Daten sind für ihn anonym (Anforderung!).
- Inhaber der Zuordnungsinformation hat die Zuordnungsinformation, (in der Regel) aber nicht die Daten.
=> pseudonyme Daten sind für ihn personenbezogen, falls er sie hat.



Nutzungsprofile unter Pseudonym



Pseudonyme Nutzungsprofile: zulässige Inhalte §

„Nutzungsprofile bei Verwendung von Pseudonymen“

=> Zulässige Inhalte für Identifikatoren und andere Datenfelder:

- anonyme oder pseudonyme Daten, d.h. Daten, die der Anbieter nicht der Person des Nutzers zuordnen kann

Verbotene Identifikatoren / verbotene Datenfelder:

- Kundennummer
- Login-Name
- E-Mail-Adresse
- Name, Vorname
- ...

Pseudonyme Nutzungsprofile: zulässige Inhalte §

Zulässige Identifikatoren / zulässige Datenfelder:

- Zufallszahl, ohne Bezug zur Person
- Hashwerte der obigen Identifikatoren, von denen nicht zurück auf die Person geschlossen werden kann
- IP-Adressen (sind Pseudonyme, soweit einer Person zugeordnet)
- Fingerprints (sind Pseudonyme, soweit einer Person zugeordnet)



TMG-Bestimmungen zu Nutzungsprofilen

Der Diensteanbieter

Der Diensteanbieter darf für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien Nutzungsprofile bei Verwendung von Pseudonymen erstellen, sofern der Nutzer dem nicht widerspricht.

- darf Nutzungsprofile unter Pseudonym erstellen, § 15 (3) 1

- muss über Erstellung von Nutzungsprofilen (+ Cookies) informieren, § 13 (1) 2

Bei einem automatisierten Verfahren, das eine spätere Identifizierung des Nutzers ermöglicht und eine Erhebung oder Verwendung personenbezogener Daten vorbereitet, ist der Nutzer zu Beginn dieses Verfahrens zu unterrichten.

- muss Widerspruchsrecht gegen Erstellung von Nutzungsprofilen einräumen, § 15 (3) 1

Der Diensteanbieter darf ... Nutzungsprofile bei Verwendung von Pseudonymen erstellen, sofern der Nutzer dem nicht widerspricht.

- muss über Widerspruchsrecht informieren, § 15 (3) 2

Der Diensteanbieter hat den Nutzer auf sein Widerspruchsrecht im Rahmen der Unterrichtung nach § 13 Abs. 1 hinzuweisen.

- muss Zusammenführungsverbot beachten, § 15 (3) 3

- muss Zusammenführungsverbot durch technische und organisatorische Maßnahmen absichern, § 13 (4) Nr. 6

Diese Nutzungsprofile dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden.

alle Bestimmungen eingehalten, datenschutzkonformes Webtracking

Der Diensteanbieter hat durch technische und organisatorische Vorkehrungen sicherzustellen, dass ...
6. Nutzungsprofile nach § 15 Abs. 3 nicht mit Angaben zur Identifikation des Trägers des Pseudonyms zusammengeführt werden können.



Ausrichtung des TMG bzgl. Nutzungsprofile

Generelle Zielrichtung des TMG:

- Zuordnung des Nutzungsprofils zur Person des Nutzers verhindern:

- ① keine Angabe im Nutzungsprofil,
aus der der Anbieter die Person des Nutzers ableiten könnte
=> Nutzungsprofile unter Pseudonym
- ② nachträgliche Zuordnung zur Person verhindern
=> Zusammenführungsverbot

- Kompromiss zwischen dem Interesse des Nutzers an weitgehender Anonymität in seinem Nutzungsverhalten und dem berechtigten Interesse des Diensteanbieters an der Auswertung der Inanspruchnahme seiner Dienste (Gesetzesbegründung TDDSG 1997)
=> keine absolute Anonymität!

- ③ Widerspruchsrecht des Nutzers



Wertung TMG zu Nutzungsprofilen

- regulieren nicht technische Details (IP-Adressen, Cookies, Fingerprints), sondern Nutzungsprofile, allgemeingültig und technologieneutral
- setzen klare Grenzen in
 - ▶ Erhebungsphase: nur anonyme und pseudonyme Daten
 - ▶ Auswertungsphase: Zusammenführungsverbot
 - ▶ Anwendungsphase: nur für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien
- Widerspruchsrecht bietet Anreiz zur Verarbeitung pseudonymer anstatt personenbezogener Daten

TMG-Bestimmungen von 1997 sind hochmodern => sollen trotz DS-GVO erhalten bleiben!



Angriffe auf pseudonyme Nutzungsprofile

3 Typen von Angriffen:

- Angriff Typ **A**:
Personenbezogenes Datum in pseudonymes Nutzungsprofil
- Angriff Typ **B**:
Zusammenarbeit beider Seiten:
Website-Anbieter erhält Zuordnungsinformation
- Angriff Typ **C**:
Website-Anbieter hat Kontextinformation

Bewertung:

- Typ A: kein pseudonymes Nutzungsprofil mehr
- Typen B+C: Verstoß gegen Zusammenführungsverbot



Angriffe auf pseudonyme Nutzungsprofile

3 Typen von Angriffen:

- **Angriff Typ A:**
Personenbezogenes Datum in pseudonymes Nutzungsprofil
- **Angriff Typ B:**
Zusammenarbeit beider Seiten:
Website-Anbieter erhält Zuordnungsinformation
- **Angriff Typ C:**
Website-Anbieter hat Kontextinformation

Bewertung:

- **Typ A: kein pseudonymes Nutzungsprofil mehr**
- **Typen B+C: Verstoß gegen Zusammenführungsverbot**

Angriffe auf pseudonyme Nutzungsprofile: Typ A



Angriff Typ **A**: Personenbezogenes Datum in Nutzungsprofil
=> kein zulässiges pseudonymes Nutzungsprofil mehr!

- Angriff **A1**: Eingabedaten als URL-Parameter übergeben
- Angriff **A2**: personenbezogenes Newsletter-Tracking

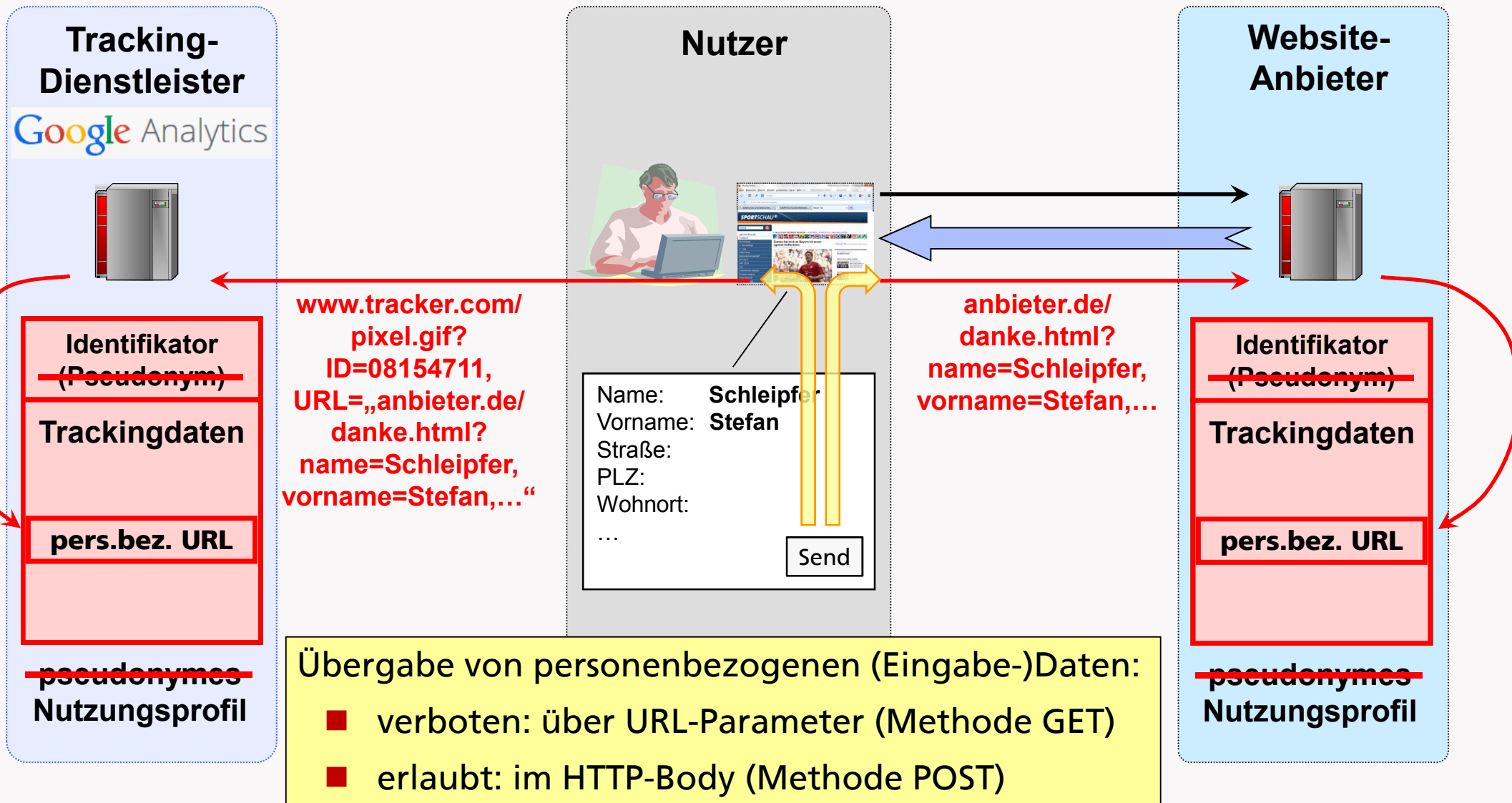
Angriffe auf pseudonyme Nutzungsprofile: Typ A



Angriff Typ **A**: Personenbezogenes Datum in Nutzungsprofil
=> kein zulässiges pseudonymes Nutzungsprofil mehr!

- Angriff **A1**: Eingabedaten als URL-Parameter übergeben
- Angriff **A2**: personenbezogenes Newsletter-Tracking

Angriff A1: Eingabedaten als URL-Parameter



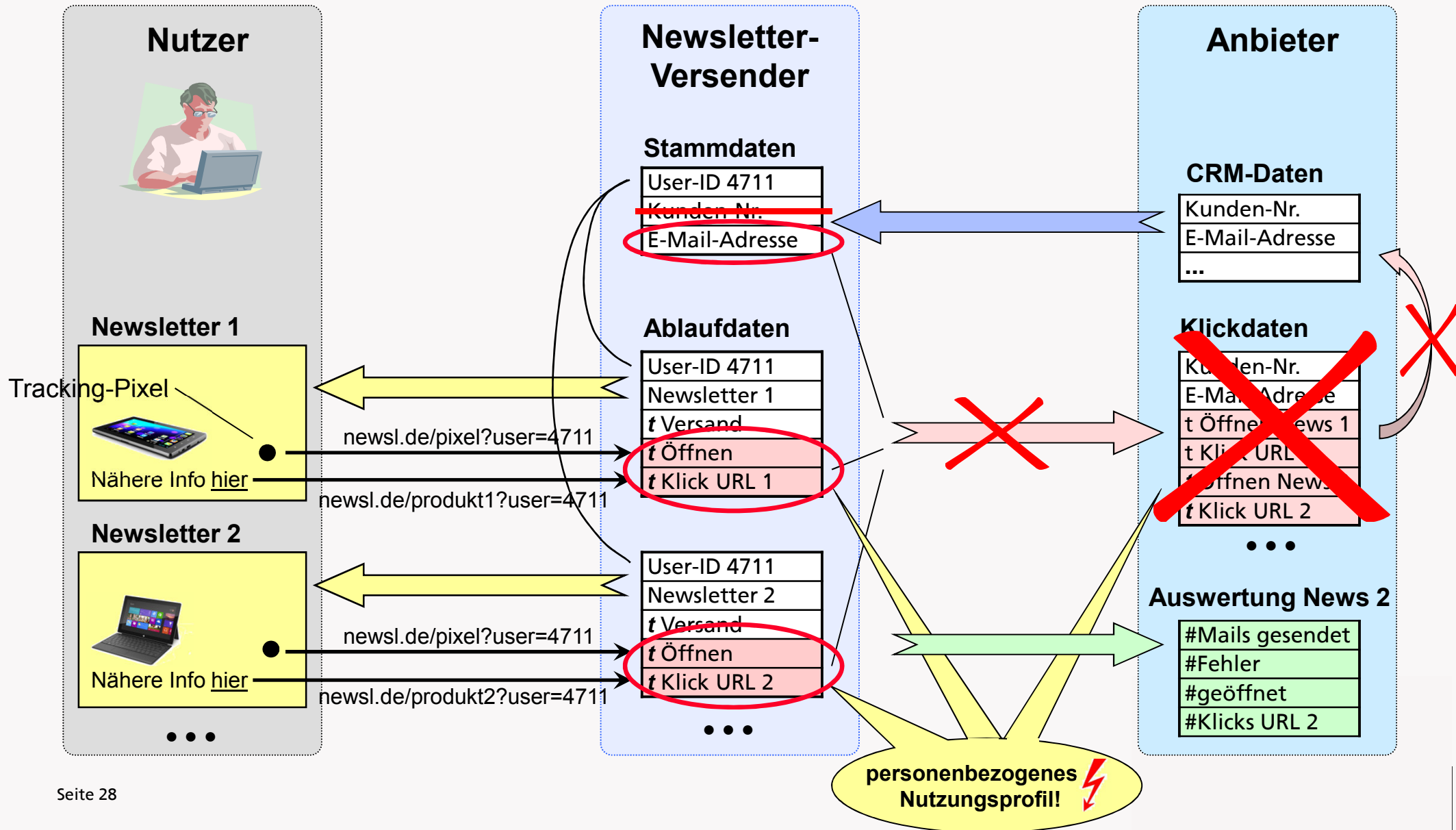
Angriffe auf pseudonyme Nutzungsprofile: Typ A



Angriff Typ **A**: Personenbezogenes Datum in Nutzungsprofil
=> kein zulässiges pseudonymes Nutzungsprofil mehr!

- Angriff **A1**: Eingabedaten als URL-Parameter übergeben
- Angriff **A2**: personenbezogenes Newsletter-Tracking

Angriff A2: personenbez. Newsletter-Tracking





Bewertung Angriffe Typ A

Personenbezogenes Datum in Nutzungsprofil

Angriff	Wie häufig möglich?	Wie schwer?	Ausbeute	zugeordnete Person	Risiko der Entdeckung
A1. Eingabedaten als URL-Parameter	häufig	leicht	Nutzungsprofil Web-Nutzung	Nutzer	mittel
A2. E-Mail-Adresse in Link in E-Mail	immer	leicht	Nutzungsprofil E-Mail-Nutzung	Nutzer	mittel



Angriffe auf pseudonyme Nutzungsprofile

3 Typen von Angriffen:

- Angriff Typ **A**:
Personenbezogenes Datum in pseudonymes Nutzungsprofil
- Angriff Typ **B**:
Zusammenarbeit beider Seiten:
Website-Anbieter erhält Zuordnungsinformation
- Angriff Typ **C**:
Website-Anbieter hat Kontextinformation

Bewertung:

- Typ A: kein pseudonymes Nutzungsprofil mehr
- Typen B+C: Verstoß gegen Zusammenführungsverbot

Angriffe auf pseudonyme Nutzungsprofile: Typ B



Angriff Typ **B**: Zusammenarbeit mit dem Inhaber der Zuordnungsinformation

=> Verstoß gegen Zusammenführungsverbot

- Angriff **B1**: Zuordnung über IP-Adresse
- Angriff **B2**: Zuordnung über Identifikator

Angriffe auf pseudonyme Nutzungsprofile: Typ B

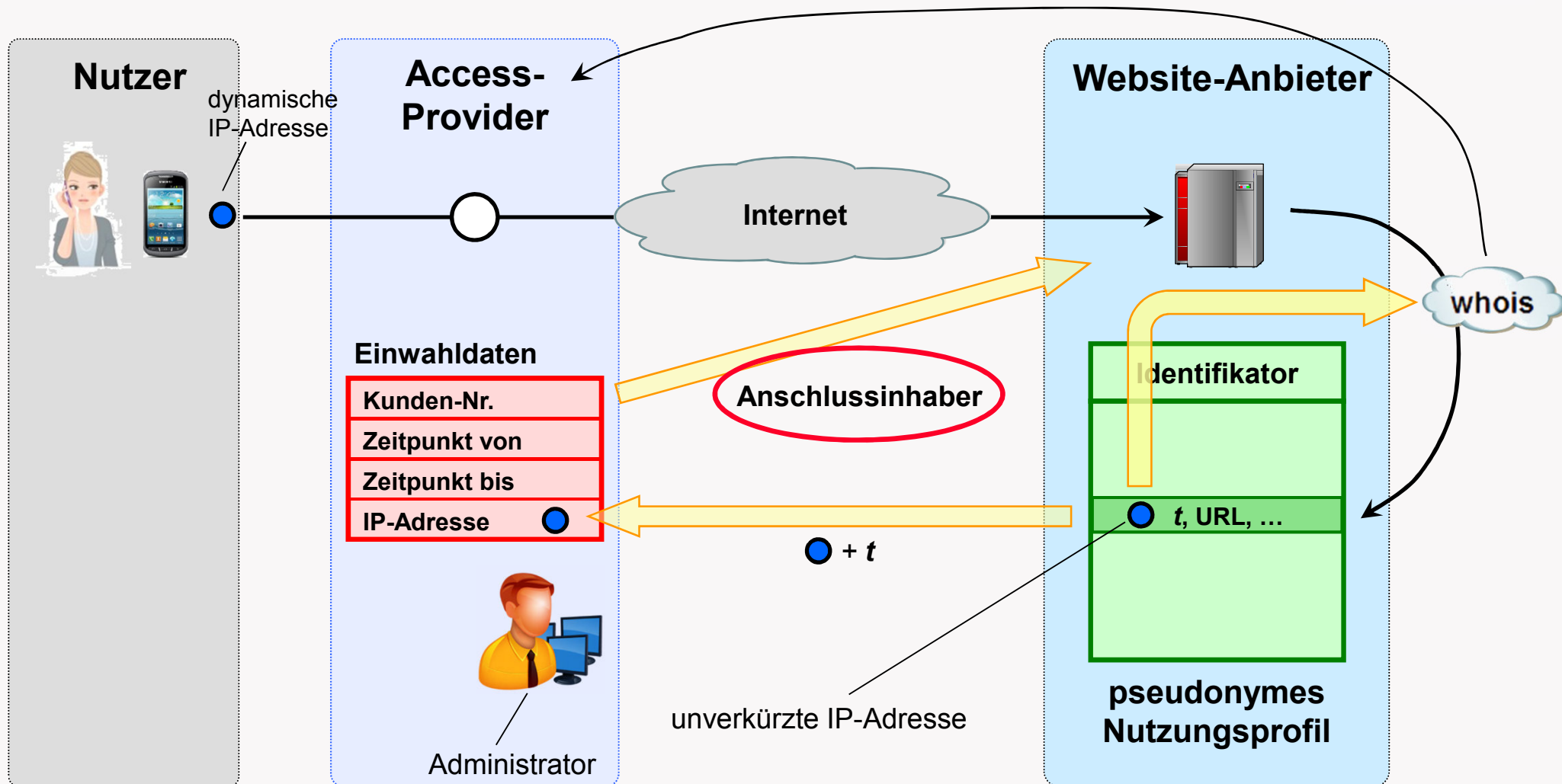


Angriff Typ **B**: Zusammenarbeit mit dem Inhaber der Zuordnungsinformation

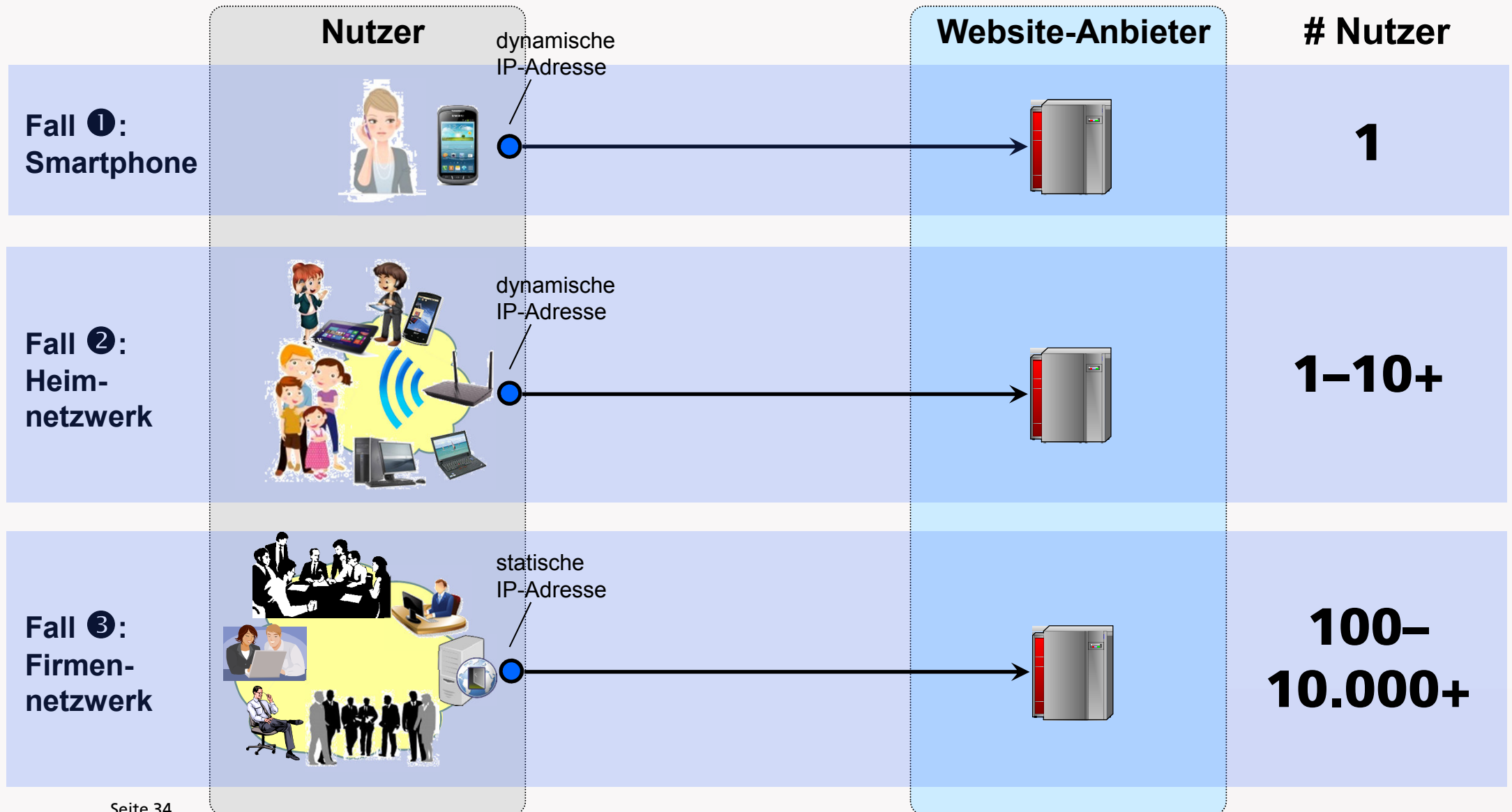
=> Verstoß gegen Zusammenführungsverbot

- Angriff **B1**: Zuordnung über IP-Adresse
- Angriff **B2**: Zuordnung über Identifikator

Angriff B1: Zuordnung über IP-Adresse



IP-Adressen: Anschlussinhaber – Nutzer



Angriffe auf pseudonyme Nutzungsprofile: Typ B

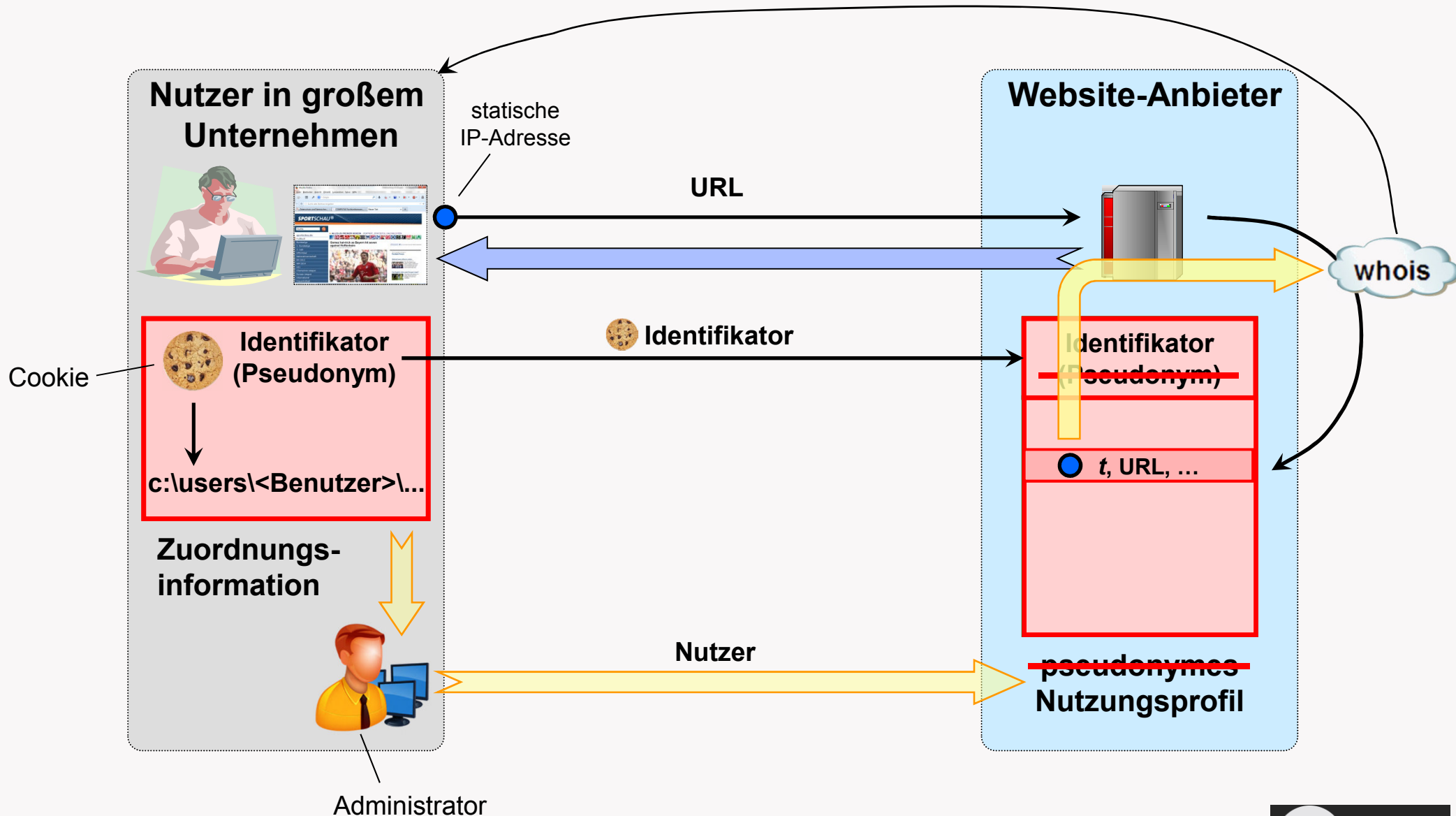


Angriff Typ **B**: Zusammenarbeit mit dem Inhaber der Zuordnungsinformation

=> Verstoß gegen Zusammenführungsverbot

- Angriff **B1**: Zuordnung über IP-Adresse
- Angriff **B2**: Zuordnung über Identifikator

Angriff B2: Zuordnung über Identifikator





Bewertung Angriffe Typ B

Zusammenarbeit mit dem Inhaber der Zuordnungsinformation

Angriff	Wie häufig möglich?	Wie schwer?	Ausbeute	zugeordnete Person	Risiko der Entdeckung
B1. Zuordnung über IP-Adresse	häufig	schwer	Nutzungsprofil Web-Nutzung	Anschluss-Inhaber	hoch
B2. Zuordnung über Identifikator (Cookie)	manchmal	sehr schwer	Nutzungsprofil Web-Nutzung	Nutzer	hoch



Angriffe auf pseudonyme Nutzungsprofile

3 Typen von Angriffen:

- Angriff Typ **A**:
Personenbezogenes Datum in pseudonymes Nutzungsprofil
- Angriff Typ **B**:
Zusammenarbeit beider Seiten:
Website-Anbieter erhält Zuordnungsinformation
- Angriff Typ **C**:
Website-Anbieter hat Kontextinformation

Bewertung:

- Typ A: kein pseudonymes Nutzungsprofil mehr
- Typen B+C: Verstoß gegen Zusammenführungsverbot

Angriffe auf pseudonyme Nutzungsprofile: Typ C



Angriff Typ **C**: Zuordnung über Vergleich mit Kontextinformation
=> Verstoß gegen Zusammenführungsverbot

- Angriff **C1**: Online-Händler: Vergleich mit Bestelldaten
- Angriff **C2**: personenbezogenes Login
- ...

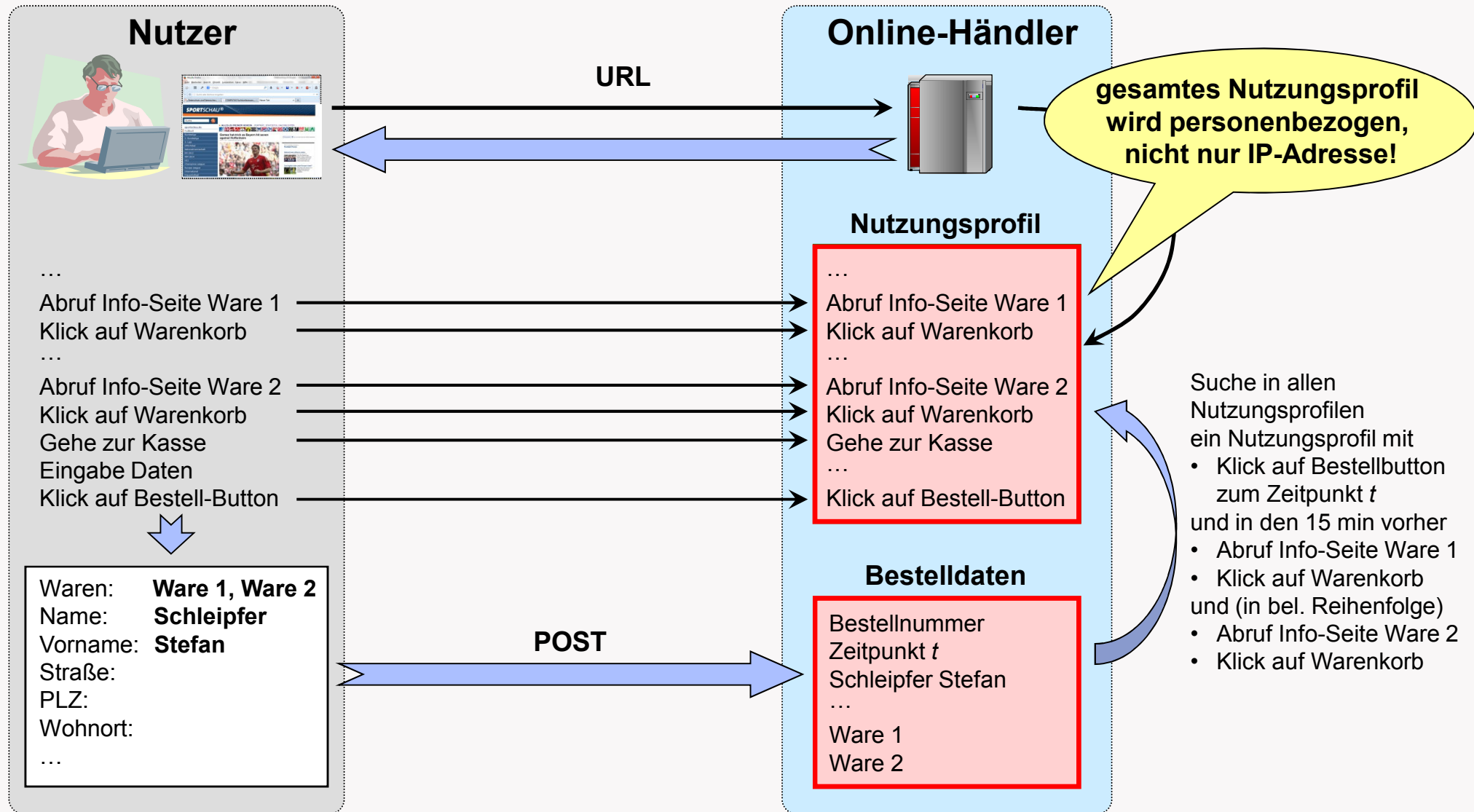
Angriffe auf pseudonyme Nutzungsprofile: Typ C



Angriff Typ **C**: Zuordnung über Vergleich mit Kontextinformation
=> Verstoß gegen Zusammenführungsverbot

- Angriff **C1**: Online-Händler: Vergleich mit Bestelldaten
- Angriff **C2**: personenbezogenes Login
- ...

Angriff C1: Online-Händler: Vergleich mit Bestelldaten



Angriffe auf pseudonyme Nutzungsprofile: Typ C

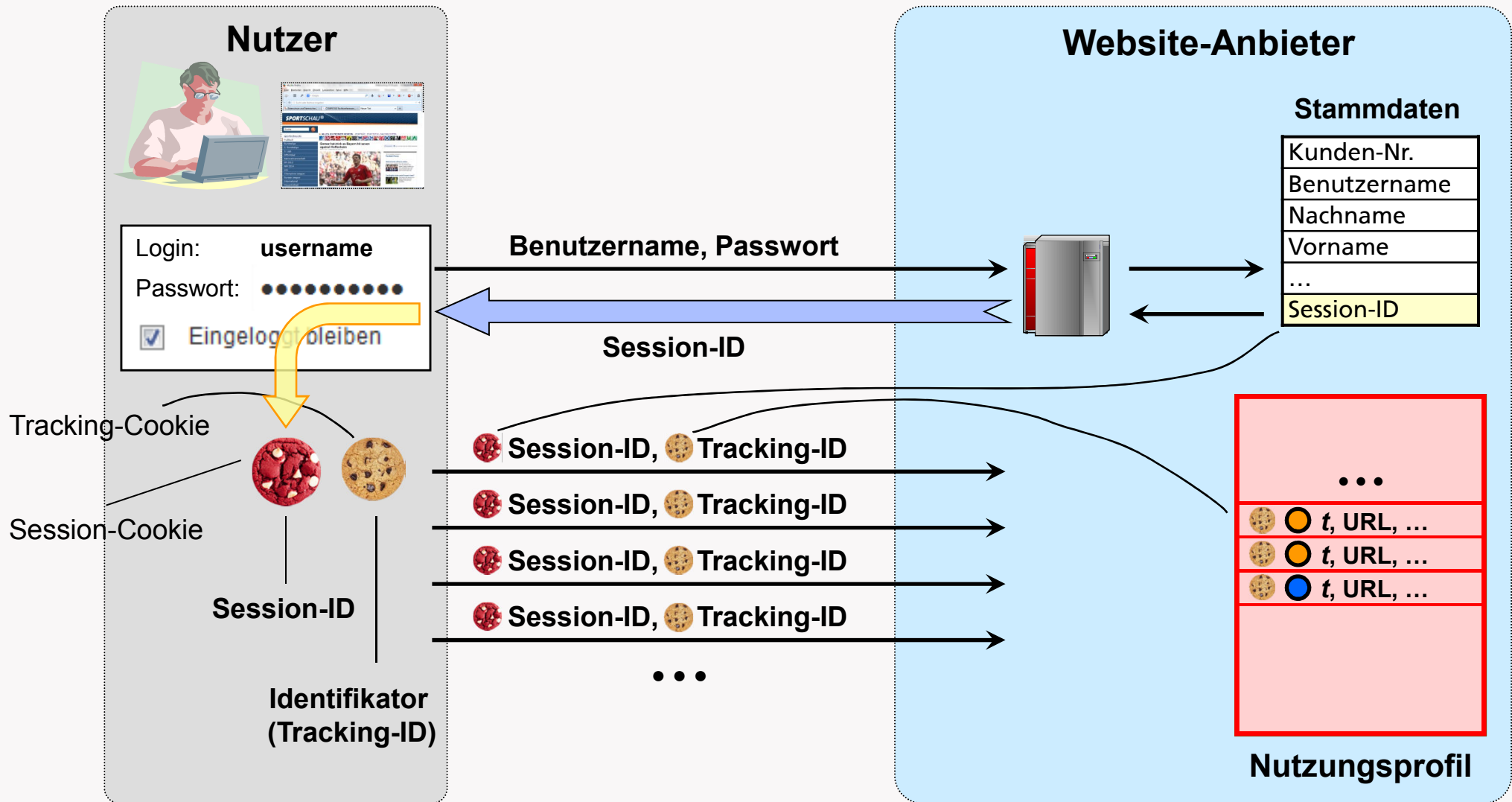


Angriff Typ **C**: Zuordnung über Vergleich mit Kontextinformation
=> Verstoß gegen Zusammenführungsverbot

- Angriff **C1**: Online-Händler: Vergleich mit Bestelldaten
- Angriff **C2**: personenbezogenes Login
- ...



Angriff C2: personenbezogenes Login



Angriffe auf pseudonyme Nutzungsprofile: Typ C



Angriff Typ **C**: Zuordnung über Vergleich mit Kontextinformation
=> Verstoß gegen Zusammenführungsverbot

- Angriff **C1**: Online-Händler: Vergleich mit Bestelldaten
- Angriff **C2**: personenbezogenes Login

Weitere Angriffe (viele!):

- Angriff **C3**: Cookie c_user bei Facebook
- Angriff **C4**: Facebook vergleicht Inhaltsdaten mit Nutzungsprofilen
- Angriff **C5**: Google vergleicht Analytics-Daten mit anderen Daten
- ...



Bewertung der Angriffe Typ C

Zuordnung über Vergleich mit Kontextinformation

Angriff	Wie häufig möglich?	Wie schwer?	Ausbeute	zugeordnete Person	Risiko der Entdeckung
C1. Vergleich mit Eingabedaten	häufig	leicht	Nutzungsprofil Web-Nutzung	Nutzer	niedrig
C2. personenbezogenes Login	häufig	leicht	Nutzungsprofil Web-Nutzung	Nutzer	niedrig

Fazit

Datenschutzkonformes Webtracking:

- ① nur anonyme (oder pseudonyme) Nutzungsdaten ins Nutzungsprofil: betrifft alle Daten im Nutzungsprofil
- ② kein Versuch der Zusammenführung mit Person:
 - keine Zusammenarbeit mit Dritten: betrifft IP-Adressen und Cookie-Identifikatoren
 - kein Ausnutzen von Kontextinformation
- ③ Widerspruchsrecht des Nutzers
- ④ Unterrichtungspflichten, TOMs

Gefahr des Verstoßes:

hohe Gefahr (Typ A)

geringe Gefahr (Typ B)

sehr hohe Gefahr (Typ C)

Fazit

- Nutzungsprofile sind sehr sensible Daten
- Nutzungsprofile sind in der hohen Gefahr, der Person des Nutzers zugeordnet zu werden
- IP-Adressen sind für sich genommen wenig sensible Daten; die Gefahr der Zuordnung von Nutzungsprofilen über IP-Adressen ist gering
- Cookies und Fingerprints sind technische Hilfsmittel zur Lösung des Wiedererkennungsproblems; Cookies werden oft mit Nutzungsprofilen verwechselt

=>

- Auf die Nutzungsprofile kommt es an.
- Ob darin IP-Adressen enthalten sind und ob Cookies / Fingerprints verwendet werden, macht keinen grundlegenden Unterschied.

Literatur

- Stefan Schleipfer: Datenschutzkonformer Umgang mit Nutzungsprofilen. Sind IP-Adressen, Cookies und Fingerprints die entscheidenden Details beim Webtracking? ZD 09/2015 S. 399–405

Vielen Dank



DS-Schleipfer@t-online.de