

Selbstdatenschutz

Identitätsmanagement, Tipps und Tools zum Selbstdatenschutz

Windbergen, 7. November 2016

Harald Zwingelberg



Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Identitätsmanagement im Netz



Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Identität, partielle Identitäten, IdM

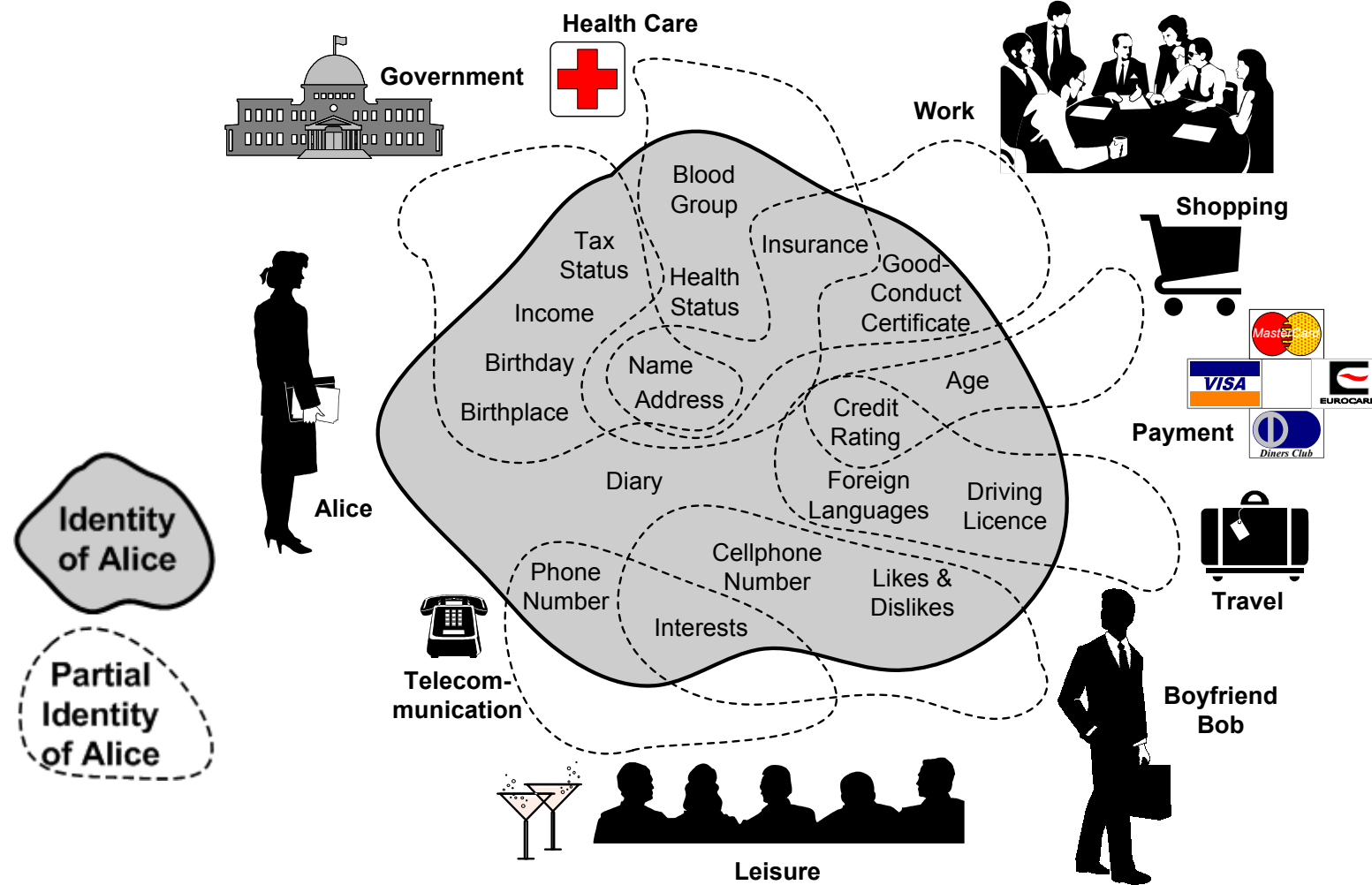
- **Digitale Identität:**
Sammlung von digitalen Informationen, die zu einem Individuum gehören
(z.B. Name, Geschlecht, Geburtstag/-ort, Nutzerkennung)
- **Teilidentitäten:**
Identität, die eine Person in einem bestimmten Kontext oder Rolle bestimmt
- **Identitätsmanagement (IdM):**
das Verwalten von Identitäten oder Identitätsdaten
 - offline: situationsabhängige Angabe von Daten
 - online: Pseudonyme, Avatarnamen, E-Mail-Adressen



Identitätsmanagement

in der Offline-Welt: intuitiv

Teilidentitäten von Alice





Und online ...

Nichts zu verbergen?

Identitätsmanagement online?

ICH BIN MEHR WERT!

DGB

Aktuell Initiative Aktionen Netzwerke Wir über uns

Initiative für Frauen

Die frauenpolitische Initiative „ICH BIN MEHR WERT!“ ist eine

Suchbegriff

beate uhse

SEX UP YOUR LIFE

HOME SHOPPING ONLINE SEX FILIALEN KALENDER

SUCHE

Shopping

1. Suchbereich wählen

ICH BIN MEHR WERT!

GÄRTNER-BLOG

Edellieschen - Impatiens neuguinea

07. August 2008, 08:40 von Gärtnerin



Willkommen im Garten!

Gartenblog-Startseite

Gartenblog-Autoren

Fragen/Gastbeiträge/Bilder schicken

Werben auf dem Gartenblog

Gästebuch

Kommentare - Hinweise

als Newsletter abonnieren

Web © gaertnerblog.de

Google-Suche

JETZT ONLINE - DIE N

Auffallende Kombinationen

Elfenbein oder junge Mode

Finden Sie jetzt die Trends

inklusive sexy Touch!

Einfache Zahlung auch per

HARRY S. MORGAN...

Ist einer der bekanntesten

deutschen Porno-

produzenten. Harry liebt

Reality. Wenn ein Mädchen

kommt, dann zeigt er das

auch.

ONLINE SEX

Entdecken Sie Best-Lieser

Alice Mustermann
Alice.M@F-I-R-M-A.de

Alice Mustermann
Alice.M@F-I-R-M-A.de

Alice Mustermann
Alice.M@F-I-R-M-A.de

Identitätsmanagement online!

ICH BIN MEHR WERT!

DGB

Aktuell Initiative Aktionen Netzwerke Wir über uns

Initiative für Frauen
Die frauenpolitische Initiative „ICH BIN MEHR WERT!“ ist eine

Suchbegriff


beate uhse
SEX UP YOUR LIFE

HOME SHOPPING ONLINE SEX FILIALEN KALENDER

SUCHE
Shopping
1. Suchbereich wählen
OK

ICH BIN MEHR WERT!


GÄRTNER-BLOG

Edellieschen - Impatiens neuguinea
07. August 2008, 08:40 von Gärtnerin



Willkommen im Garten!
Gartenblog-Startseite
Gartenblog-Autoren
Fragen/Gastbeiträge/Bilder schicken
Werben auf dem Gartenblog
Gästebuch
Kommentare - Hinweise
als Newsletter abonnieren

Web © gaertnerblog.de
Google-Suche

JETZT ONLINE - DIE N
Auffallende Kombinationen
Elfenbein oder junge Mode
Finden Sie jetzt die Trends
inklusive sexy Touch!
Einfache Zahlung auch per
Zum Shop

HARRY S. MORGAN...
ist einer der bekanntesten
deutschen Porno-
produzenten. Harry liebt
Reality. Wenn ein Mädchen
kommt, dann zeigt er das
auch.
mehr >>

ONLINE SEX
Günstige Sex-Partys...

Login: AM.Kiel

AM_BR@mail

Dessous.5.dparty@
spamgourmet.com
& anonyme Zahlung

Login: Gartenfee
alice-garten76@gmx.de

Nichts zu verbergen?



KROLL

Events | Locations | Careers

Home | Background Checks | Drug Testing | Other Services | Legal Library | About

Background Checks

Screening Services

Kroll Advantages

Our Technology

Vendor Screening

Executive-level Screening

Investment Due Diligence

Canadian Searches

Hiring Risks

Hit Ratio Report

BECOME A CLIENT

Pre-Employment Screening Services

Kroll (formerly InfoLink Screening Services) offers a comprehensive list of pre-employment background checks and verification services to help companies screen applicants and Hire With Confidence®. We offer the flexibility of ordering services individually or establishing a standard screening program, which our experienced staff can help you design. As a cornerstone to your search program, Kroll recommends the Five Points Search to protect your business.

Five Points Search

- [Social Security Trace](#)
- [Criminal History Report](#)
- [Criminal Federal Court Search](#)
- [Motor Vehicle History Report](#)
- [National Criminal Database](#)
- [First Alert](#)

Additional Criminal Records

- [Criminal Federal Court Search](#)
- [State Sexual Offender Registry](#)
- [State Repository Search](#)
- [State Incarceration Records](#)
- [OFAC Foreign Nationals Search](#)

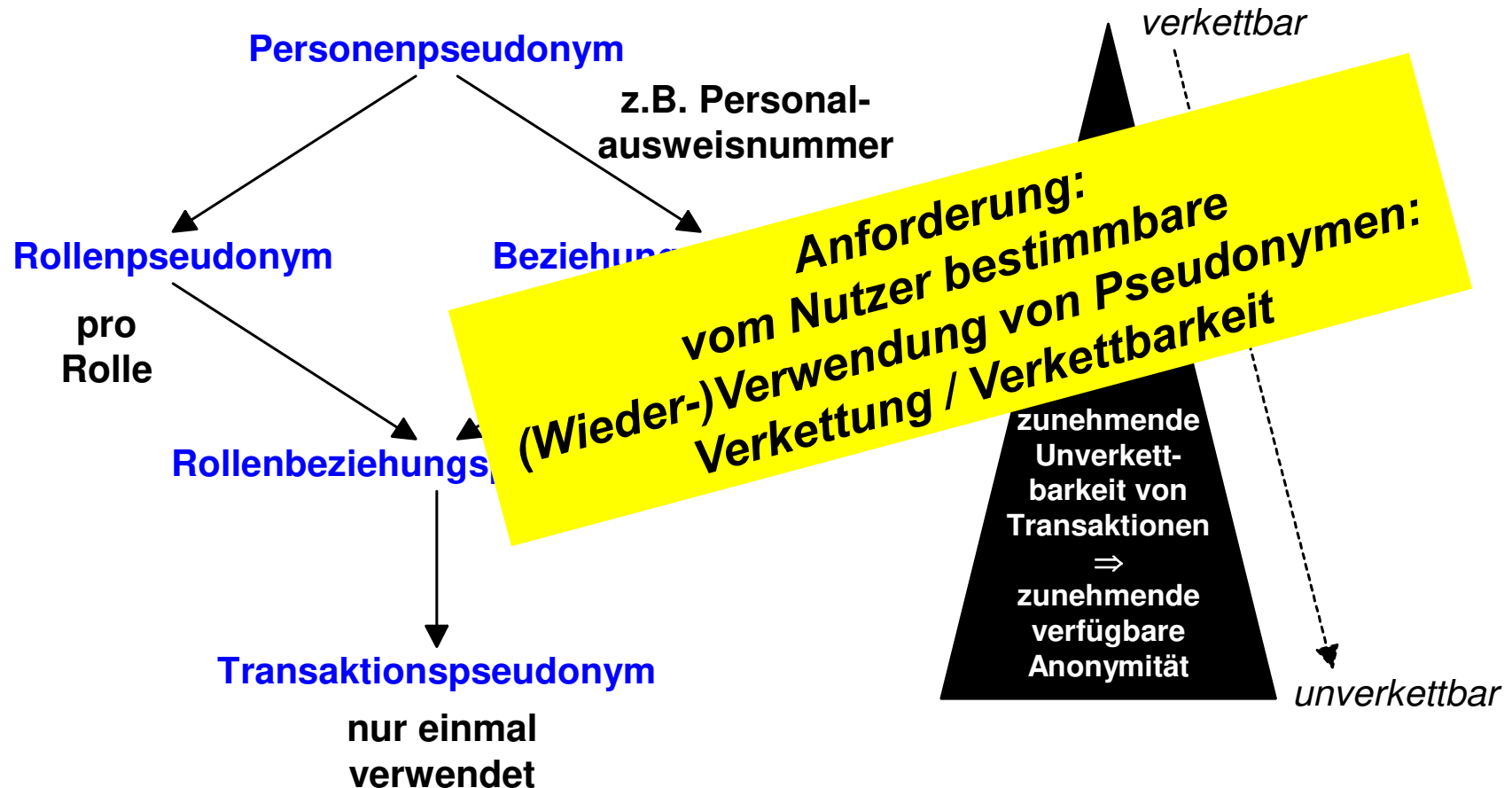
Denkbare Verwendung erstellter Online-Profile:

- Hintergrundinformationen über Stellenbewerber
- Zielgerichtete Werbung
- Bewertung der Kreditwürdigkeit
- ...

Herausforderungen im Netz

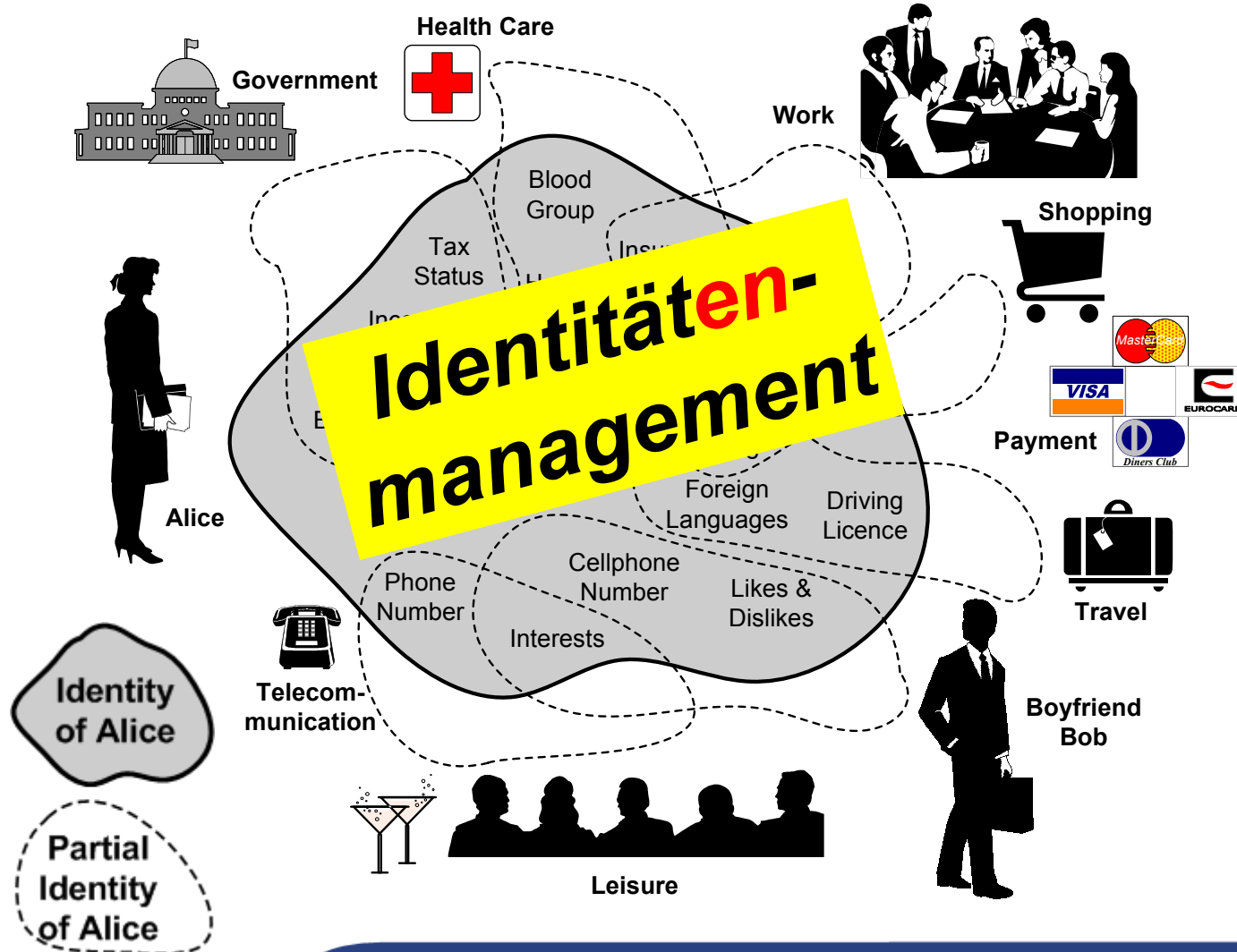
- Intuitives Identitätsmanagement ist nicht übertragbar auf die Online-Welt:
 - Datensammlung bei einzelnen Anbietern (war gestern)
 - Verkettung von digitalen Identitäten, Profilbildung über Anbietergrenzen hinweg
 - Mangelnde wirtschaftliche Anreize für Anbieter, datenschutzfreundliche Technologien einzusetzen
 - Neu DS-GVO: rechtliche Anreize teilweise vorhanden
 - Mangelnde Verfügbarkeit von Tools zum Selbstdatenschutz
 - **Mangelnder breiter Einsatz von vorhandenen Lösungen**

Verkettbarkeit II: Verwendung derselben Pseudonyme



Aus: Pfitzmann/Hansen (Hrsg., 2005); Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management, http://dud.inf.tu-dresden.de/Literatur_V1.smtl

Teilidentitäten von Alice



Überblick behalten?

- Passwortmanager ist Lösungen zum Organisieren und zur sicheren Ablage der Zugangsdaten
 - Verschlüsselte Ablage der Passwörter
 - Offline auf dem lokalen Rechner
 - Idealerweise mit Passwort-Generator
 - Betriebssystemübergreifend nutzbar

Teil 2: Tipps und Tools

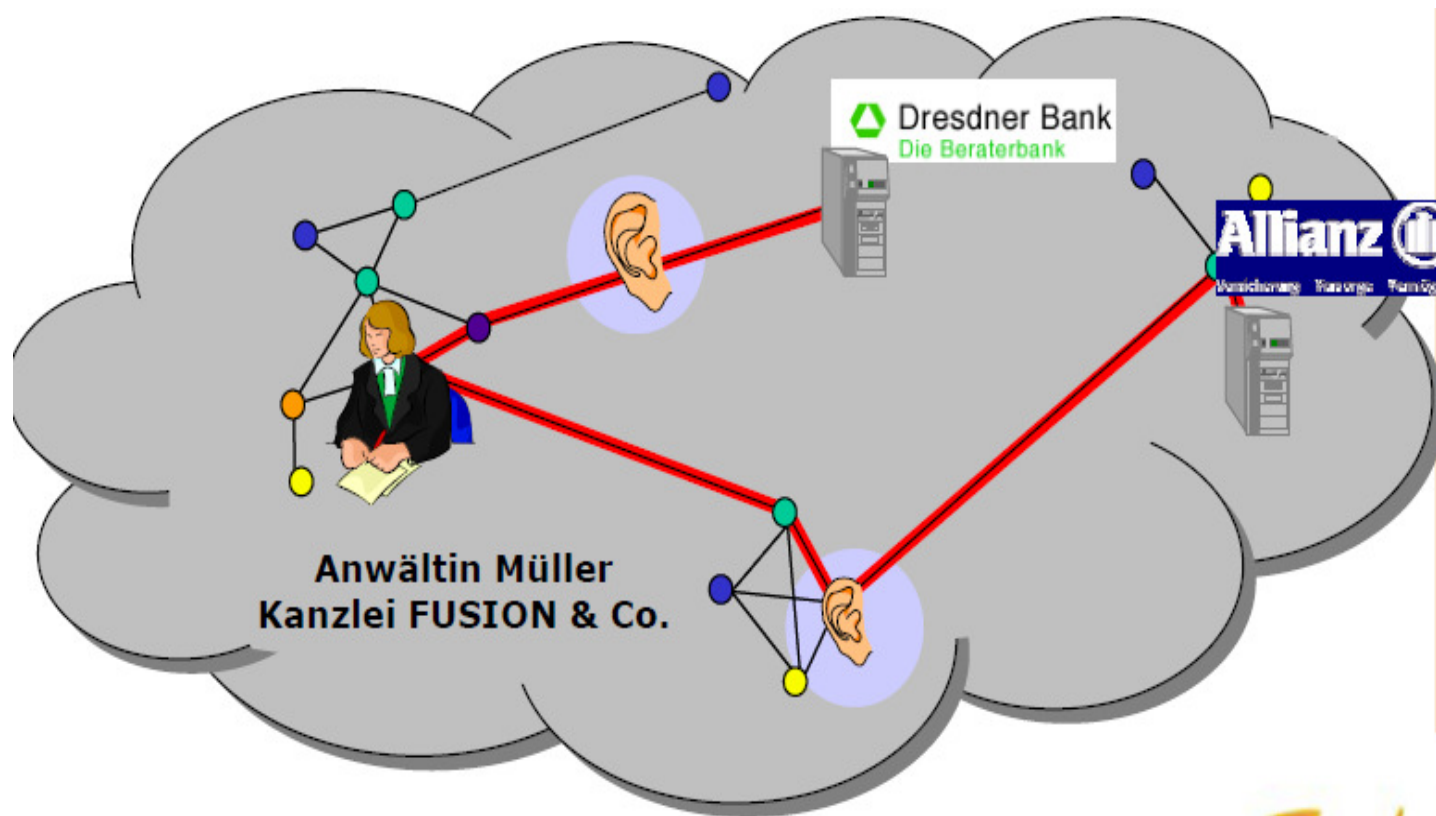


ULD



Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Warum Verschlüsselung nicht genügt



Kommunikationsbeziehungen lassen Rückschlüsse auf die Kommunikationsinhalte zu.

Lösung Proxy?

- Proxies – Der Stein der Weisen?



Vorteil: Dienstanbieter kennt Quelladresse nicht.
Zugangsprovider kennt Zieladresse nicht.

Nachteil: Proxy-Betreiber erfährt komplettes Surfprofil und Dienstleister verkettet über Browserprofile.

Lösung Proxy-Hopping?

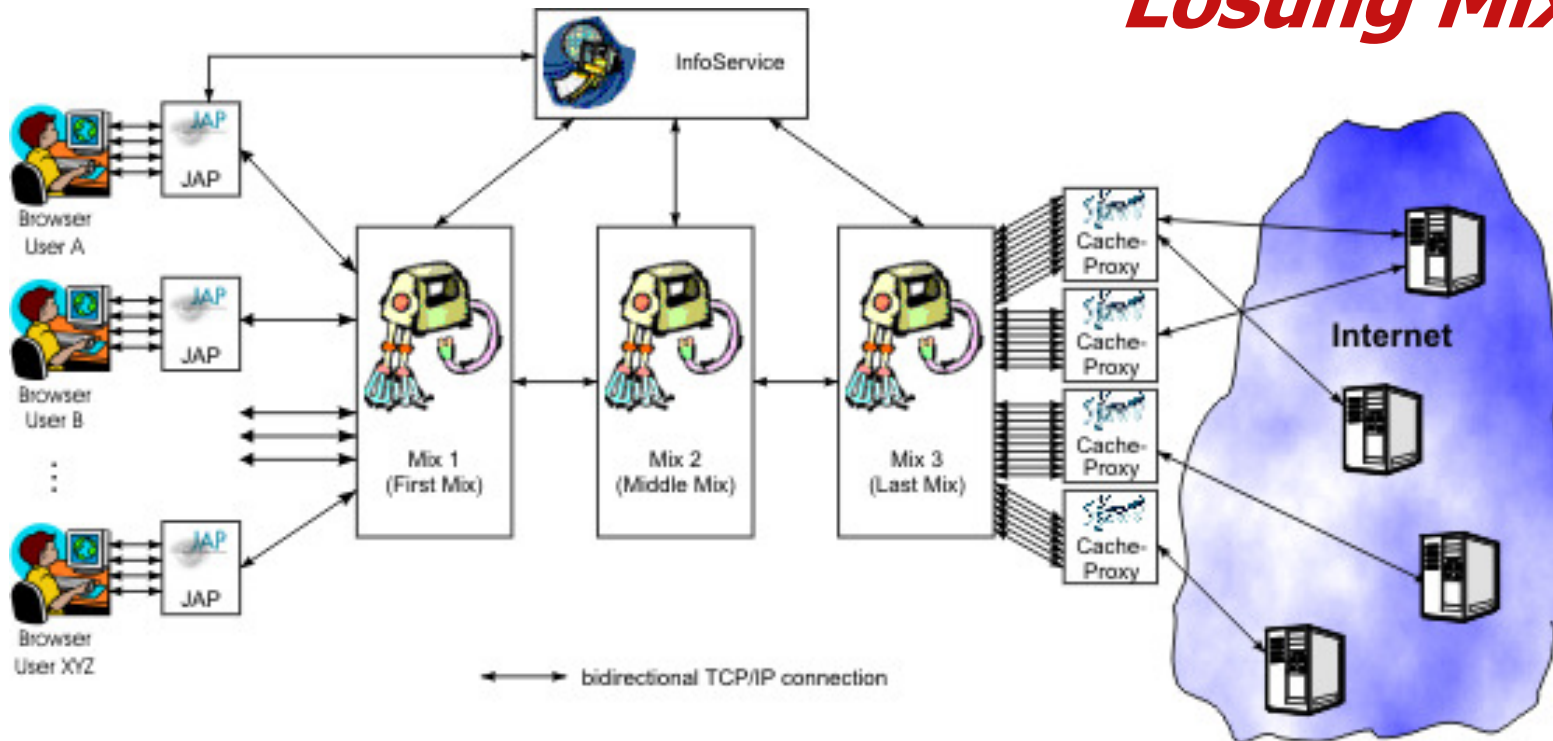
- Viel hilft viel: Das Proxy-Hopping



Vorteil: Webserver erfährt die Absenderadresse nicht.

Nachteil: Viele Proxy-Betreiber haben Zuordnung zwischen Nutzer und Dienstleister. **Dienstleister kann Verkettung über Browser Fingerprinting herstellen.**

Lösung Mixe



Vorteil: Veränderung der Reihenfolge der Anfragen bei jedem Mix, Einheitliche Größe der Datenpakete, Verwerfen von Datenpaketen bei Replay-Angriff.

Verbleibender Angriff: Alle anderen Nutzer des Anonymitätssets kooperieren mit dem Angreifer.

Nachteile: Zu langsam für Mediendateien oder kostenpflichtig.

Datenträgerverschlüsselung

- **Datenträgerverschlüsselung erwägen**

- Gefahr: Verlust von Laptop, Smartphone, USB-Sticks und SD-Karten mit eigenen und fremden(!) Daten (Adressbücher, Bilder, Mails, Briefe, Kalender, ...)
- Pflicht, wenn beruflich genutzt, als Selbstständiger, im Unternehmen, Lehrer, Vereinsvorstand,

⇒ Lösung: Verschlüsseln!

⇒ Festplatten und mobile Datenträger: z.B. mit TrueCrypt (v7.1a), Veracrypt (TrueCrypt-Nachfolger), Bitlocker (enthalten in Windows Ultimate und Enterprise)

⇒ Smartphone: Abhängig von Version des Betriebssystems. Teilweise automatisch aktiviert, teilweise installiert, aber Aktivierung notwendig. Sichere PIN / Passwort wählen!

Auswahl von Diensten

- **Auswahl z.B. für Synchronisation von Kalendern**

- Gefahr: Datenabfluss in Drittstaaten, unsichere Dienste

⇒ Sind Dienste mit zentraler Datenverarbeitung nötig oder werden Daten Dritter verarbeitet: den Dienst gezielt auswählen (Pflicht: für Unternehmen die Daten Dritter verarbeiten: sog. Auftragsdatenverarbeitung). Kriterien:

⇒ Anbieter- und Serverstandorte in der EU?

⇒ Datenschutzerklärung prüfen. Dürfen Daten auch für Zwecke des Anbieters genutzt werden?

⇒ Wie wird der Dienst finanziert? Wenn keine Werbung gewünscht ist, muss man sich darauf einstellen, für gute und faire Leistung zu bezahlen.

Auswahl von Geräten Internet of Things

„Smarte“ Geräte auswählen und Rechte beschränken

- Gefahr: Smarte Geräte kommunizieren unkontrolliert mit dem Hersteller, mit Dritten oder haben offene Konfigurationszugänge, die freien Zugriff gestatten.
- Gefahr: DDoS-Angriffe durch Bot-Netze aus dem IoT
 - ⇒ Auswahl der Geräte (kaum realistisch, teilweise wird Sicherheit aber in Testberichten berücksichtigt)
 - ⇒ Updates regelmäßig und zeitnah verfügbar?
 - ⇒ Herkunftsland des Herstellers?
 - ⇒ Geräte beim Aufstellen datensparsam konfigurieren
 - ⇒ Mit dem Router die Kommunikation ins Netz unterbrechen oder einschränken



Phishing-Schutz

- **Phishing vermeiden**

- Gefahr: Kontrollverlust über eigene und fremde Accounts, ungewollte Preisgabe von Daten
- ⇒ Links in E-Mail kontrollieren. Funktion „Mouse-over“ zeigt den tatsächlichen Link. Nicht direkt anklicken, ggf. kopieren und im Browser einfügen.
- ⇒ Bekannte Seiten selbst eingeben oder direkt eingeben
- ⇒ Seite für Onlinebanking immer selbst eingeben
- ⇒ Ggf. Plug-in nutzen, das den Link (lokal!) analysiert und die relevanten Teile hervorhebt
(in Testphase derzeit z.B.: „TORPEDO Phishing Detection“ für Thunderbird)

Datenverlust verhindern

- **Backups machen**

- Gefahr von Datenverlust (Risiko: alles von lästig bis existenzbedrohend für einen selbst und Dritte)
- Weitere Gefahr: Verschlüsselungstrojaner
- Pflicht: u.a. aus Steuergesetzen, Handelsrecht, vertraglichen Obliegenheiten, Eigeninteresse

⇒ Sicherung auf externen Datenträgern an sicherem Ort (idealerweise verschlüsselt!)

⇒ Papierkopie in Akten der wichtigsten Unterlagen

Surfprofile vermeiden 1

- **Umfassende zentrale Surfprofile vermeiden**

- Gefahr: Dienste erstellen seiten- und geräteübergreifend Surf- und Interessenprofile. Risiko u.a. Erpressung
- Gefahr: Dienste tracken Nutzer, auch wenn diese nicht angemeldet sind – Buttons eingebunden als iframe
- ⇒ Mehrere Geräte und Browser benutzen mit klarer Zwecktrennung + ggf. eigenen getrennten Identitäten
- ⇒ Social Media gar nicht oder nur mit einem designierten Browser nutzen
- ⇒ Seiten mit aktiven Social-Media-Plugins meiden
- ⇒ Werbe-Blocker helfen u.a. gegen aktive Buttons
- ⇒ Nur selektiv freischalten

Surfprofile vermeiden 2

- **Umfassende zentrale Surfprofile vermeiden**
 - Gefahr: Dienste mit zentraler Plattform
 - Aktuell: NDR-Reportage Dienst Web of Trust (WOT)
 - ⇒ Dienste mit serverseitiger Datenverarbeitung meiden oder diese nur ganz gezielt einsetzen (Online-Virens Scanner, Werbewarnungen, Social Media, Kinderschutzfilter, Übersetzungsdienste, ...)
 - ⇒ Lösungen mit lokaler Datenverarbeitung bevorzugen (Antivirus installieren, Kinderfilter im eigenen Internetrouter, Zeitkontingent im Fernseher, ...)
 - ⇒ Anbieter und Serverstandorte in der EU, Lesen der Datenschutzerklärung.
 - ⇒ Tracking- und Ad-Blocker verwenden (z.B. uBlock mit EasyPrivacy-Liste)

Surfprofile vermeiden 3: eigene Daten im Netz

- **Eigene Daten im Netz veröffentlichen**

- Gefahr: Verkettung ermöglicht Persönlichkeitsprofil, Diskriminierung, ...
- Beispiele: Personalverantwortliche suchen im Netz
- ⇒ Privates unter Pseudonym(en) und getrennt nach Zwecken und Seiten (Identitätsmanagement) veröffentl.
- ⇒ Datenschutzeinstellungen der Seiten restriktiv einstellen
- ⇒ Mehrere E-Mail-Konten / Aliasadressen nutzen
- ⇒ Niemals Daten Dritter ohne Einwilligung online stellen
- ⇒ Einwilligungen prüfen (Schule, Kita, Arbeitgeber, ...)
- ⇒ Ggf. eigenes seriöses Profil für professionelle Kontakte erstellen

Surfprofile vermeiden 4 weitere Hinweise

- **Surfprofile verhindern**

- ⇒ Browser aktuell halten und zwischen mehreren Instanzen bzw. Browsern wechseln
- ⇒ Cookies gezielt verwalten und regelmäßig löschen lassen
- ⇒ Browser-Add-ons kontrollieren
- ⇒ Datensparsame Suchmaschinen verwenden (und nur dann auf große Anbieter wechseln, wenn die Ergebnisse unzureichend sind)
- ⇒ Sich selbst über große aktuelle Risiken mit dringendem Handlungsbedarf informiert halten, z.B. auf
 - ⇒ Datenschutz.de
 - ⇒ bsi-fuer-buerger.de
 - ⇒ Heise.de

Weitere Quellen: Forum Privatheit

- Selbstdatenschutz ist interdisziplinärer Forschungsgegenstand
- Befassung aus der Sicht diverser Disziplinen erfolgte im Forum Privatheit

Quelle:

<https://www.forum-privatheit.de/forum-privatheit-de/texte/veroeffentlichungen-des-forums.php>



Förderhinweis



AN.ON-Next – Anonymität Online der nächsten Generation



Forum Privatheit und selbstbestimmtes Leben in der Digitalen Welt (Privacy-Forum)

sämtliche Projekte gefördert vom Bundesministerium für Bildung und Forschung:



Vertrauenswürdige
Verteilung von
Verschlüsselungsschlüsseln

VVV – Vertrauenswürdige Verteilung von Verschlüsselungsschlüsseln



AppPETs – Datenschutzfreundliche Smartphone-Anwendungen ohne Kompromisse

GEFÖRDERT VOM



Bundesministerium
für Bildung
und Forschung

Links: <https://www.datenschutzzentrum.de/projekte/>

Zeit für Fragen und Diskussion



Kontakt:

Harald Zwingelberg

uld6@datenschutzzentrum.de

www.datenschutzzentrum.de

0431/988-1222

ULD



Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein