Verteilte soziale Netzwerke

Technik, Chancen, Risiken

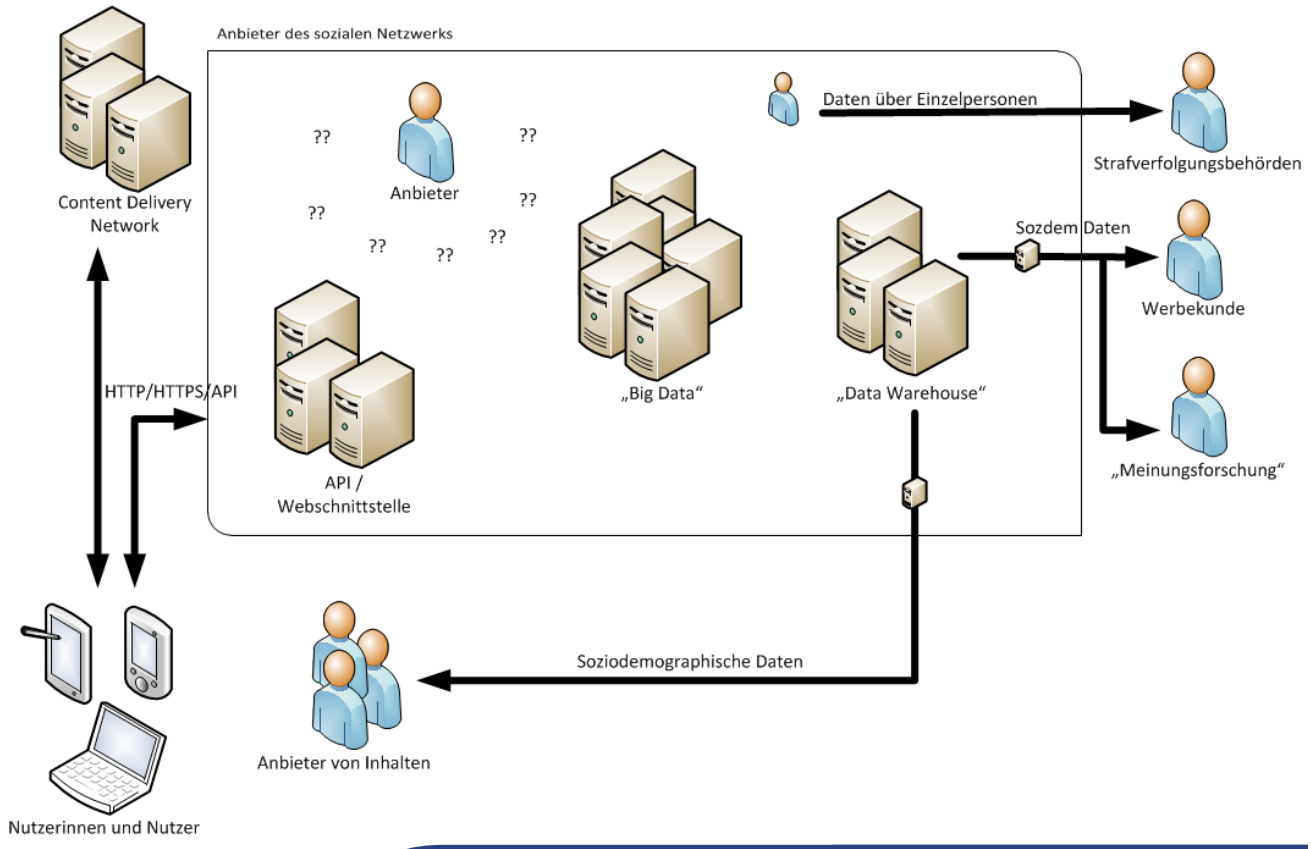
Sven Thomsen

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Agenda

- Risikosituation: zentralisierte sozialen Netzwerken
- Risikosituation: dezentral, „server-basiert“
- Risikosituation: dezentral, „peer-to-peer“
- Fazit

zentral


Anbieter des sozialen Netzwerks
Content Delivery Network
Anbieter
??
??
??
??
??
??
??
Daten über Einzelpersonen
Strafverfolgungsbehörden
Sozdem Daten
Werbekunde
„Big Data“
„Data Warehouse“
„Meinungsforschung“
HTTP/HTTPS/API
API / Webschnittstelle
Soziodemographische Daten
Anbieter von Inhalten
Nutzerinnen und Nutzer

Risiken zentraler Netzwerke

- Klassische Risikoszenarien, bekannte Risiken
  - User-User-Angriffe:
    - Crawler, fehlerhafte Berechtigungsvergabe
    - Modelle und zumindest besteht Kontrollfiktion
  - Technische Fehler:
    - Systemfehler, fehlerhafte Verschlüsselung,...
    - Sicherheitsmanagement, „ordentlicher“ Betrieb
- Dominierendes Szenario: Anbieter als „Angreifer“

Anbieter als Angreifer

- Aktuelle Situation
  - Keine Auskunft über interne Verarbeitung der Daten
  - Kein Nachweis oder nur Hinweis auf aktives Datenschutzmanagement:
    - Anlassbezogene Kontrollen
    - Regelmäßige Kontrollen
    - Integration von Datenschutz in Produktdesign
    - Verhalten bei Datenschutzvorfällen
  - Hinweise auf Unterauftragnehmer
    - Softwareentwicklung (Einsatz von Fremd-Anwendungen)
    - Betrieb (z.B. Content-Delivery-Networks)

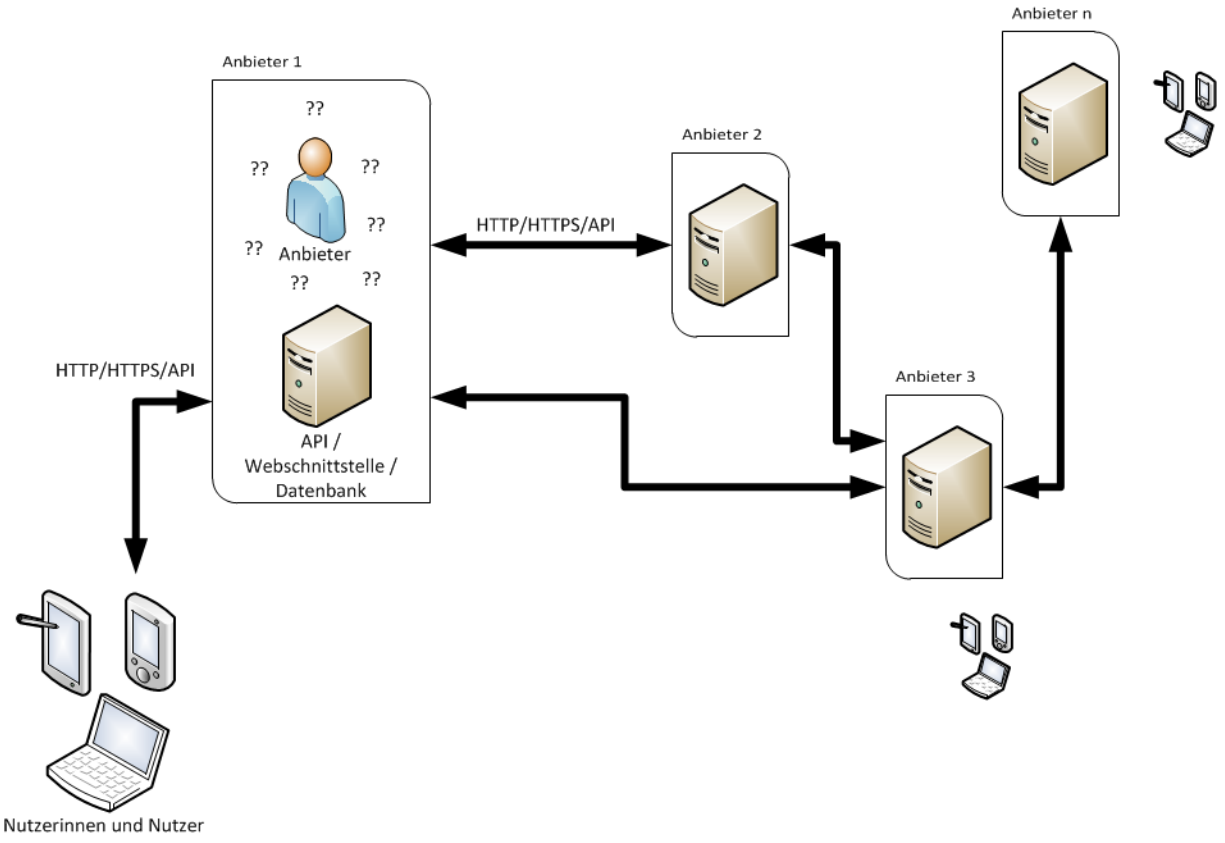
Anbieter als Angreifer

- Keine Nachweise -> „Schlüsselloch-Datenschutz“
  - Analyse und Durchsicht von Veröffentlichungen
  - Analogie-Bildung aus vergleichbaren Setups
- Werkzeuge zentraler Netzwerke teilweise bekannt

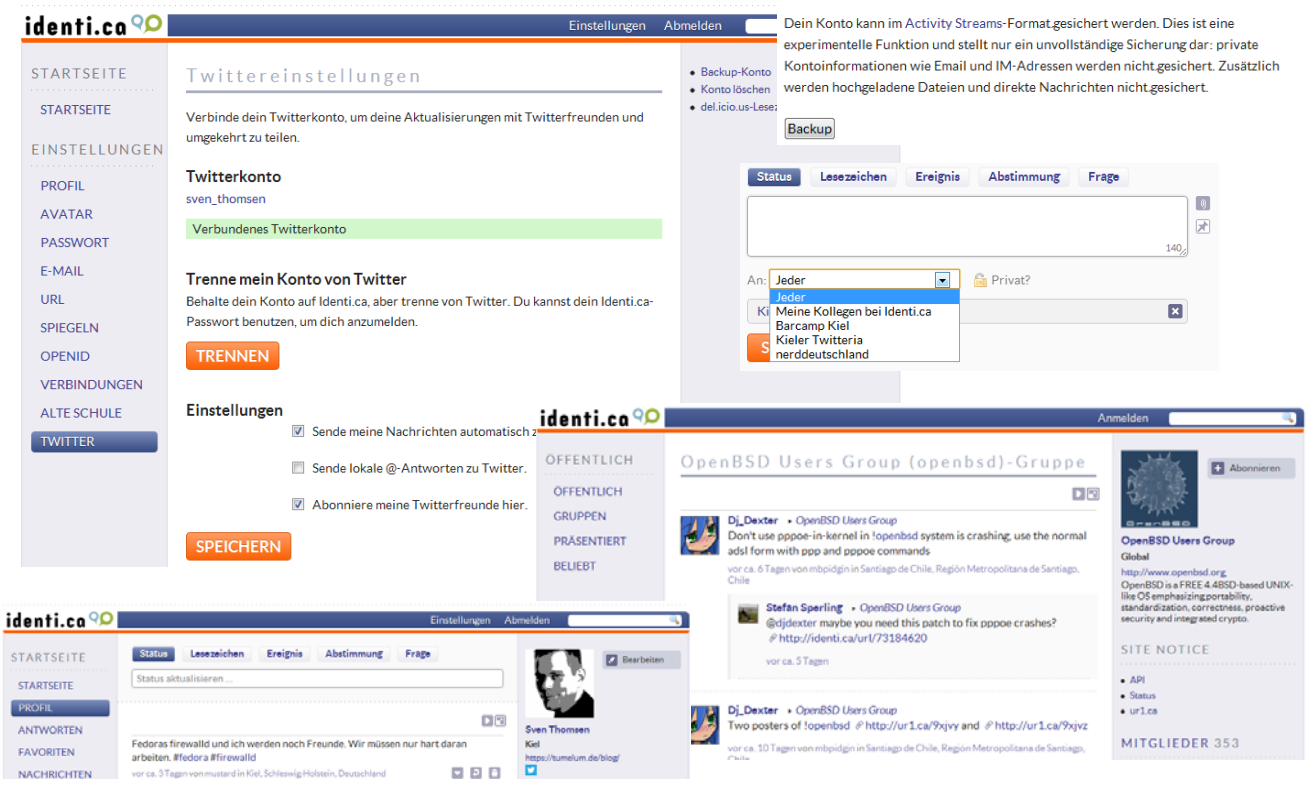
Anbieter als Angreifer

- Risikofaktoren teilweise bekannt
  - „Big-Data“-Umgebungen mit mangelhaften Mechanismen zur Zugriffssteuerung und -protokollierung
  - „Data-Warehouse“-Problematiken
- Probleme sind lösbar
  - Segmentierung von Datenpools, Kontrolle der Verkettung, Lenkung von Zugriffen,....
  - Standard-Auswertungen und ad-hoc-Analyse unter Beteiligung des internen Datenschutzmanagements
- Datenschutz-Maßnahmen gegen bekannte Risiken werden nicht nachgewiesen.
- Datenschutzmanagement in „BigData-Umgebungen“

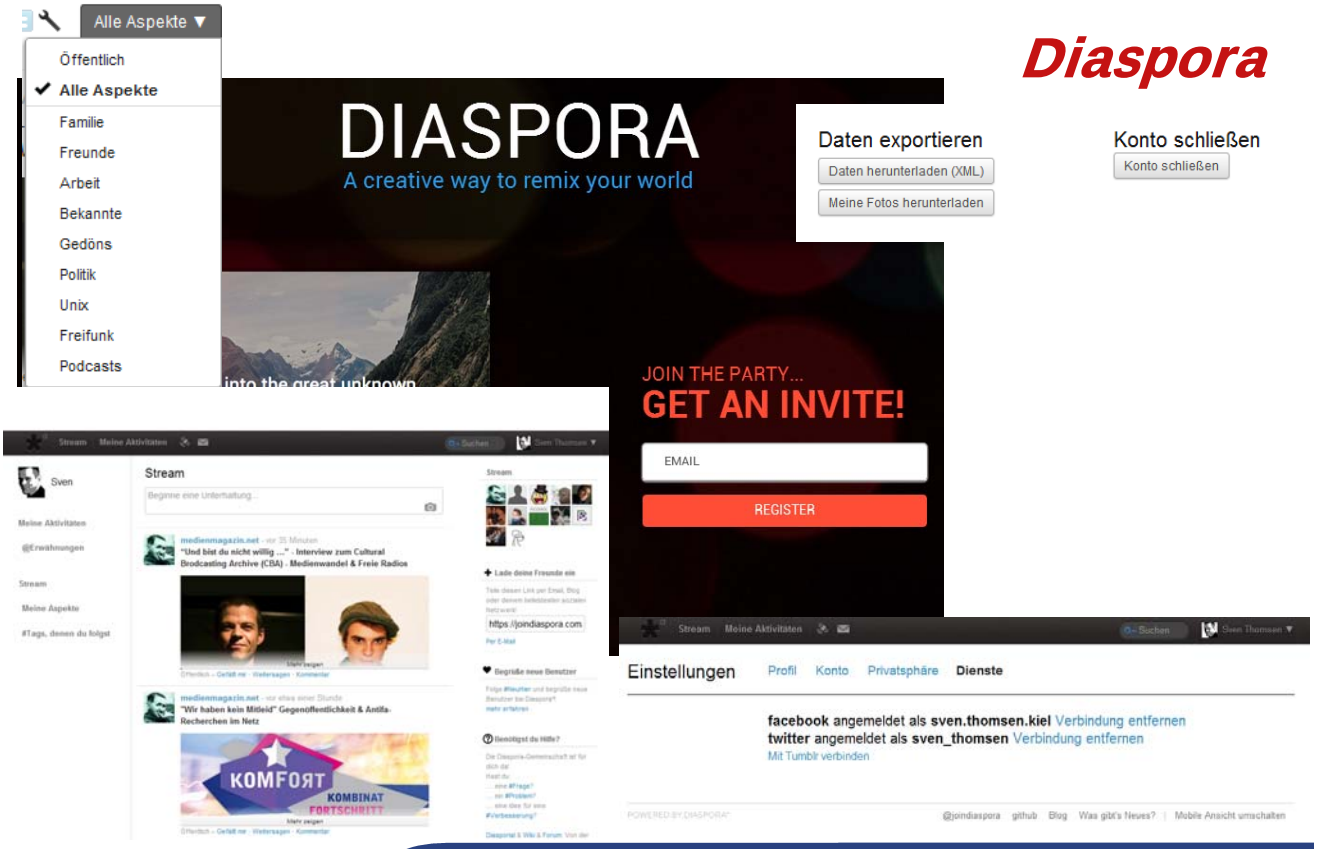
dezentral, „server-basiert“



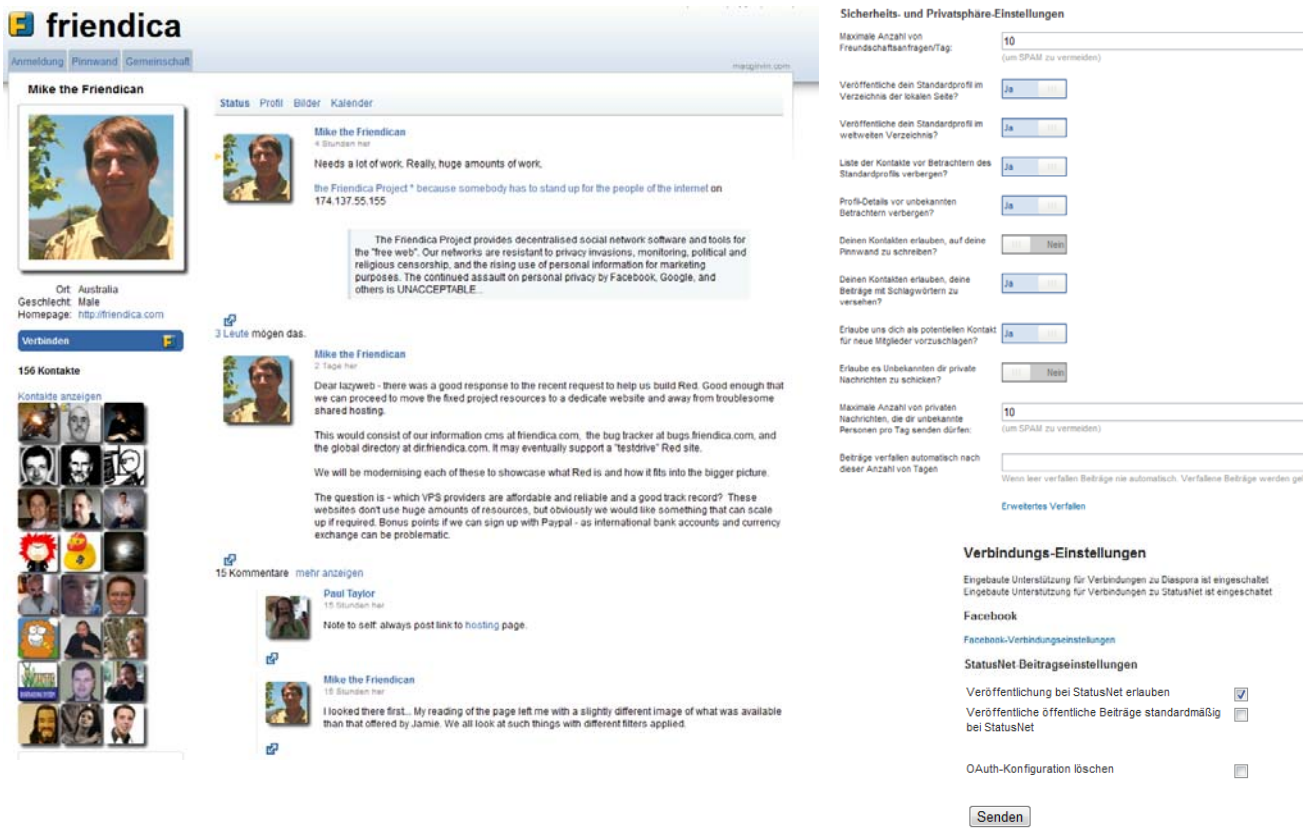
Identi.ca



Diaspora



Friendica



Protokolle und Datenformate

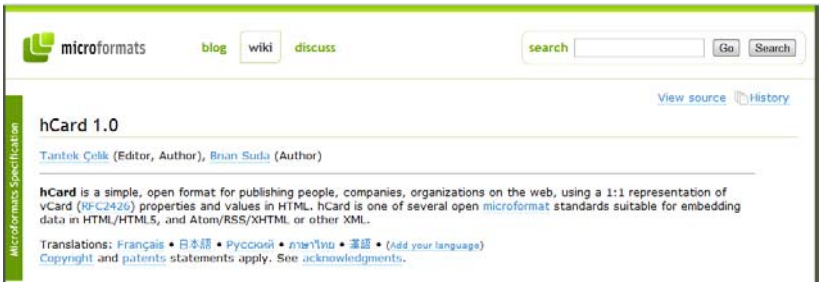
- WebFinger
  - HTTP/HTTPS um Informationen über Nutzerkonten in verteilten Netzwerken zu erhalten

https://friendica.tumelum.de/.well-known/host-meta

```
▼<XRD xmlns="http://docs.oasis-open.org/ns/xri/xrd-1.0" xmlns:hm="http://host-meta.net/xrd/1.0">
  <hm:Host>friendica.tumelum.de</hm:Host>
  <Link rel="lrdd" template="https://friendica.tumelum.de/xrd/?uri={uri}"/>
  <Link rel="acct-mgmt" href="https://friendica.tumelum.de/amcd"/>
  <Link rel="http://services.mozilla.com/amcd/0.1" href="https://friendica.tumelum.de/amcd"/>
  <Link rel="http://oexchange.org/spec/0.8/rel/resident-target" type="application/xrd+xml" href="https://friendica.tumelum.de/oexchange/xrd"/>
  <Link rel="http://purl.org/zot/1.0/post" href="https://friendica.tumelum.de/post"/>
  <Property xmlns:zot="http://purl.og/zot/1.0" type="http://purl.org/zot/1.0/version" zot:version="1"/>
  <Property xmlns:zot="http://purl.og/zot/1.0" type="http://purl.org/zot/1.0/accept" zot:accept="application/atom+xml"/>
 ▼<Property xmlns:mk="http://salmon-protocol.org/ns/magic-key" type="http://salmon-protocol.org/ns/magic-key" mk:key_id="1">
    RSA.AKSHF-4LHNGSRK1OhH6G4XnI4sKKqPCdj-KKJyfLeVtF0yF-chDsVokW0b9nir_Gw5eBgzuA8qDgTLoAMftttw5TEBgZ6Z7hgbHcJbjJf3OUlkGc3Zhw7SF8t8v5OjoByScUXQs
    5aMZTUOohvAvZ1MhLOa3CSkGSviPEb4fmGEjFsG9alVORkJs2qdiWfCNxnMPbdZalohkALwTyr82v5n23mb1AIxMJRSxPgLJx-a9OK-9DniY4nrU_H3pbaMqM7mxIg-
    a0Xuh386LlcLMkZTRG0ZSdy3_uwRaPvJuV3NnlGhAzrU_8VtWB1pbgxtj6PGwWc60CFOtTTIdfIOyy0ls9z7Mv4IKNhtONxrCdvkJLxVzI1vo_WE_2Alvo28xd1ysrBVqWuSXi9kOis
    9mPbx3aC-21s_bKan9W6Irx65TUC4o5g6s3np_9_Vrks13f1iuInEVfwFC0mNNrBc2FaVBq75HrvXXm_VYLYz-EWIJ9NktbZ16Umcr5.AQAB
  </Property>
</XRD>
```

Protokolle und Datenformate

- hCard
  - Analog zu vCard, Kontaktinformationen



Protokolle und Datenformate

- ActivityStreams
  - Standardisiertes Format, um Aktivitäten zu beschreiben
  - JSON, ATOM und XML-Schema
  - Breite Unterstützung: Microsoft, IBM,...

Snell

Verb Definitions

For example:

```
{
  "actor": "person",
  "object": "note",
  "target": "*",
  "targetRequired": true,
  "templates": {
    "*": "{actor} sent {object} to {target}",
    "de-*": "{actor} geschickt {target} das {object}",
  }
}
```

```
{
  "objectType": "comment",
  "content": "<p>This is a comment</p>",
  "inReplyTo": [
    {
      "objectType": "note",
      "id": "http://example.org/objects/123",
      "displayName": "A simple note"
    }
  ]
}
```

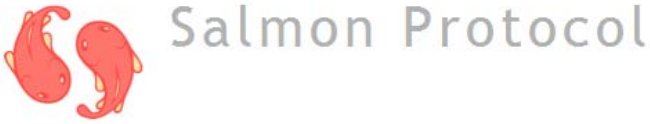
Verbs

The following verbs are currently registered:

Name	Identifier
Post	post
add	add
cancel	cancel
checkin	checkin
delete	delete
favorite	favorite
follow	follow
give	give
ignore	ignore
invite	invite

Protokolle und Datenformate

- Protokoll
  - zur Adressierung von Inhalten
  - Anbringen von Kommentaren
  - Verifizieren von Kommentaren
- Transport: HTTP / HTTPS
- Verifikation: GPG bzw. andere Public-Key-Verfahren



Risikobetrachtung

- Verändert sich das dominierende Risiko „Anbieter als Angreifer“?
  - (+) verteilte Server, weniger „User pro Server“
  - (-) unabhängige, teilweise unbekannte Betreiber
  - (+) offene Protokolle, Wahlmöglichkeiten
  - (-) teilweise unverschlüsselte Kommunikation

⇒ Serveranbieter bleibt weiterhin größtes Risiko

⇒ Segmentierung und Eigenbetrieb verringert Risiko

Risikobetrachtung

- Grundsatz:
  Private Kommunikation nur durch Ende-zu-Ende-Sicherheit
- Herausforderung: Geschlossene Kommunikation
  - Kommunikation innerhalb einer Gruppe über mehrere Instanzen verteilt
  - Paradoxon:
    „Vertraulichkeitskontrolle in lose gekoppelten System“
  - Strikte Kontrolle und Durchsetzung kann effektiv nur vom Initiator und im Einzelfall erfolgen

  ⇒Latenzprobleme, hohe Anzahl an Anfragen
- Geschlossene Kommunikation ist in dezentralen Netzwerken mit unmittelbarer Kontrolle und Lenkung der genutzten Serverinstanzen verbunden

Risikobetrachtung

- Ungelöst (Unlösbar?):
  Sicheres Löschen in lose gekoppelten Systemen.

- Problem: Zusätzlicher Kontext durch persönliche Nähe zum Betreiber des Servers
  - Beispiel: „Freiwillige Feuerwehr Dunkeldorf“
  - Beispiel: „Ich nutze den Server meines Bekannten mit“

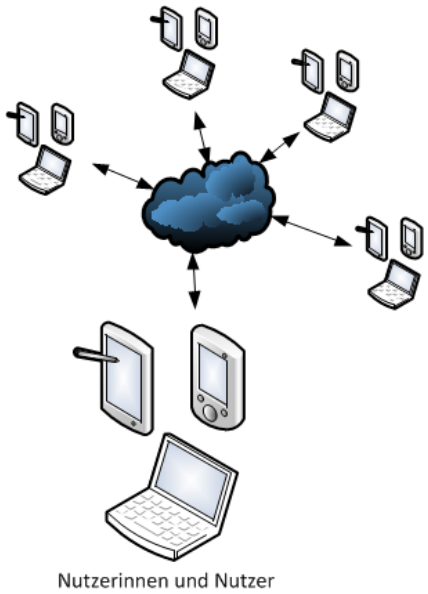
- Diskussion
  - Tauschen wir „einzelnen Missbrauch von Massendaten gegen „massenhaften Missbrauch von Einzeldaten“?

Empfehlungen

- Empfehlung des ULD zu dezentralen, servergestützten Netzwerken:
  - Eigenbetrieb oder Betrieb durch kontrollierte und gelenkte Stelle
  - Service- und Dienst-Härtung durchführen
  - HTTPS-Verschlüsselung und –Authentifizierung erzwingen

- Grundsätzlich:
  - Geschlossene Kommunikation und nachträgliches Löschen aktuell nur in geschlossenen sozialen Netzwerken sicher möglich

dezentral, „peer-to-peer“



Risikobetrachtung

- „Pervertierung“ des dezentralen, servergestützten Modells:
  - Jeder betreibt eigenen Hub/Pod/Server
  - Skalierung voll vermaschter sozialer Netzwerke?
  - Wahrscheinlich: Angepasste Software notwendig
- Chance: Direkte Adressierbarkeit von Endgeräten durch IPv6 (vgl. Entschließung der 82. DSK, Förderung von Privacy durch P2P-Lösungen statt zentraler Serverdienste)
- Prototypen seit längerer Zeit vorhanden

Dezentral, P2P

PROJECT DANUBE
IDENTITY AND COMMUNICATION FOR POLITICAL AND SOCIAL INNOVATION

SECURE SHARE

Social Swarm

FREEDOMBOX

Fazit

Fazit

- Risikosituation in sozialen Netzwerken wird wesentlich durch Betreibermodell beeinflusst
- Dezentrale, servergestützte Modelle sind Fortschritt, aber keine Lösung für „Anbieter als Angreifer“
- Dezentrale, servergestützte Modelle im Eigenbetrieb bilden eine gute Alternative zu großen Anbietern sozialer Netzwerke
- P2P-basierte Ansätze mit Ende-zu-Ende-Sicherheit sind aus Datenschutzsicht anzustreben und zu unterstützen

Diskussion

Vielen Dank!

Sven Thomsen
Unabhängiges Landeszentrum für Datenschutz
Holstenstraße 98
24103 Kiel

Tel: 0431 – 988 1211
Mail: ULD3@datenschutzzentrum.de