

# Verteilte soziale Netzwerke

Technik, Chancen, Risiken

Sven Thomsen

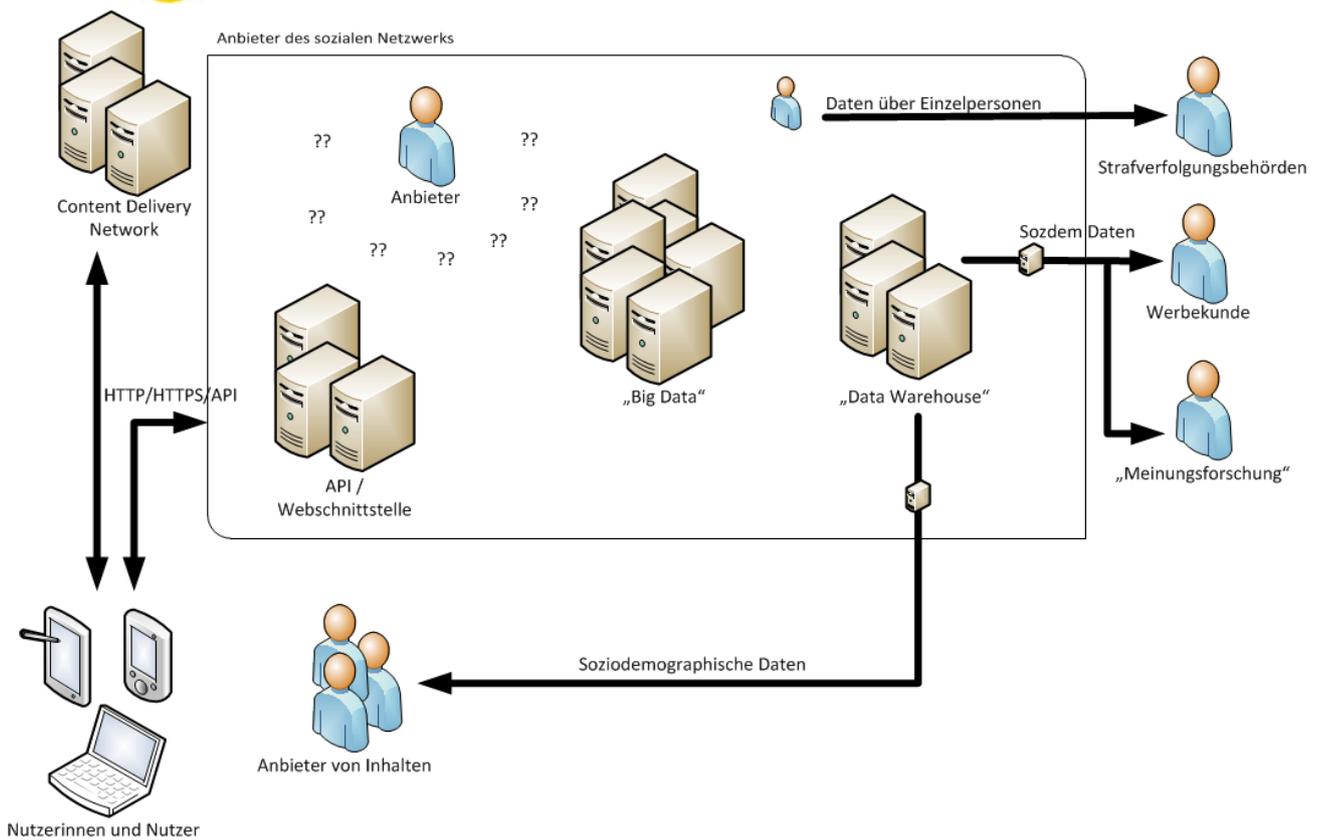


[www.datenschutzzentrum.de](http://www.datenschutzzentrum.de)

## *Agenda*

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

# zentral



## *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

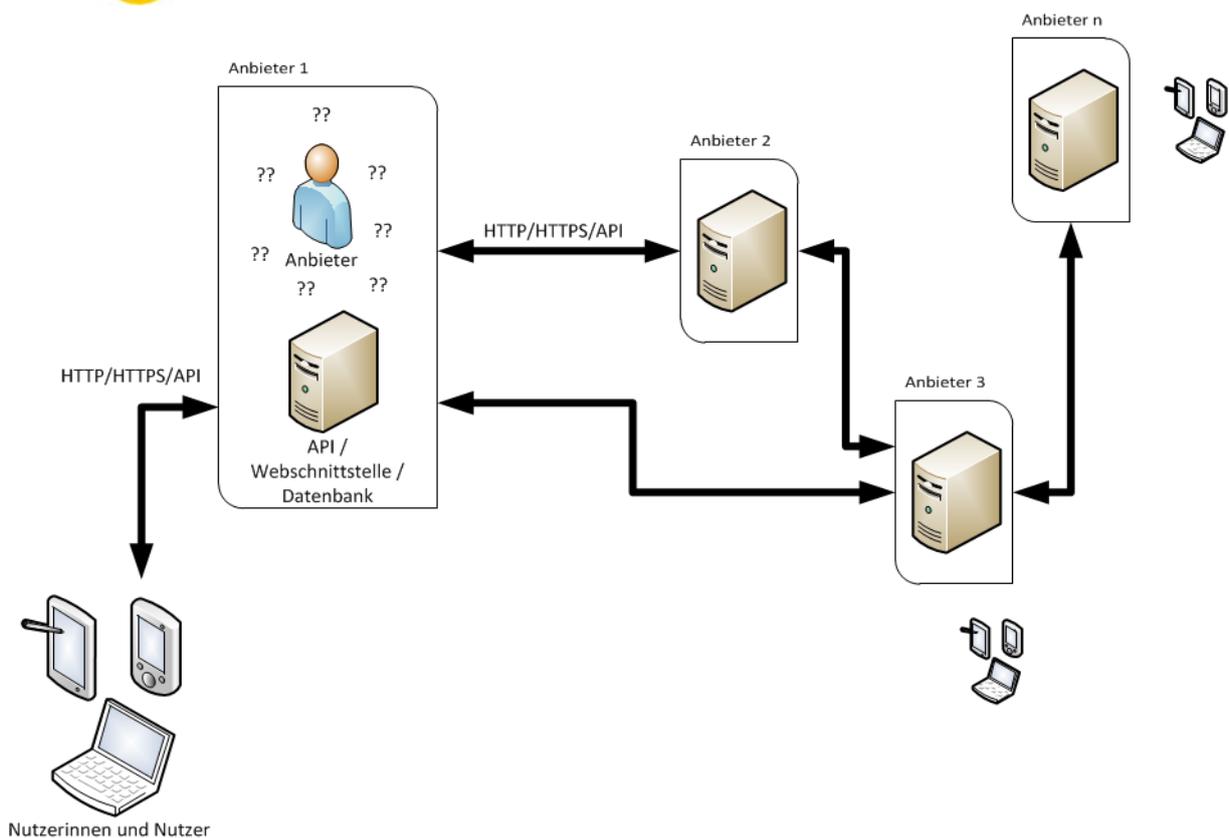
- Keine Nachweise -> „**Schlüsseloch-Datenschutz**“
  - Analyse und Durchsicht von Veröffentlichungen
  - Analogie-Bildung aus vergleichbaren Setups
- Werkzeuge zentraler Netzwerke teilweise bekannt



## 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“



Backup-Konto

**identi.ca** Einstellungen Abmelden

**STARTSEITE**

**EINSTELLUNGEN**

PROFIL  
AVATAR  
PASSWORT  
E-MAIL  
URL  
SPIEGELN  
OPENID  
VERBINDUNGEN  
ALTE SCHULE  
TWITTER

**Twitterereinstellungen**

Verbinde dein Twitterkonto, um deine Aktualisierungen mit Twitterfreunden und umgekehrt zu teilen.

**Twitterkonto**  
sven\_thomsen  
Verbundenes Twitterkonto

**Trenne mein Konto von Twitter**  
Behalte dein Konto auf Identi.ca, aber trenne von Twitter. Du kannst dein Identi.ca-Passwort benutzen, um dich anzumelden.

**TRENNEN**

**Einstellungen**

- Sende meine Nachrichten automatisch
- Sende lokale @-Antworten zu Twitter.
- Abonniere meine Twitterfreunde hier.

**SPEICHERN**

Dein Konto kann im Activity Streams-Format gesichert werden. Dies ist eine experimentelle Funktion und stellt nur ein unvollständige Sicherung dar: private Kontoinformationen wie Email und IM-Adressen werden nicht gesichert. Zusätzlich werden hochgeladene Dateien und direkte Nachrichten nicht gesichert.

**Backup**

Status Lesezeichen Ereignis Abstimmung Frage

An: Jeder

Ki Meine Kollegen bei Identi.ca

S Barcamp Kiel

Ki Kieler Twitteria

S nerdeutschland

**identi.ca** Einstellungen Abmelden

**STARTSEITE**

STATUS Lesezeichen Ereignis Abstimmung Frage

Status aktualisieren ...

**PROFIL**

ANTWORTEN  
FAVORITEN  
NACHRICHTEN

**Sven Thomsen**  
Kiel  
https://tumelum.de/blog/

Fedoras firewall und ich werden noch Freunde. Wir müssen nur hart daran arbeiten. #fedora #firewall

vor ca. 3 Tagen von mussard in Kiel, Schleswig-Holstein, Deutschland

**identi.ca** Anmelden

**OpenBSD Users Group (openbsd)-Gruppe**

**Dj\_Dexter** • OpenBSD Users Group  
Don't use ppooe-in-kernel in 1openbsd system is crashing, use the normal adsl form with pop and ppooe commands

vor ca. 6 Tagen von mbpdiqn in Santiago de Chile, Región Metropolitana de Santiago, Chile

**Stefan Sperling** • OpenBSD Users Group  
@djdexter maybe you need this patch to fix ppooe crashes?  
# http://identi.ca/url/73184620

vor ca. 5 Tagen

**Dj\_Dexter** • OpenBSD Users Group  
Two posters of 1openbsd # http://ur.1ca/9xyjv and # http://ur.1ca/9xyjv

vor ca. 10 Tagen von mbpdiqn in Santiago de Chile, Región Metropolitana de Santiago, Chile

**OpenBSD Users Group**  
Global  
http://www.openbsd.org  
OpenBSD is a FREE 4.4BSD-based UNIX-like OS emphasizing portability, standardization, correctness, proactive security and integrated crypto.

**SITE NOTICE**

- API
- Status
- ur1.ca

**MITGLIEDER 353**

**Alle Aspekte**

- Öffentlich
- Alle Aspekte**
- Familie
- Freunde
- Arbeit
- Bekannte
- Gedöns
- Politik
- Unix
- Freifunk
- Podcasts

**DIASPORA**  
A creative way to remix your world

into the great unknown

**Stream**

Beginne eine Unterhaltung...

medienmagazin.net vor 32 Minuten  
"Und bist du nicht willig..." Interview zum Cultural Broadcasting Archive (CBA) | Medienwandel & Freie Radios

medienmagazin.net vor etwa einer Stunde  
"Wir haben kein Mittel!" Gegenöffentlichkeit & Antifa. Recherchen im Netz

**KOMFORT KOMBINAT FORTSCHRITT**

**Daten exportieren**

Daten herunterladen (XML)

Meine Fotos herunterladen

**Konto schließen**

Konto schließen

**JOIN THE PARTY... GET AN INVITE!**

EMAIL

**REGISTER**

**Einstellungen** Profil Konto Privatsphäre Dienste

facebook angemeldet als sven.thomsen.kiel Verbindung entfernen  
twitter angemeldet als sven\_thomsen Verbindung entfernen  
Mit Tumblr verbinden

POWERED BY DIASPORA

@jondiaspora github Blog Was gibt's Neues? | Mobile Ansicht umschalten

**friendica**

Anmeldung Pinnwand Gemeinschaft

Mike the Friendican



Ort: Australien  
Geschlecht: Male  
Homepage: http://friendica.com

Verbunden

156 Kontakte



Status Profil Bilder Kalender

Mike the Friendican  
4 Stunden her

Needs a lot of work. Really, huge amounts of work.

the Friendica Project \* because somebody has to stand up for the people of the internet on 174.137.55.155

The Friendica Project provides decentralised social network: software and tools for the "free web". Our networks are resistant to privacy invasions, monitoring, political and religious censorship, and the rising use of personal information for marketing purposes. The continued assault on personal privacy by Facebook, Google, and others is UNACCEPTABLE.

3 Leute mögen das.

Mike the Friendican  
2 Tage her

Dear lazweb - there was a good response to the recent request to help us build Red. Good enough that we can proceed to move the fixed project resources to a dedicate website and away from troublesome shared hosting.

This would consist of our information cms at friendica.com, the bug tracker at bugs.friendica.com, and the global directory at dir.friendica.com. It may eventually support a "testdrive" Red site.

We will be modernising each of these to showcase what Red is and how it fits into the bigger picture.

The question is - which VPS providers are affordable and reliable and a good track record? These websites don't use huge amounts of resources, but obviously we would like something that can scale up if required. Bonus points if we can sign up with Paypal - as international bank accounts and currency exchange can be problematic.

15 Kommentare mehr anzeigen

Paul Taylor  
15 Stunden her

Note to self: always post link to hosting page.

Mike the Friendican  
18 Stunden her

I looked there first... My reading of the page left me with a slightly different image of what was available than that offered by Jamie. We all look at such things with different filters applied.

Sicherheits- und Privatsphäre-Einstellungen

Maximale Anzahl von Freundschaftsanfragen/Tag:  (um SPAM zu vermeiden)

Veröffentliche dein Standardprofil im Verzeichnis der lokalen Seite?  Ja  Nein

Veröffentliche dein Standardprofil im weltweiten Verzeichnis?  Ja  Nein

Liste der Kontakte vor Betrachtern des Standardprofils verbergen?  Ja  Nein

Profil-Details vor unbekanntem Betrachtern verbergen?  Ja  Nein

Deinen Kontakten erlauben, auf deine Pinnwand zu schreiben?  Ja  Nein

Deinen Kontakten erlauben, deine Beiträge mit Schlagwörtern zu versehen?  Ja  Nein

Erlaube uns dich als potenziellen Kontakt für neue Mitglieder vorzuschlagen?  Ja  Nein

Erlaube es Unbekannten dir private Nachrichten zu schreiben?  Ja  Nein

Maximale Anzahl von privaten Nachrichten, die dir unbekannte Personen pro Tag senden dürfen:  (um SPAM zu vermeiden)

Beiträge verfallen automatisch nach dieser Anzahl von Tagen:  (Wenn leer verfallen Beiträge nie automatisch. Verfallene Beiträge werden gel.)

[Erweitertes Verhalten](#)

Verbindungs-Einstellungen

Eingebaute Unterstützung für Verbindungen zu Diaspora ist eingeschaltet  
Eingebaute Unterstützung für Verbindungen zu StatusNet ist eingeschaltet

**Facebook**

Facebook-Verbindungseinstellungen

**StatusNet Beitragseinstellungen**

Veröffentlichung bei StatusNet erlauben

Veröffentliche öffentliche Beiträge standardmäßig bei StatusNet

OAuth-Konfiguration löschen

**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/amod/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.org/zot/1.0" type="http://purl.org/zot/1.0/version" zot:version="1"/>
  <Property xmlns:zot="http://purl.org/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-4LHNGSRK1OhH6G4XnI4eKqPCdj-KKJyLeVtF0yF-chDsVokW0b9nir_Gw5eBgzuA8qDgTLoAMftttw5TEBg2627hgbHcJbjJf30UlkGc3Zhw7SF8t8v50joByScUXQe5aM2TU0ohvAvZ1MhLOa3CSkGSviPEb4fmEjFfG9a1VORkJs2qdiWfCNxMPbdZalohkALwTyr82v5n23mb1AixMURSxPgLJx-a9OK-9DniY4nrU_H3pbamQm7mxIg-a0Xuh386LlcLmKzTRG0Z8dy3_uwRaPvJuv3NnlGhAzrU_8VtWB1pbgtj6PGwGc60CF0tTTIdfIOyy01s9z7Mv4IKNhtONxrCdvkJLXVzI1vo_WE_2Alvo28xd1ysrBVqWuSX19k0is9mPbx3aC-21s_bKan9W6Irx65TUC4o5g6s3np_9_Vrks13f1iuInEVfWFC0mNnrBc2FavBq75HrvXXm_VYLYz-EWIJ9Nktb216Umcr5.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	<a href="#">post</a>
add	<a href="#">add</a>
cancel	<a href="#">cancel</a>
checkin	<a href="#">checkin</a>
delete	<a href="#">delete</a>
favorite	<a href="#">favorite</a>
follow	<a href="#">follow</a>
give	<a href="#">give</a>
ignore	<a href="#">ignore</a>
invite	<a href="#">invite</a>

## *Protokolle und Datenformate*

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



## Salmon Protocol

## *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

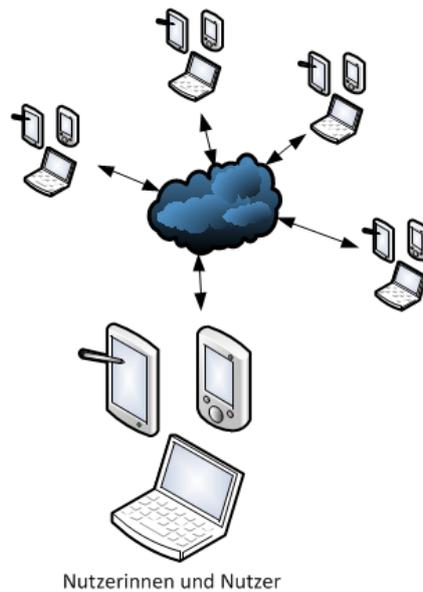
## *Risikobetrachtung*

- 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



# 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](mailto:ULD3@datenschutzzentrum.de)