

Datenschleudern im Web-2.0: Gläserne Menschen durch soziale Netzwerke

- ➔ 17. DFN Workshop, Hamburg — 10. Februar 2010
- © Dominik Birk, Felix Gröbert, Dr. Christoph Wegener
- ☎ felix@groeibert.org
- ✂ creativecommons.org/licenses/by-nc-nd/3.0/de

Mitwirkende



Dominik Birk



Felix Gröbert



Dr. Christoph Wegener

Menschen & Technik

Wert von Information

Information	Preis in US\$
Internetbanking Zugang	10–1000
Kreditkarten mit CCV2	0,50–12
Kreditkarten	0,10–25
E-Mail Adressen	ca. 0,35 / MB
komplette Identitäten	0,90–25
Cash-out Service	8-50% share
Proxy	0,30–20
angepasster Banking-Trojaner	1000

Quellen: Panda Labs: The Business of Cybercrime, Symantec Report on the Underground Economy

Wert von Information

Information	Preis in US\$
Internetbanking Zugang	10–1000
Kreditkarten mit CCV2	0,50–12
Kreditkarten	0,10–25
E-Mail Adressen	ca. 0,35 / MB
komplette Identitäten	0,90–25
Cash-out Service	8-50% share
Proxy	0,30–20
angepasster Banking-Trojaner	1000

Quellen: Panda Labs: The Business of Cybercrime, Symantec Report on the Underground Economy

Identitätsdiebstahl

- Missbräuchliche Nutzung personenbezogener Daten einer Identität durch Dritte
- *„Identitätsdiebstahl ist eine der am stärksten zunehmenden Kriminalitätsformen in hochtechnisierten Ländern.“ – FTC*

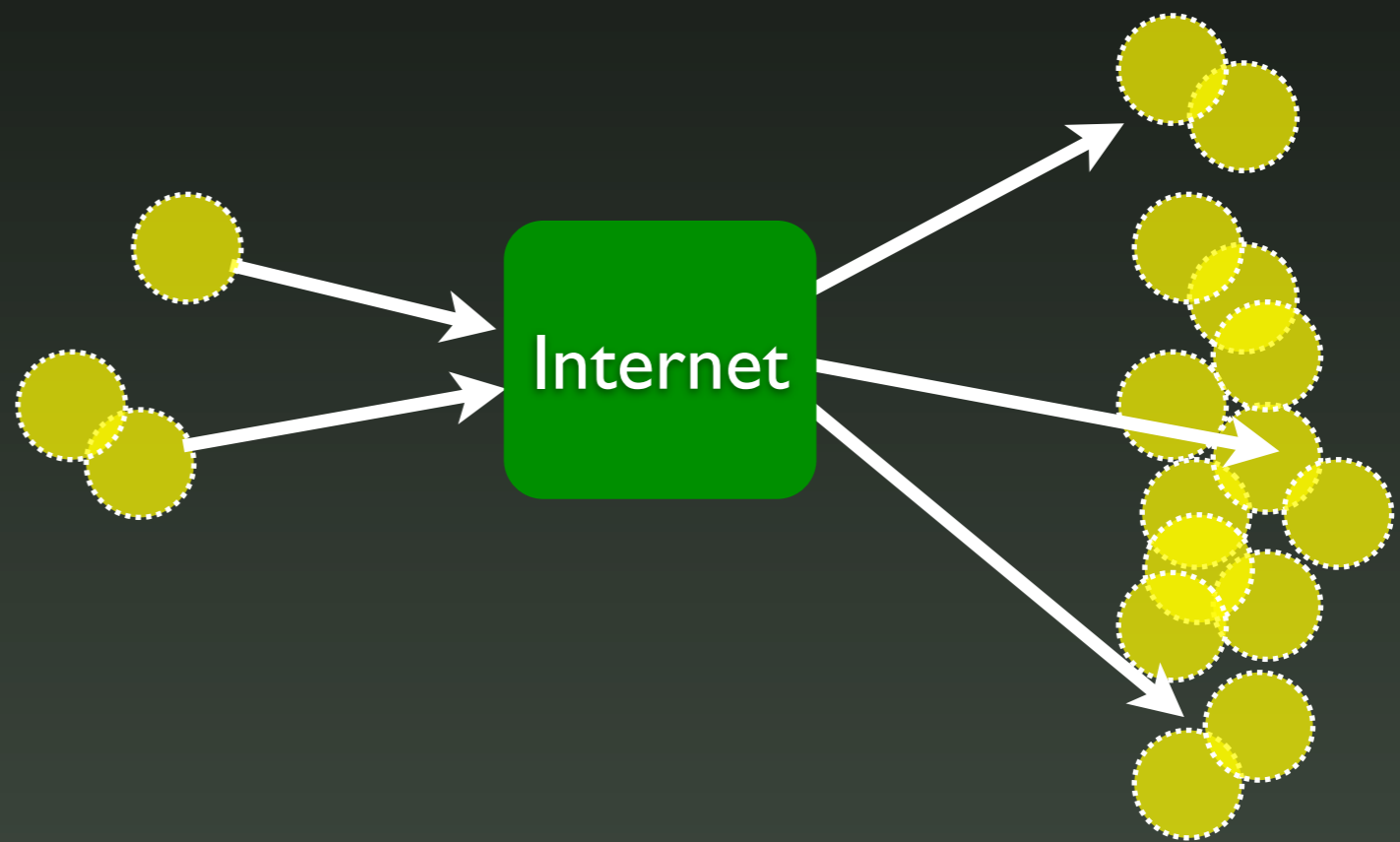
Attribut	Gefahr
Name	Niedrig
Adresse	Niedrig
Geburtsdatum	Mittel
SSN	Hoch
Bank Konto	Hoch
Passwort	Hoch
PIN	Hoch

Quelle: yourcreditadvisor.com

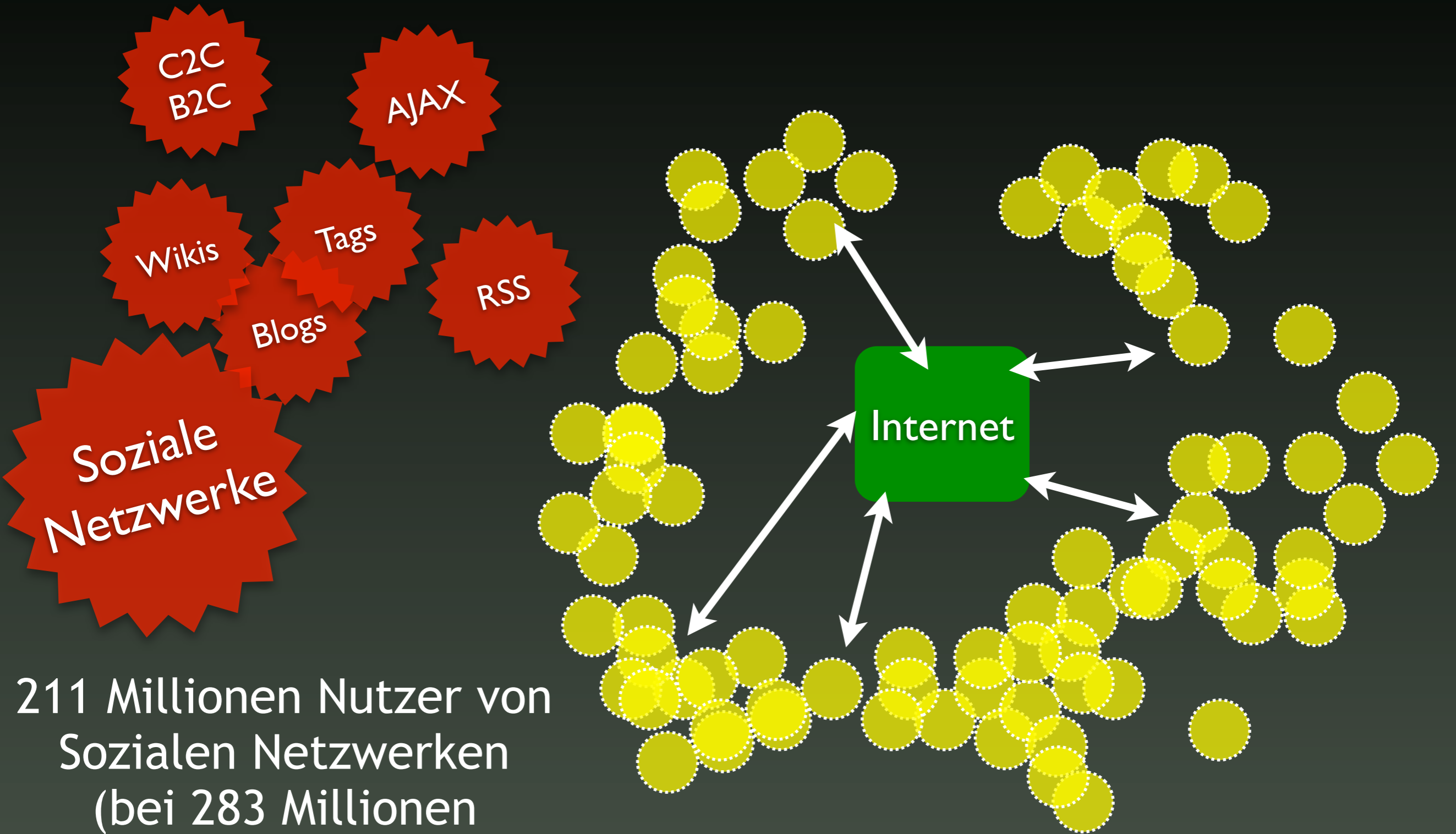
Web 1.0

E-Mail

B2C
E-Commerce



Web 2.0



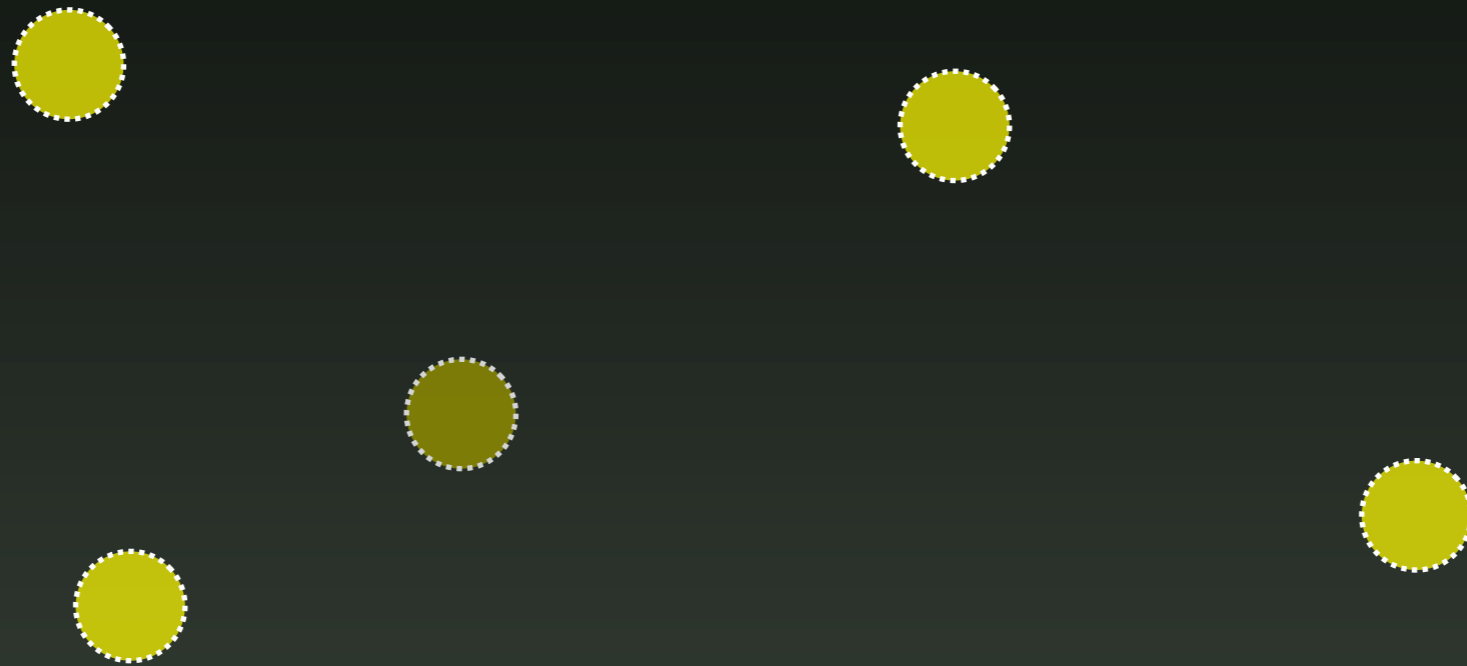
211 Millionen Nutzer von
Sozialen Netzwerken
(bei 283 Millionen
Internetnutzern in der EU)

Web 2.0 Hebel

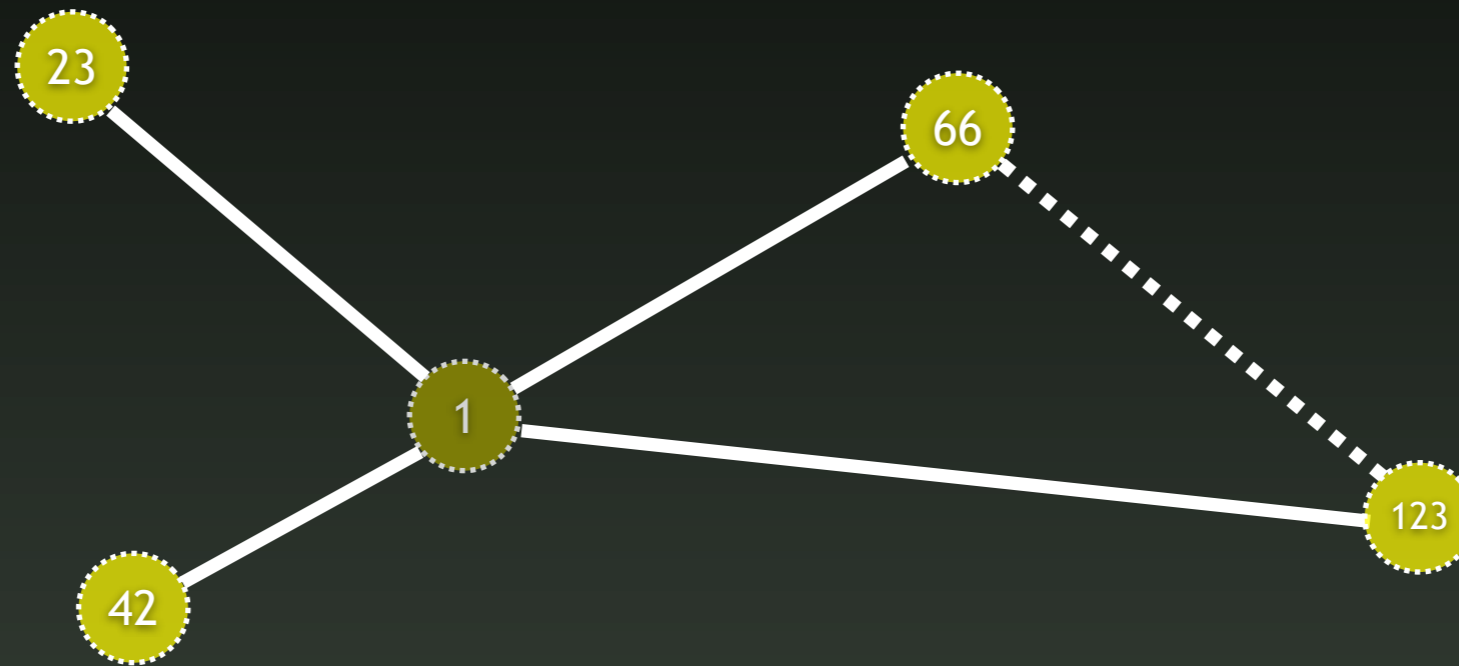
- Viele verschiedene Dienste mit offenen Schnittstellen
- Essenz: multimediale, personenbezogene Daten
- Daten sammeln, durch Verknüpfung anreichern
 - ❖ Wert der Daten steigt
 - ➔ Weiterverkauf
 - ➔ Nutzen der angereicherten Daten



Modellierung Soziale Netzwerke

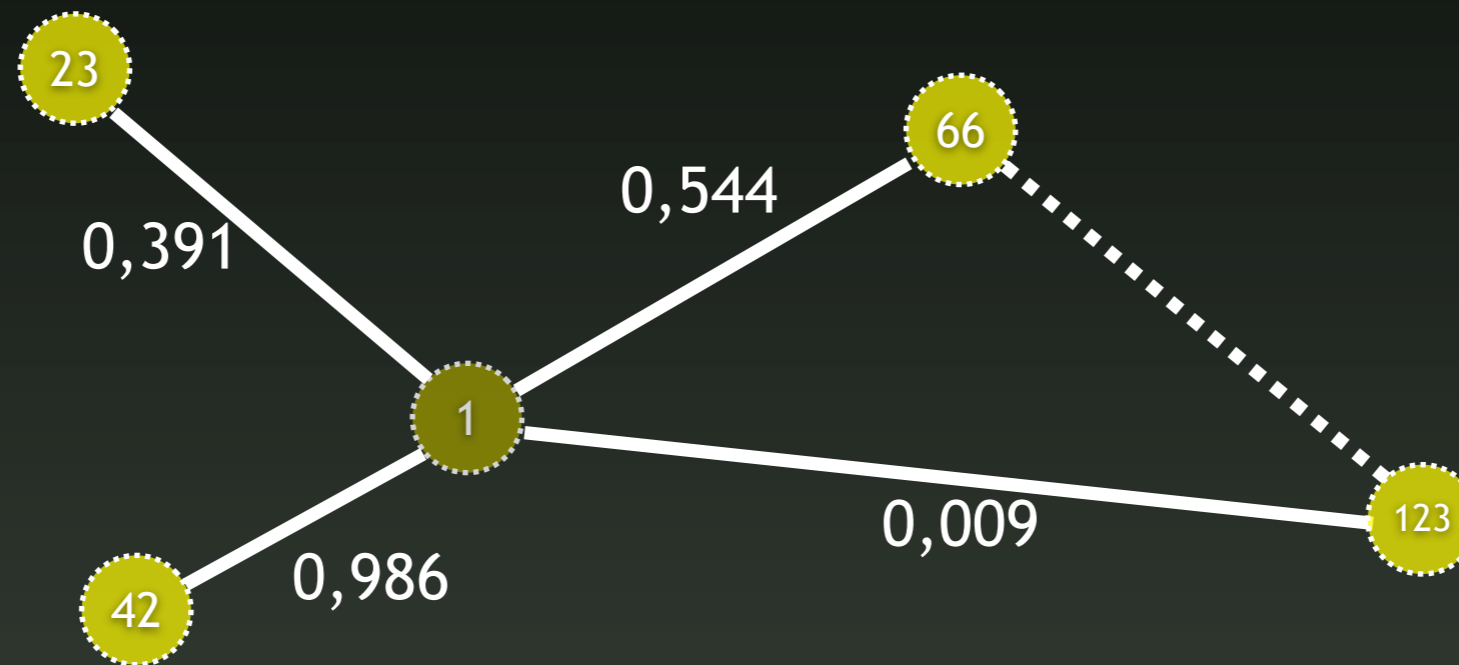


Soziale Netzwerke



i_n	23	42	66	123

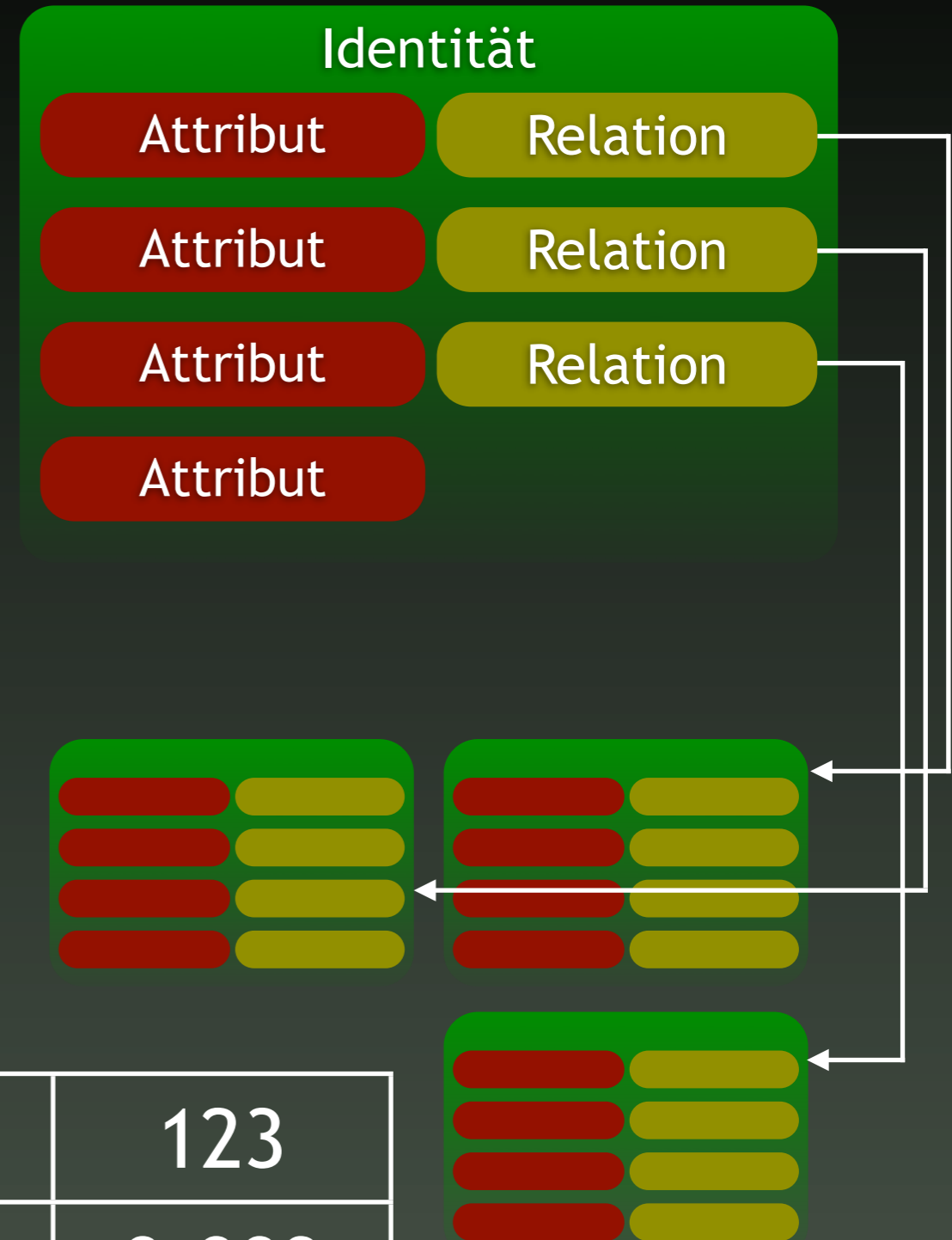
Soziale Netzwerke



i_n	23	42	66	123
w_n	0,391	0,986	0,544	0,009

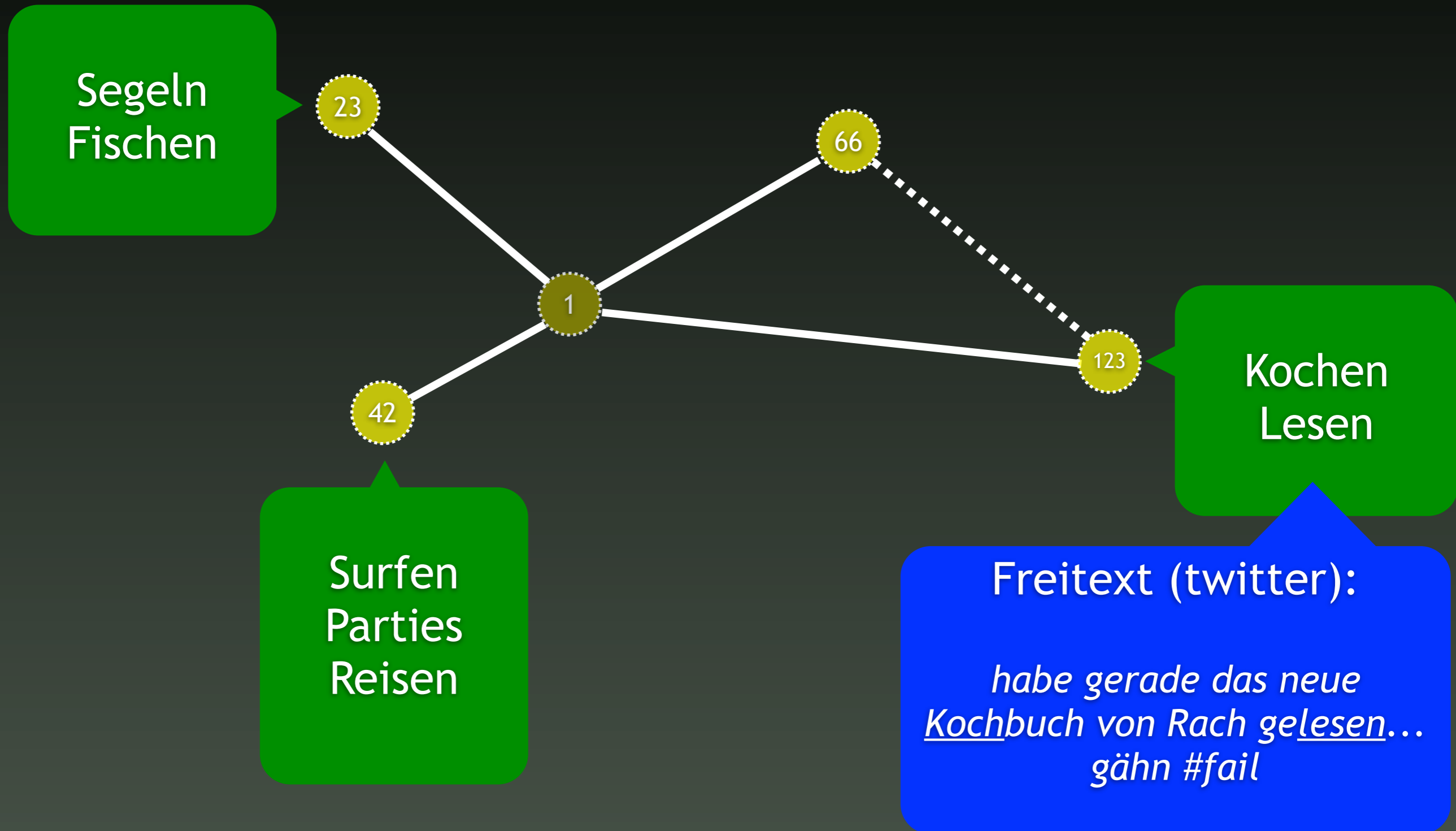
Identität

- $(i, A, R) = 3$ -Tupel zur Beschreibung einer Identität
- Attribute:
Name, Adresse, Hobbys, Geburtsdatum, E-Mail, Arbeitgeber, CV, Mitgliedschaften
- Relationen:



i_n	23	42	66	123
w_n	0,391	0,986	0,544	0,009

Aggregation



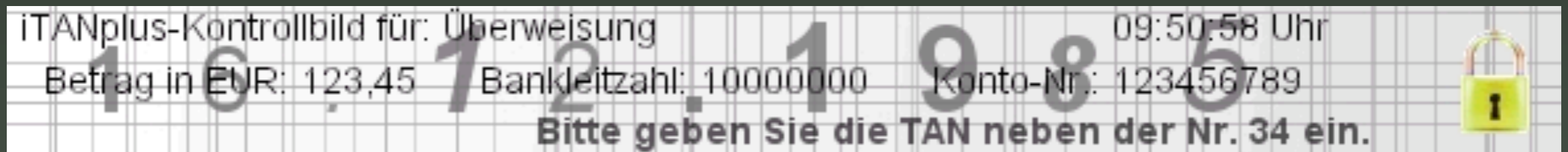
Datenbeschaffung



- Methoden:
 - ❖ Crawling
 - ❖ Cracking
 - ❖ Buying

Angriffsvektoren: Crawling

- Crawling
 - ❖ Iterieren über `profile.php?id=12001`
 - ❖ Einheitliche Darstellung & Strukturen
 - ❖ Captchas - Turingtest zur Differenzierung zwischen Mensch und Maschine



prefuse | graphview

Data

BodyForce

GravitationalConst... -10.0

Distance -1.0

BarnesHutTheta 0.899

DragForce

DragCoefficient 0.009

SpringForce

SpringCoefficient 9.99E-5

DefaultSpringLength 50.0

Connectivity Filter

Distance 30

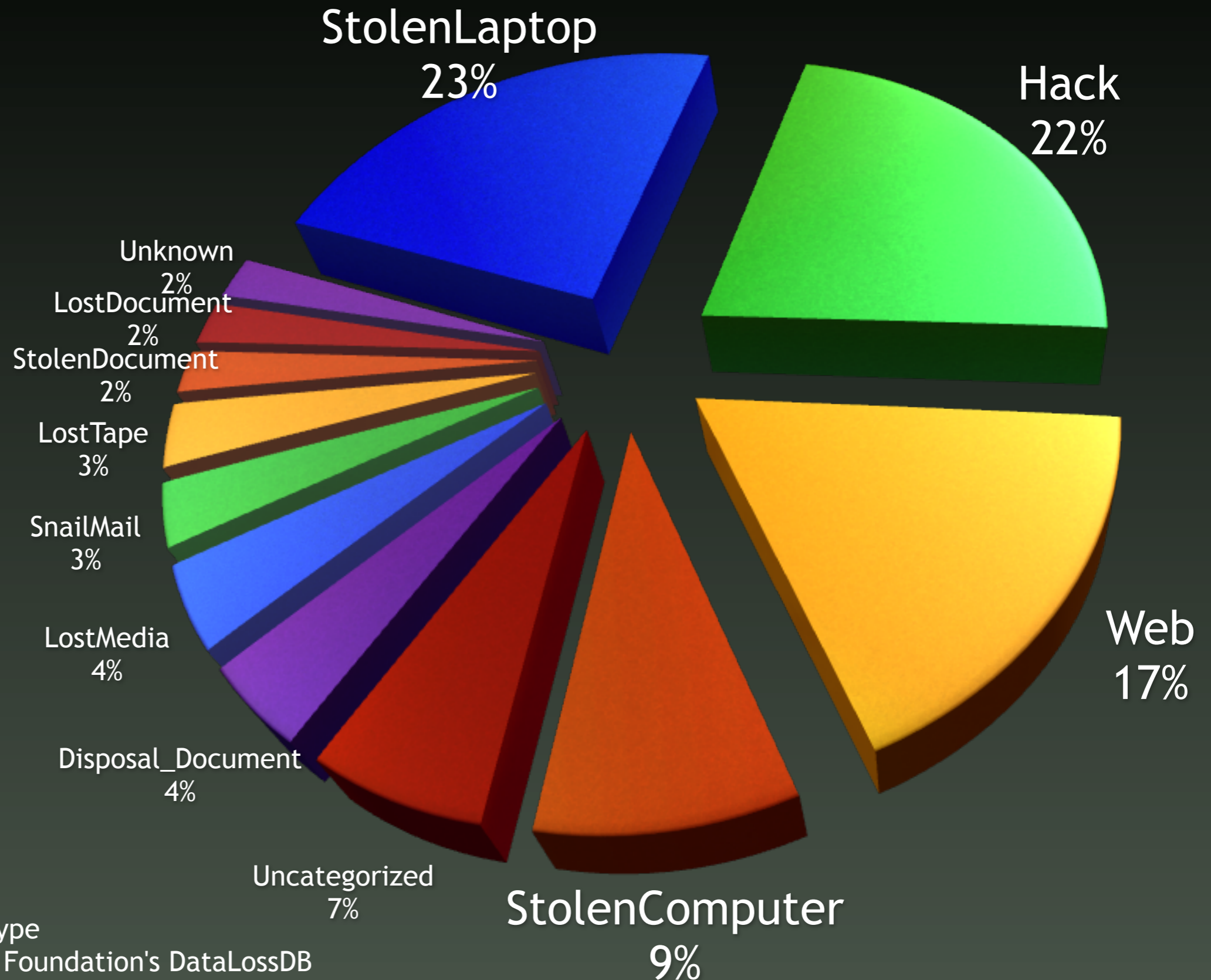
Start | Postein... | Deathcr... | 212. Pin... | FlashFIP | Lokaler... | Java 2... | prefuse | Java -... | Downlo... | 16:37

Quelle: <http://icepic.org/wiki/doku.php?id=studivz-analyse-tool>

Angriffsvektoren: Cracking

- Cracking
 - ❖ Breites Angriffsspektrum, Technologievielfalt
 - ❖ SQL Injection häufigst gemeldete Schwachstellenkategorie
 - ❖ Im Zeitraum vom 1.1. bis 29.7.08:
25118409 personenbezogene Daten gestohlen

Angriffsvektoren: Cracking

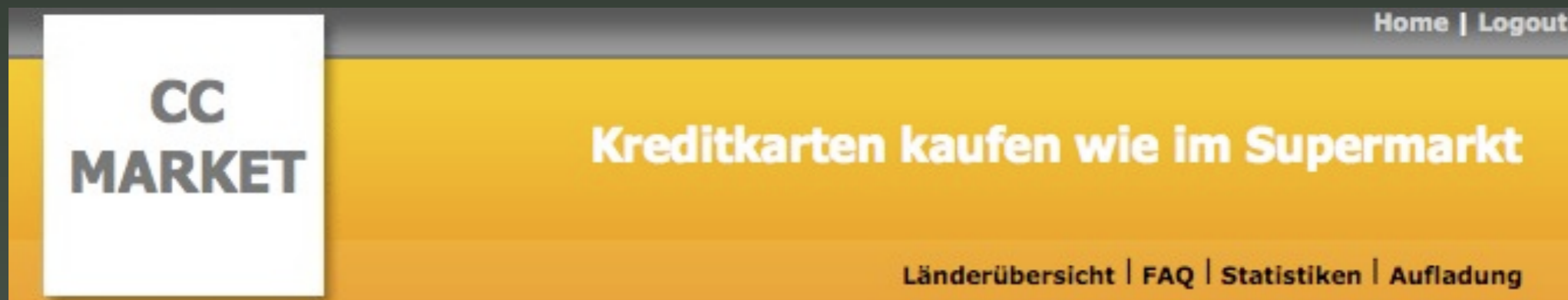
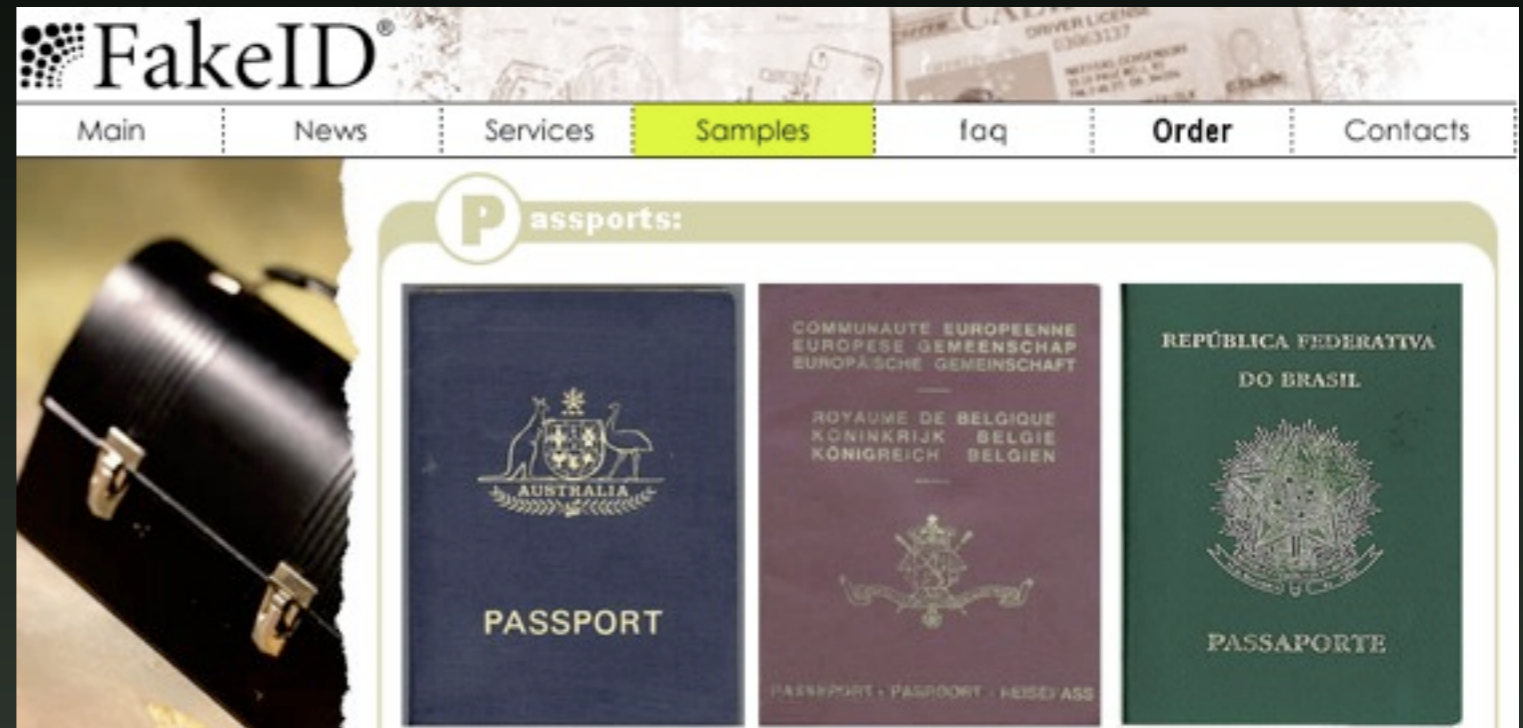


Incidents by Breach Type

Quelle: Open Security Foundation's DataLossDB

Angriffsvektor: Buying

- Illegaler Einkauf
 - ❖ Foren, IM, IRC
- Legalen Einkauf
 - ❖ Datenhändler
 - ❖ Call Center
 - ❖ Crawling Services (80legs)



studiVZ Web
Leute finden

- Start
- Meine Seite ändern
- Meine Freunde
- Meine Fotos
- Meine Gruppen
- Nachrichtendienst
- Mein Account
- Privatsphäre

studiVZ-Eleganz:
Die Wahl: April

Top Suche -Anzeige-

- Arena
- Veranstaltung
- Videothek
- Event
- Kinofilm



Alle Freunde von Sara

Sara eine Nachricht schicken

Sara gruscheln

Sara als Freund hinzufügen

Sara melden

Gemeinsame Freunde

Freunde (gleiche Hochschule)

Sara hat 8 Freunde an der Uni Passau



David Tasche



Kira Reinert



Tobias R.....



Fabian Lennartz



Thomas Siemes



Robbin Altmann

Verbindung

Keine gefunden

Information

Account

Name: Sara Bongartz
Mitglied seit: 30.06.2006
Letztes Update: 09.05.2007

Allgemeines

Hochschule: Uni Passau (seit 2005)
Status: Studentin
Geschlecht: weiblich
Studienrichtung: Jura / Rechtswissenschaft
Heimatland: D
Heimatstadt: Passau
Land: Deutschland

Persönliches

Beziehungsstatus: solo
Politische Richtung: unpolitisch

Interessen:

Filme, Partys, Freunde, Sport, Segeln,

Lieblingsbücher: Damien Rice...
Herr der Ringe, Geh wohin dein Herz dich trägt, Girl next door---
Lieblingsfilme: Forrest Gump, Fear and Loathing in Las Vegas, die Farbe lila, die Reifeprüfung
Lieblingszitat: Go stand in the middle of the street and wait for me, I'll be right back
Über sich selbst: absolut wahnsinnig































Gruppen

- Alles~ist~Scheiße
- Anti-Polohemdtragen-hochgeklappt-Träger
- Die Bibel - Wahn oder Sinn??
- Drawn Together Fanclub
- gott gibt es nicht
- Ich habe Tolstois "Krieg und Frieden" komplett gelesen!
- Indie - Fans
- Mark Twain - The Awful German Language
- Moderne Christen
- Mütter holt die Kinder rein, Natascha hatn Führerschein

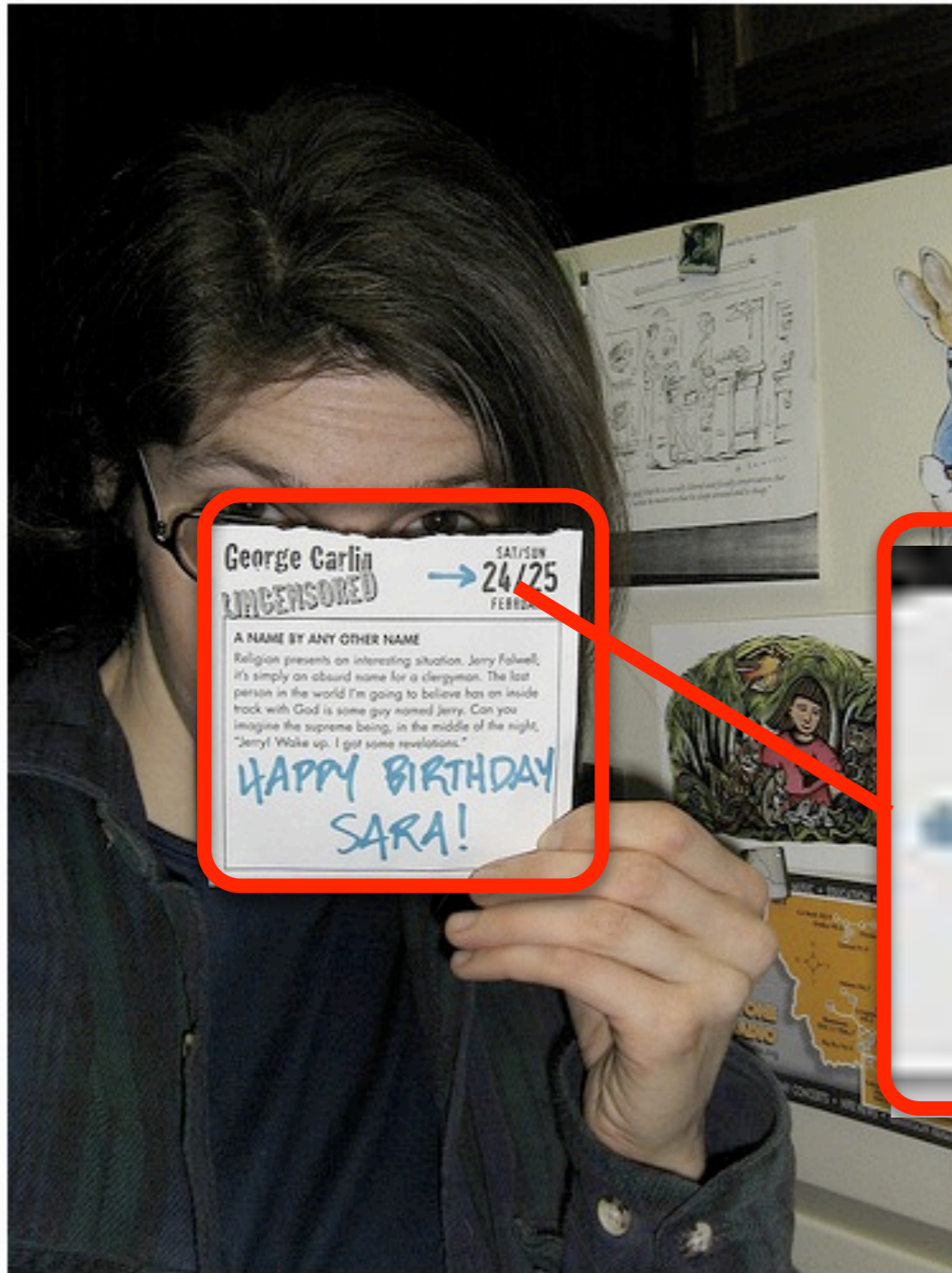
Verbindungen zu Sara Bongartz

Verbindungen 1-10 von 11

<< Zurück | Weiter >>

- | | | | | |
|--|---|--|---|---|
| 
Rudi Ruppert
Uni ID-Theft | 
Peter Schurzer  
Ernst & Old AG | 
Donald Duck 
Ernst & Old AG | 
Dieter Obermann 
Adventure AG | 
Sara Bongartz
Adventure AG |
| 
Rudi Ruppert
Uni ID-Theft | 
Abraham Aldahaussen
Creative-Media &
Communication
Consulting | 
Kai Baumstamm  
krasse AG | 
Dr. Hendrik Wurzler 
Adventure AG | 
Sara Bongartz
Adventure AG |
| 
Rudi Ruppert
Uni ID-Theft | 
Dr. Franz Futtermann 
It-blubb | 
Florian Bummel 
Sun Minispielzeug GmbH | 
Bernd Bretter
Adventure AG | 
Sara Bongartz
Adventure AG |
| 
Rudi Ruppert
Uni ID-Theft | 
Ertschan Sinnvoll 
Ching-Chang AG | 
Jörg Hengst
Oral GmbH | 
Bruder Erbstrahl
Esterella Corporation | 
Sara Bongartz
Adventure AG |

geburtstagsgruss von maike



maike hat mir diese liebe foto gruss karte letztes jahr geschickt

Hochgeladen am 10. März 2007 von [sara.bongratz](#)

Fotostream von sara.bongratz



906 Fotos

durchsuchen

Dieses Foto gehört auch zu:

2007 in birthdays, with george carlin (Album)

7 Fotos



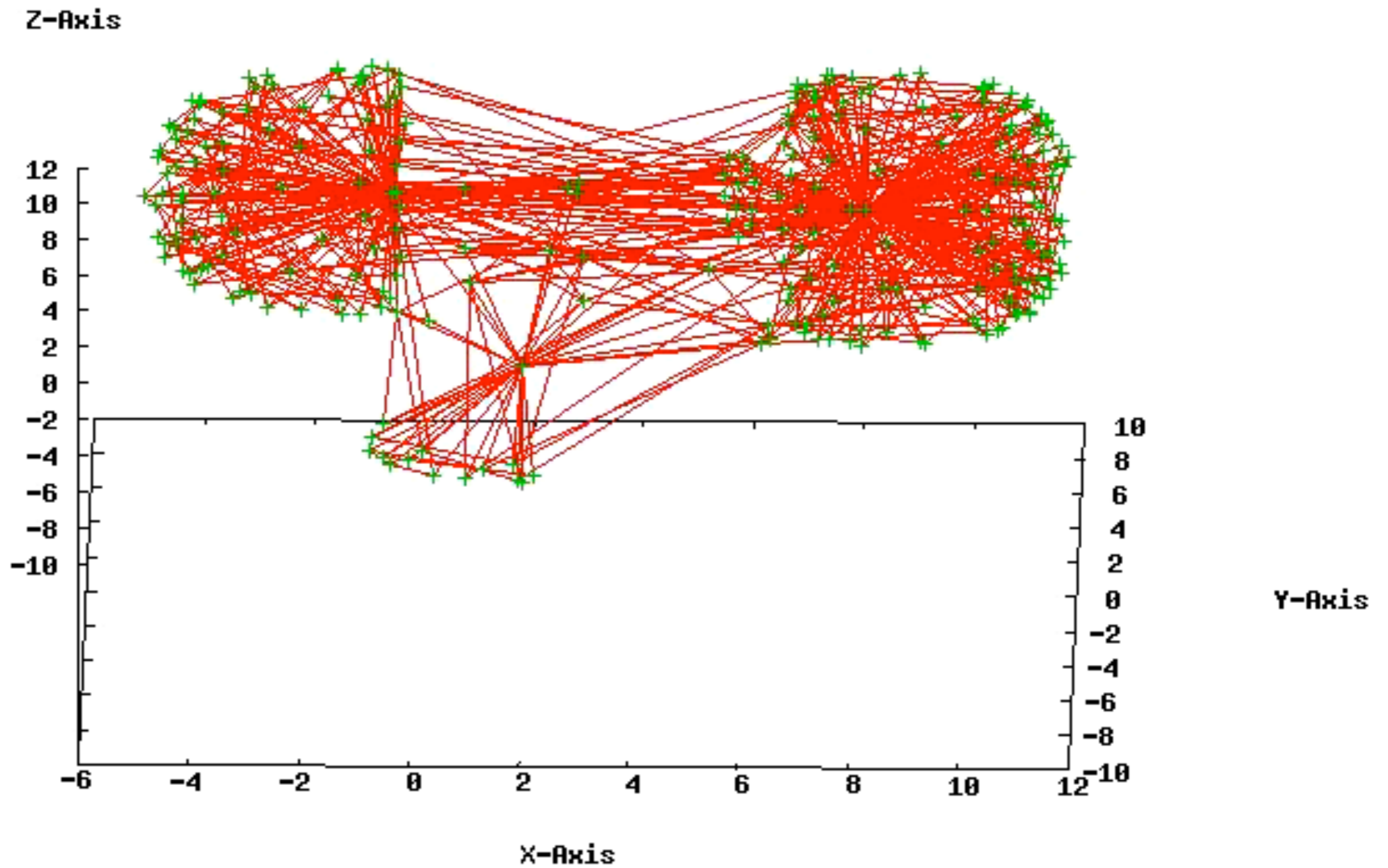
Weitere Informationen

Bestimmte Rechte vorbehalten.

- Aufgenommen mit [Canon PowerShot A410](#). [Weitere Eigenschaften](#)
- Aufgenommen: 10. März 2007
- [Weitere Größen anzeigen](#)
- 54-mal angesehen

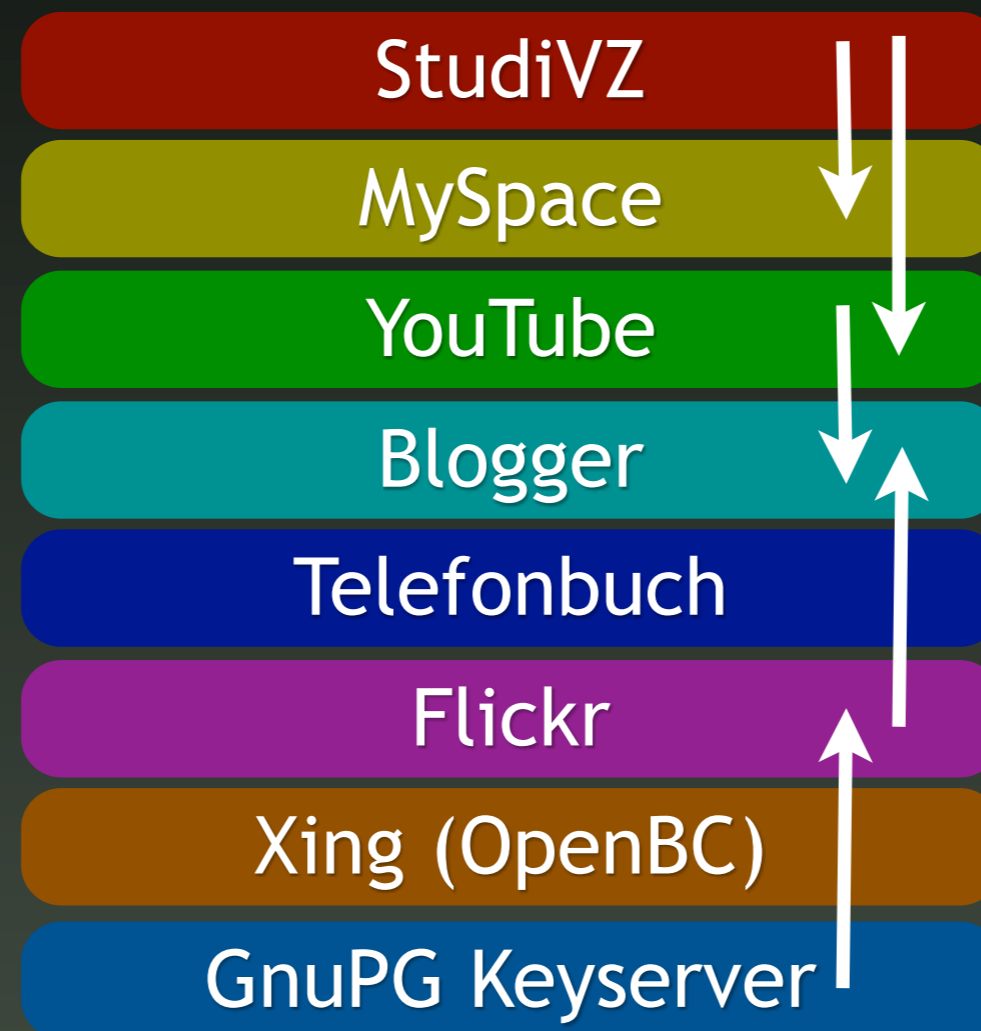
cycle 1=3

Resultat



Quelle: Alexander Kasper

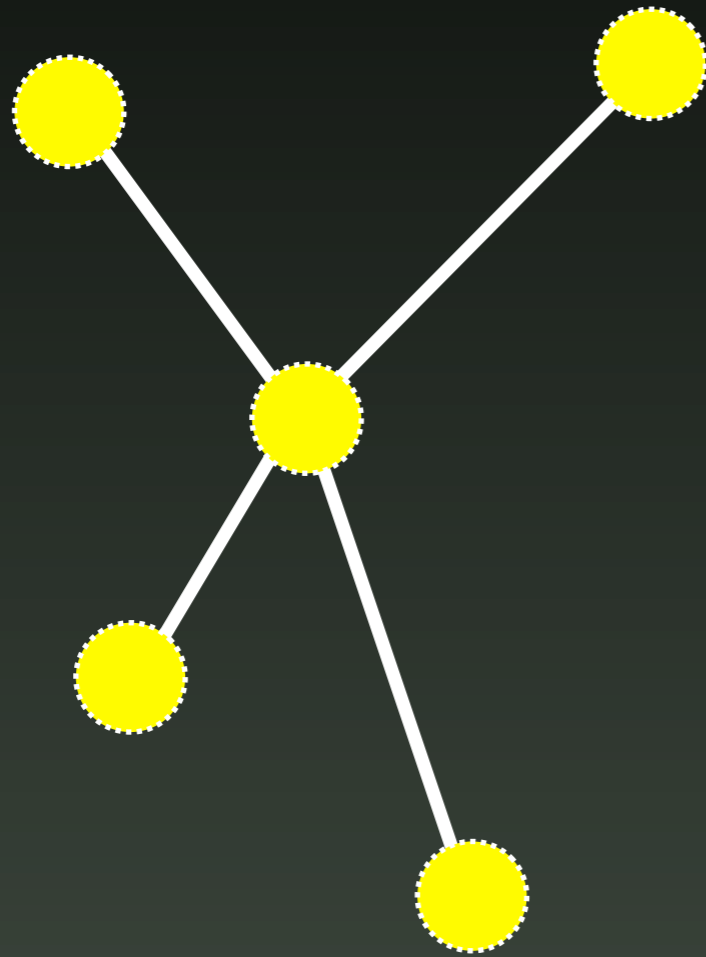
Profilergänzung



↑ Korrelation

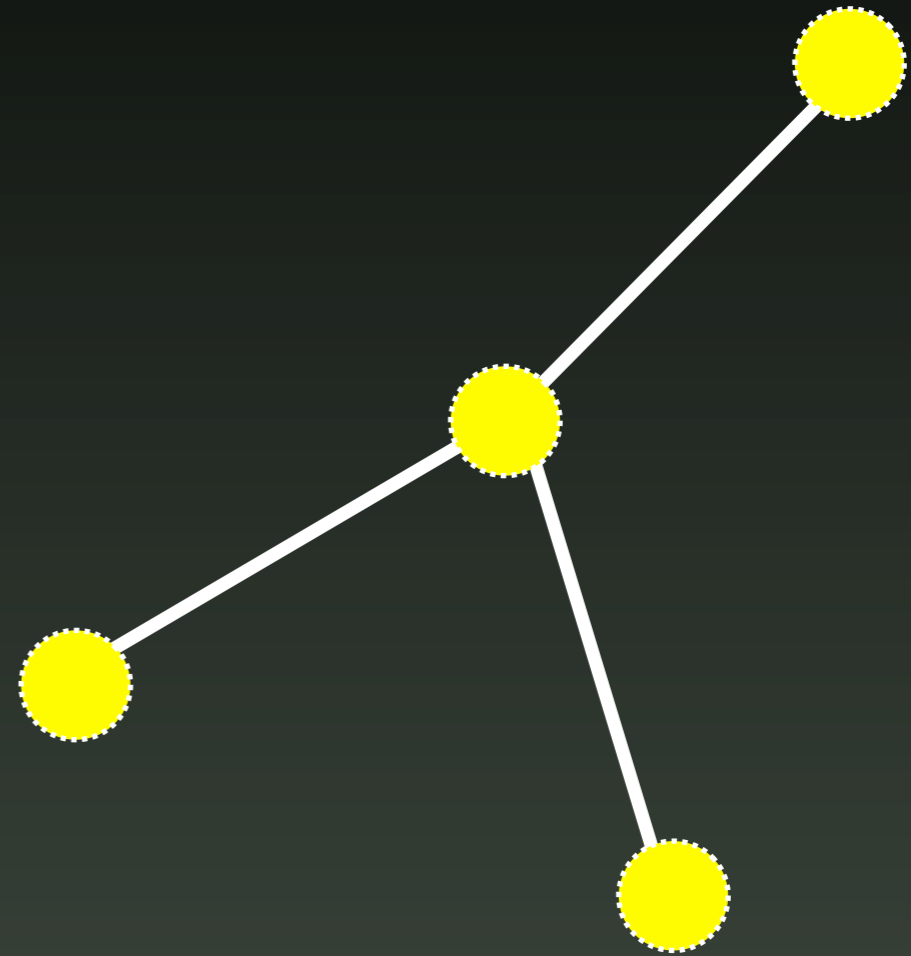
Korrelation

Netzwerk 1



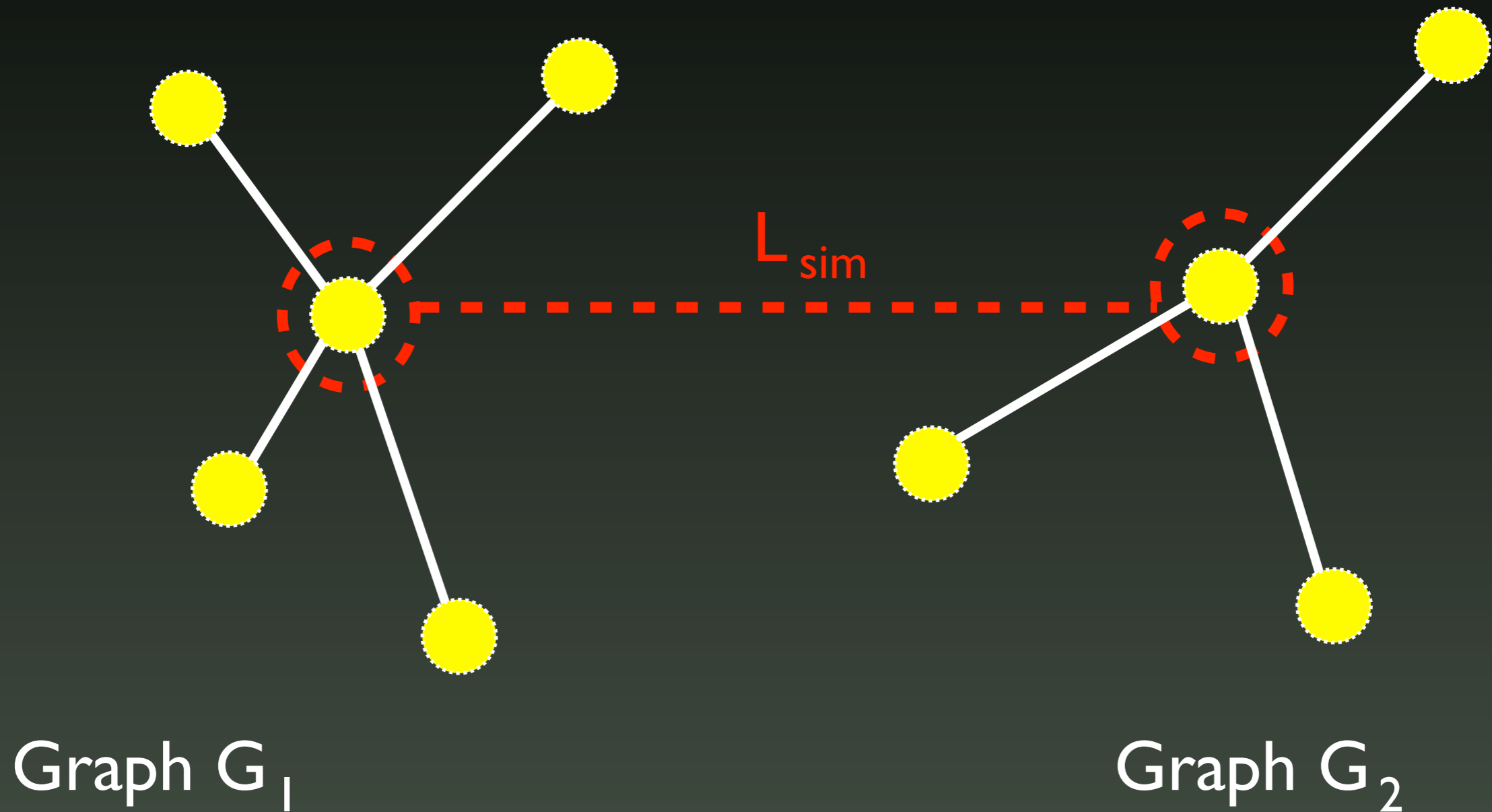
Graph G_1

Netzwerk 2

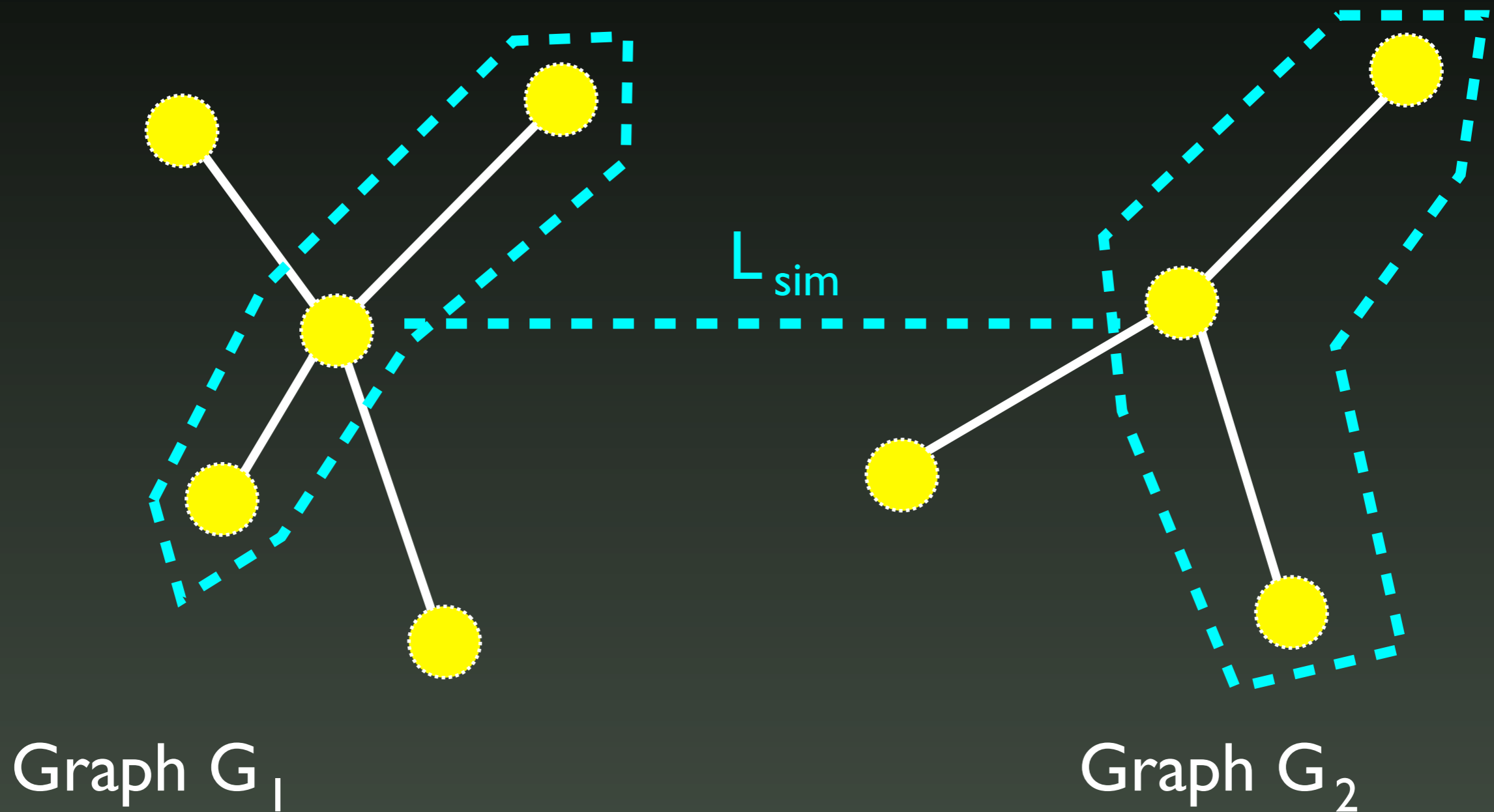


Graph G_2

Korrelation



Korrelation

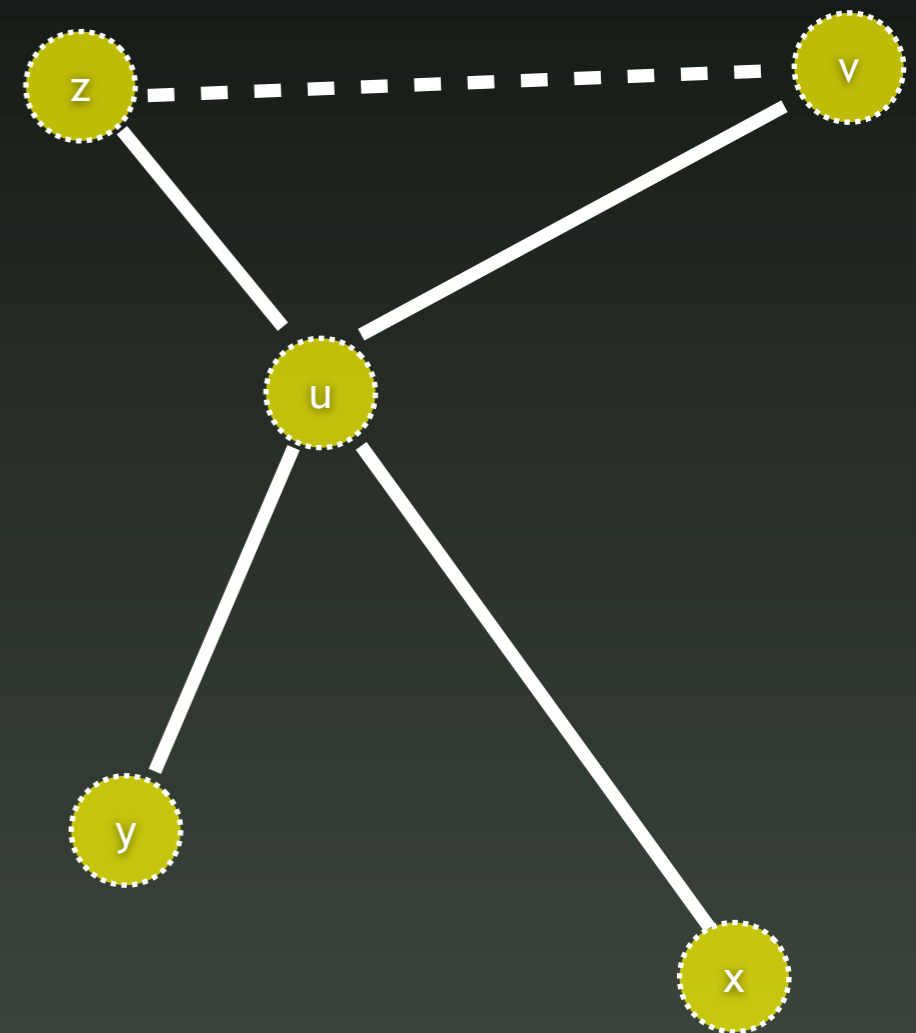


Attribut-basierte Korrelation

- 87 % der Amerikaner sind *eindeutig* identifizierbar über die drei Attribute:
Quelle: <http://bit.ly/a2Pct>
 - ❖ Geschlecht
 - ❖ Postleitzahl
 - ❖ Geburtsdatum
- Zudem: weitere Attribute können über Freitexte (zB twitter) gewonnen werden

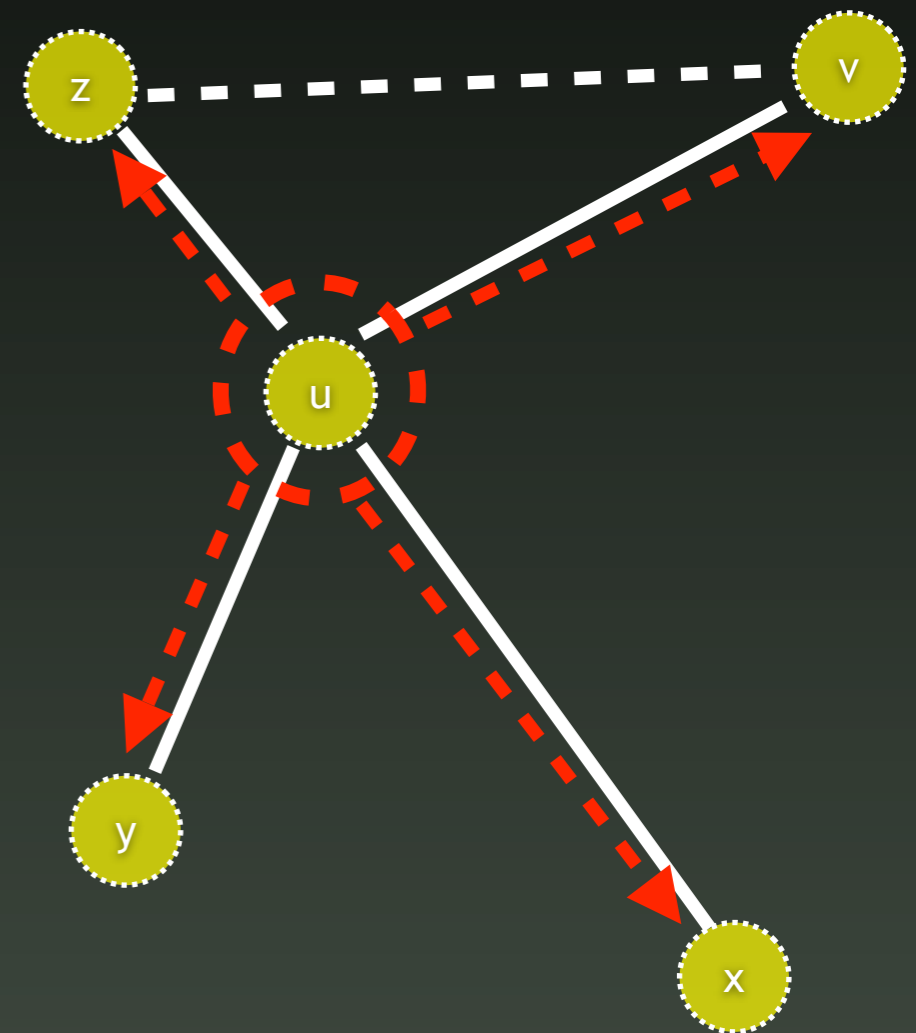
Angriffsphase

- Missbrauch der Vertrauensbeziehung unter den Nutzern
- Vorherige Phasen helfen bei Auswahl geeigneter Opfer
- Missbrauch öffentlicher, persönlicher Attribute
- „Hallo [v, x, y, z], ich bins u“



Angriffsphase

- Missbrauch der Vertrauensbeziehung unter den Nutzern
- Vorherige Phasen helfen bei Auswahl geeigneter Opfer
- Missbrauch öffentlicher, persönlicher Attribute
- „Hallo [v, x, y, z], ich bins u“



Autom. Sophisticated Phishing

- Phishing Mails verleiten das Opfer eine Aktion zu tätigen
- sophisticated, da zielgerichtete Adressierung
- (Manueller) Advanced Persistent Threat (APT) war auch beim Angriff auf Google erfolgreich

An: <bongartz@adventure-ag.de>
Von: <obermann@adventure-ag.de>

Hallo Frau Bongartz,

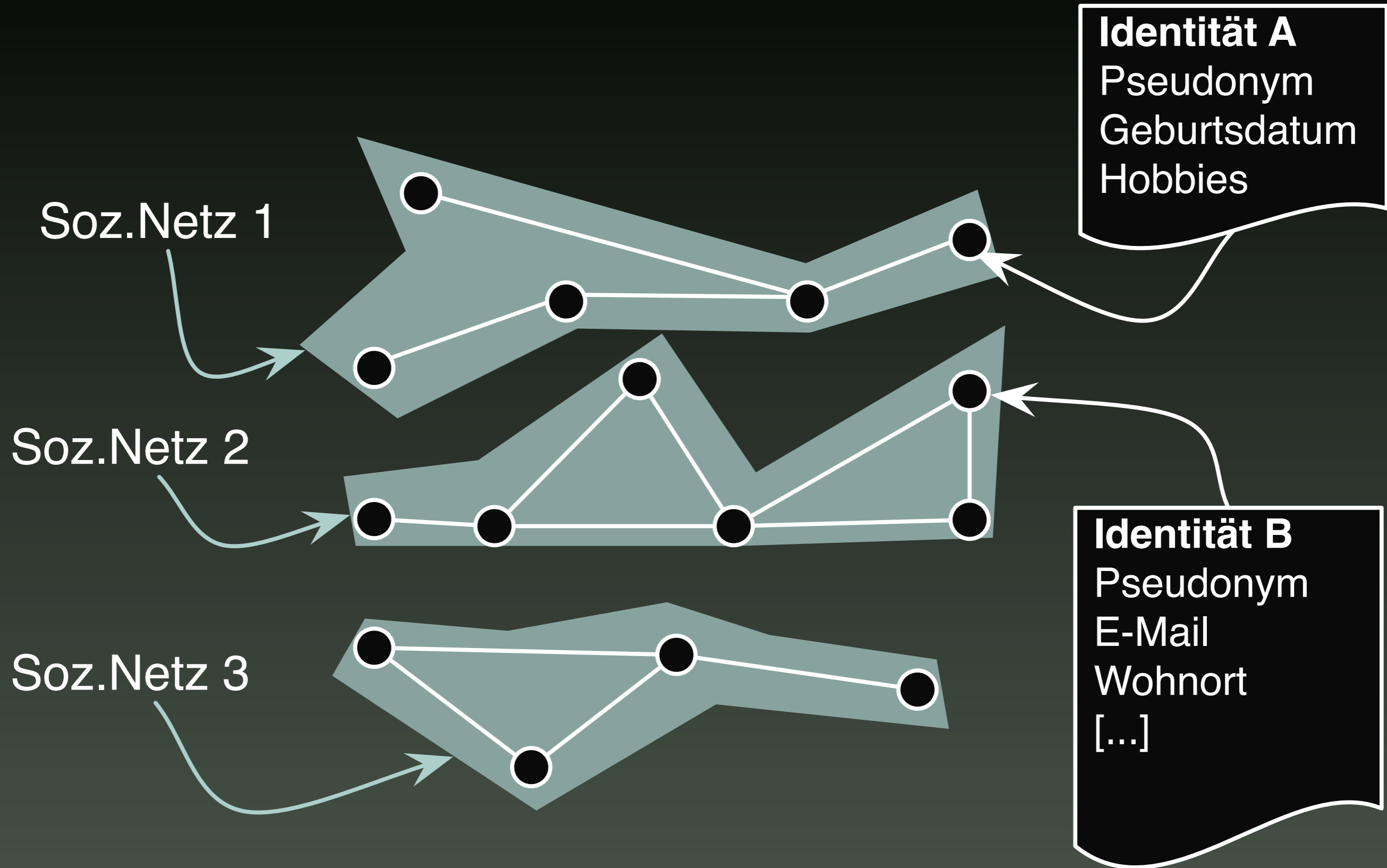
herzlichen Glückwunsch auch von mir. Uwe Mustermann hat mir gestern diesen [Link](#) vom Segeln geschickt!

Beste Grüße, Dieter Obermann

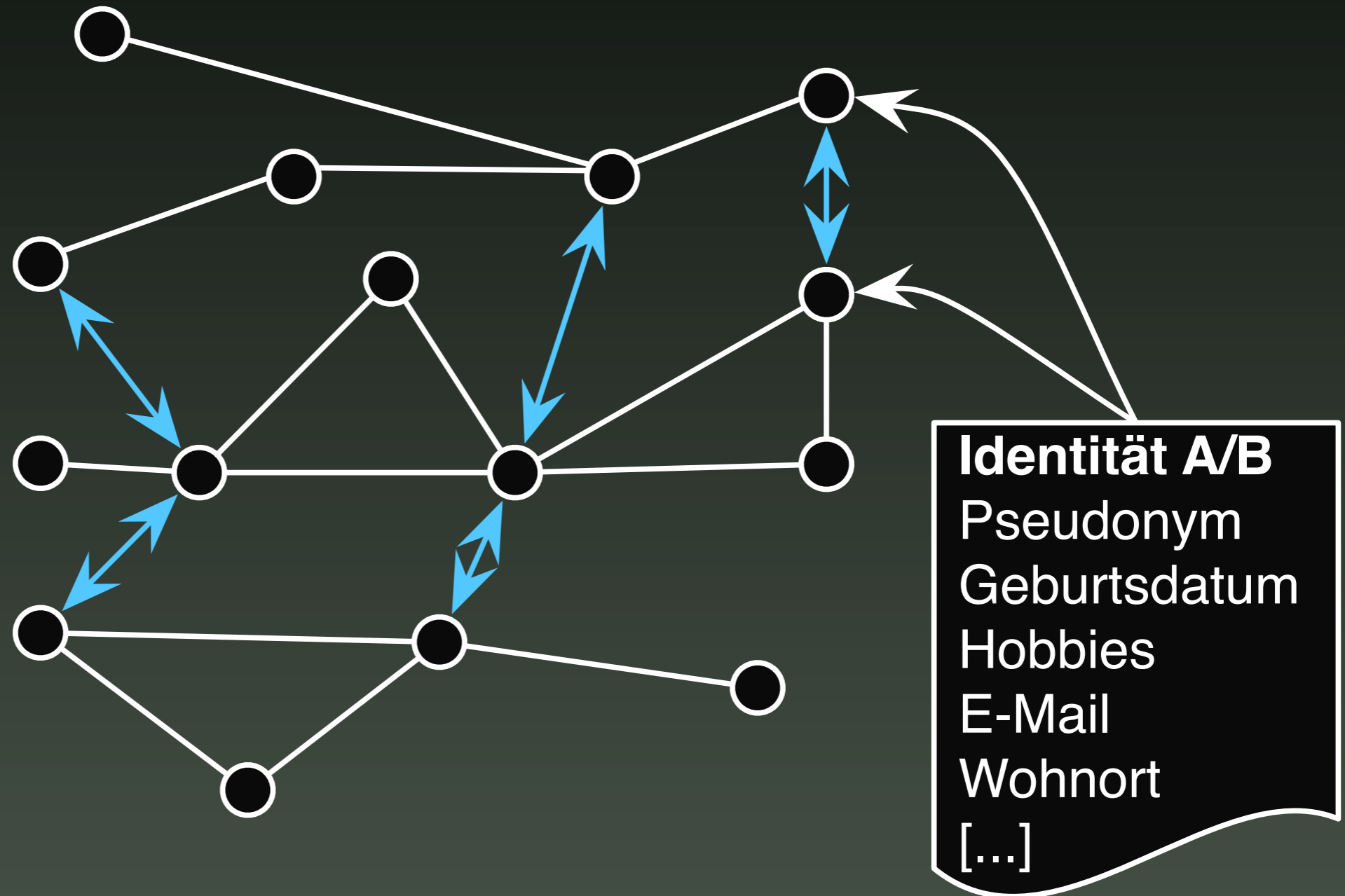
Ergebnis

- Reaktion auf eine Nachricht folgt in:
 - ❖ Datendiebstahl von Passwörtern, etc.
 - ⦿ Vertrauen durch Referenz auf Attribute und Relationen
 - ❖ Office, PDF oder Browser-basierte Malware-Infektion
 - ❖ Browser-basiertes Cross-site Request Forgery (XSRF)
 - ❖ usw.
- Wie bei Spam, macht die Automatisierung den Angriff profitabel

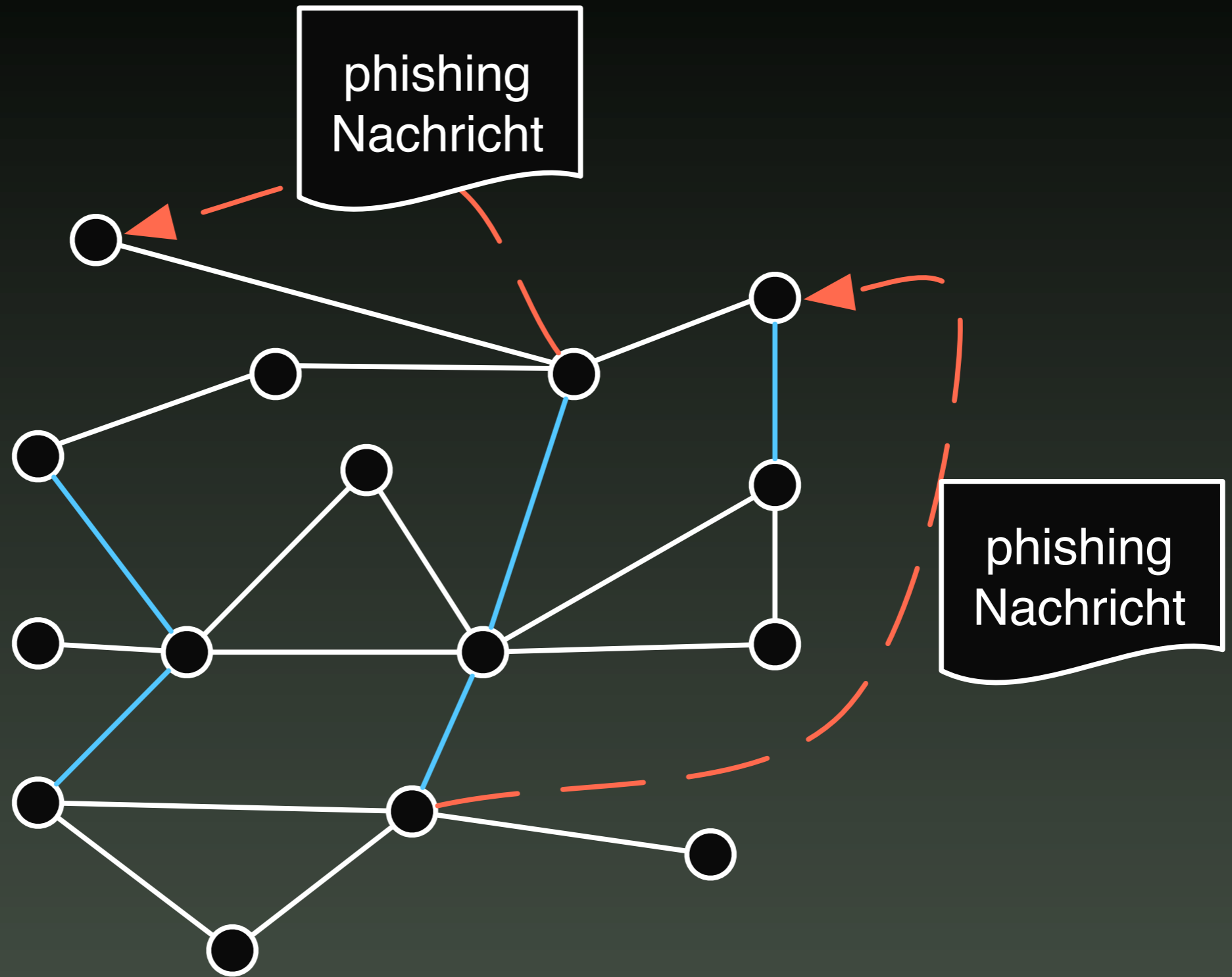
Zusammenfassung



Zusammenfassung

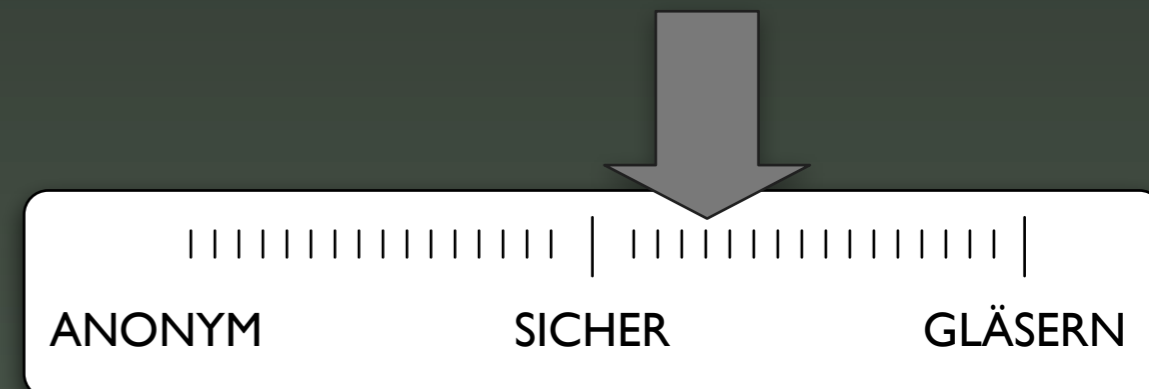


Zusammenfassung

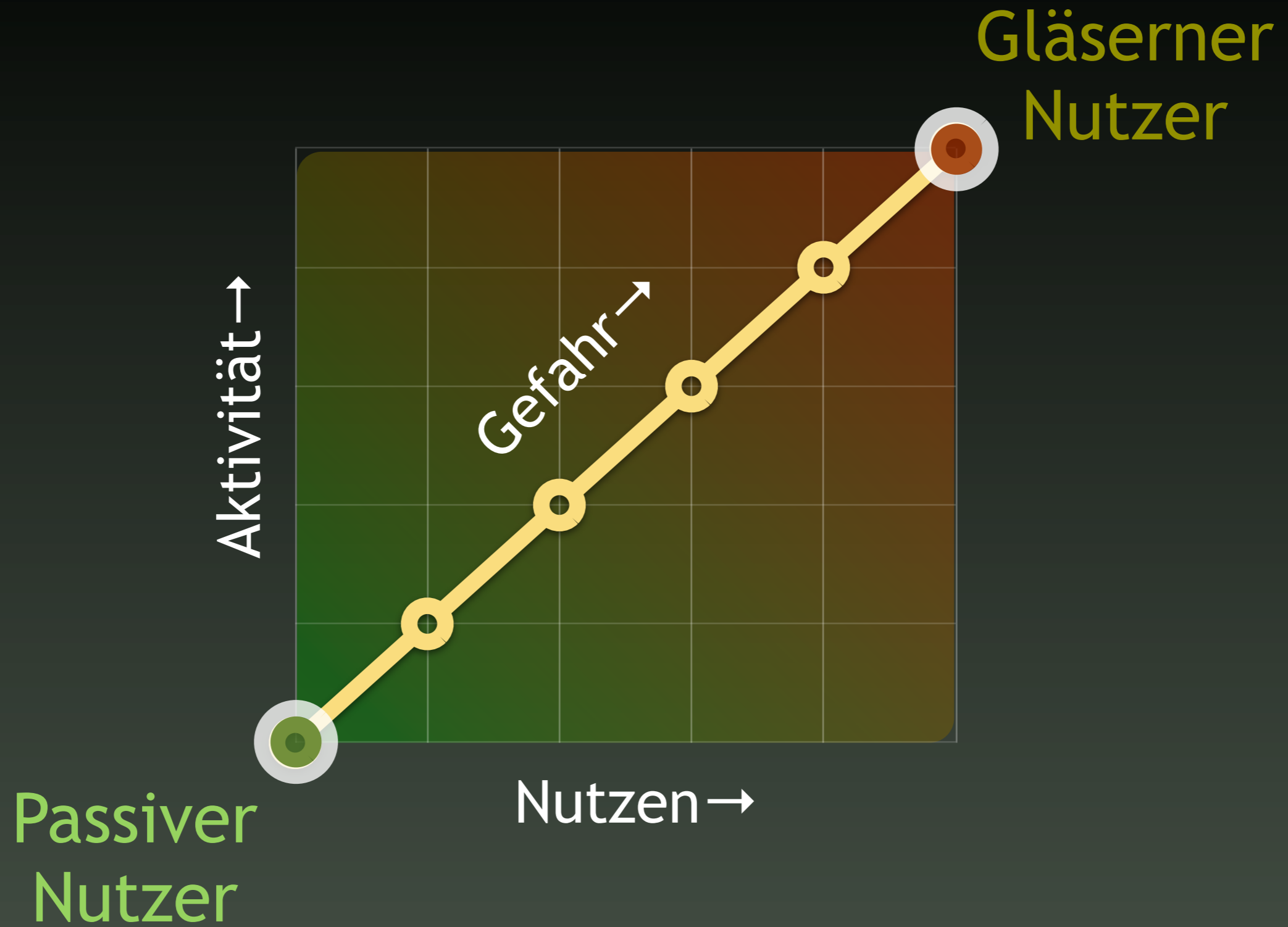


Gegenmaßnahmen

- Mehrere Ebenen:
 - ❖ Nutzer-Ebene: Pseudonyme, Datensparsamkeit
 - ❖ Anbieter-Ebene: Anti-Crawling, Software-Sicherheit
 - ❖ Allgemein:
 - ⦿ Bewusstsein für Datensparsamkeit schärfen
 - ⦿ Datenschutzmöglichkeiten der Anbieter bewerben



Balance



Fazit

- Status Quo
 - ❖ Kern von Sozialen Netzwerken sind personenbezogene Daten
 - ❖ Crawling, Korrelation und Missbrauch der Daten ist für Kriminelle leicht möglich
 - ➔ Datendiebstahl, Malware-Infektion
- Daher
 - ❖ Anbieter müssen Nutzerdaten stärker schützen
 - ❖ Datensparsamkeit beim Nutzer fördern



*Vielen Dank!
Fragen oder Anmerkungen?*



- ➔ 17. DFN Workshop, Hamburg — 10.02.2010
- © Dominik Birk, Felix Gröbert, Dr. Christoph Wegener
- ☎ felix@groeibert.org
- ✂ creativecommons.org/licenses/by-nc-nd/3.0/de