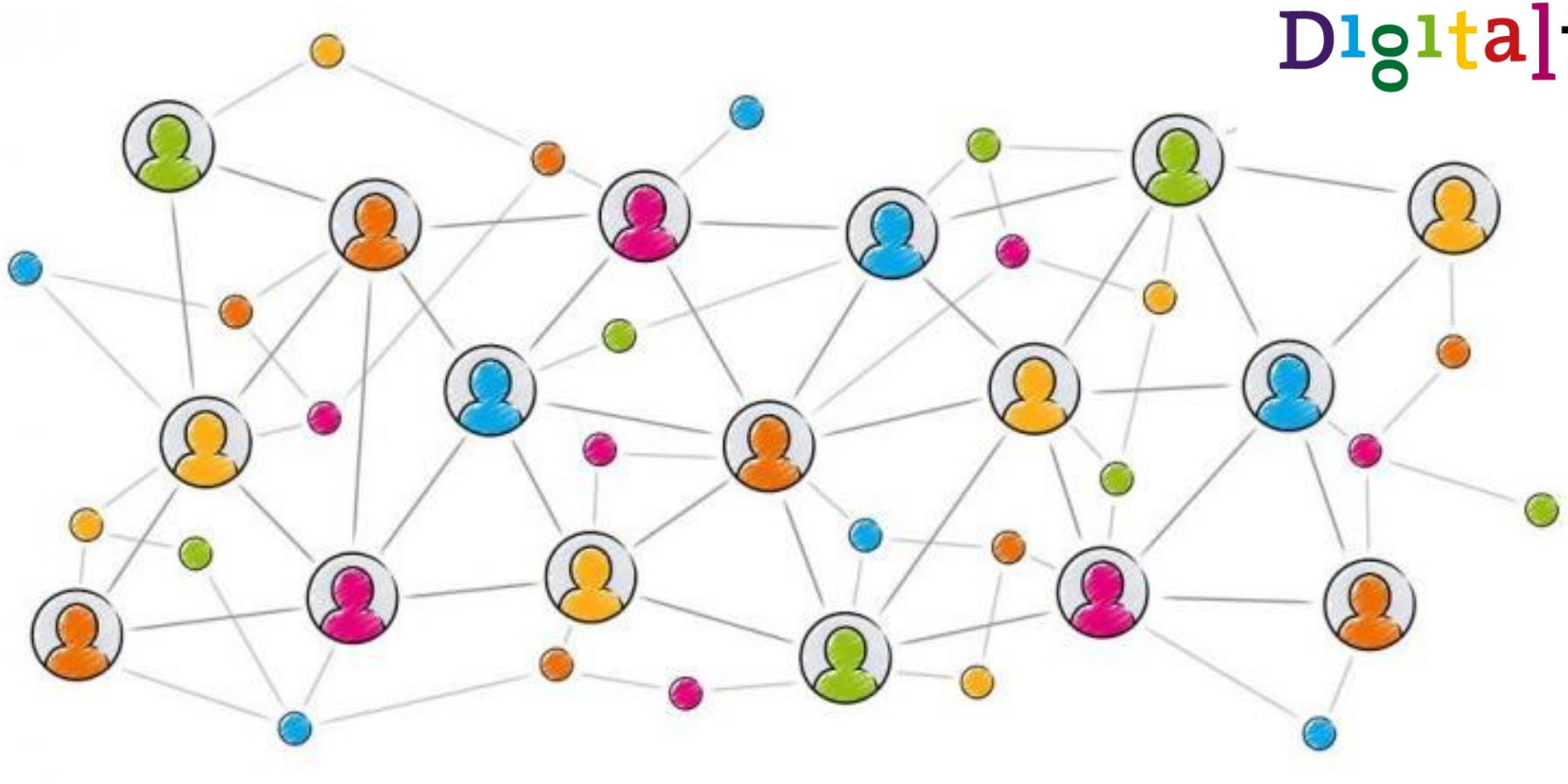


SICHERES SURFEN UND SICHERE PASSWÖRTER

Online-Seminar am 19. Juni 2020

DIE VERBRAUCHERZENTRALE

Private Altersvorsoge und Geldanlage, Ärger mit Mobilfunkanbietern, Fragen zum Online-Shoppen und Datenschutz oder Probleme mit Vertragspartnern: Die Verbraucherzentrale Niedersachsen berät individuell und anbieterunabhängig zu vielen Themen, die für Sie als Verbraucher wichtig sind. Und wir unterstützen Sie dabei, Ihre Rechte durchzusetzen!

Kurzberatungen sind zu vielen Themen **kostenlos**
– sowohl telefonisch als auch in unseren Beratungsstellen.

SO ERREICHEN SIE UNS

Vor-Ort-Beratung (nach Terminvereinbarung)
(05 11) 9 11 96-0 oder auf **unserer Website**

Video- und Telefonberatung
www.verbraucherzentrale-niedersachsen.de/fuer-sie-da

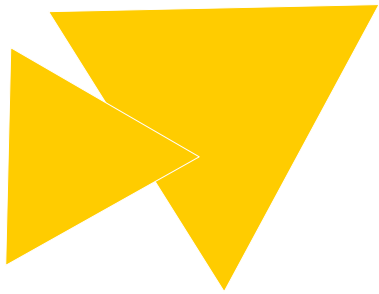
Kostenlose telefonische Kurzberatung
(05 11) 9 11 96-96 (Mo, Di, Do 10 bis 17 Uhr, Fr 10 bis 14 Uhr)

www.verbraucherzentrale-niedersachen.de

Sicheres Surfen
und
sichere Passwörter

verbraucherzentrale
Niedersachsen

– Online-Seminar –
19. Juni 2020



digitalcourage

digitalcourage e.V.

- Gemeinnütziger Verein für Datenschutz und Bürgerrechte
  - "Für eine lebenswerte Welt im digitalen Zeitalter"
  - Big Brother Awards
  - Aktionen zu aktuellen Themen

- digitalcourage Braunschweig
  - Eine von 8 regionalen Gruppen
  - https://digitalcourage.de/treffen-vor-ort/braunschweig

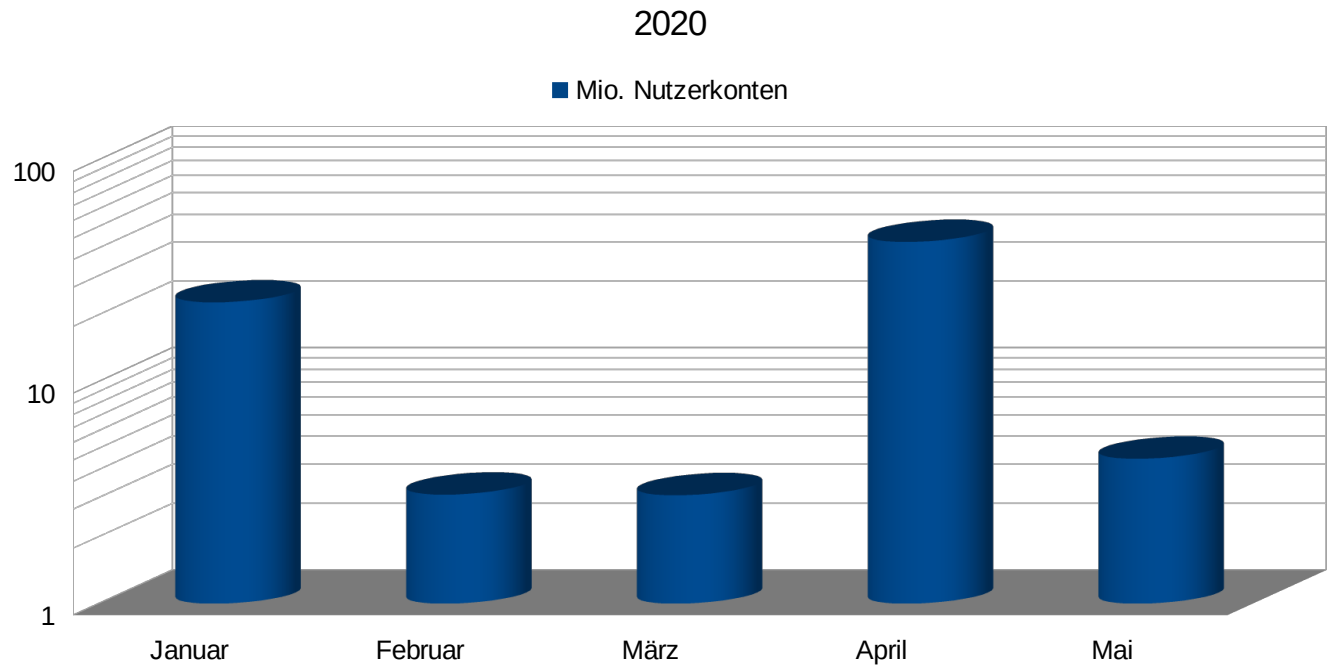
Agenda

- Sichere Passwörter
  - Was macht ein Passwort sicher?
  - Passwortmanager
  - PINs, Gesten und TANs
- Spurenarmes & anonymes Surfen
  - Werbeblocker
  - Anonymes Surfen

Agenda

- Sichere Passwörter
  - Was macht ein Passwort sicher?
  - Passwortmanager
  - PINs, Gesten und TANs
- Spurenarmes & anonymes Surfen
  - Werbeblocker
  - Anonymes Surfen

Kompromittierte Nutzerkonten



2020 bislang:

76.278.473

(Quelle: Hasso-Plattner-Institut, https://sec.hpi.de/ilc/statisics)

Sichere Passwörter

- Was macht ein Passwort stark?

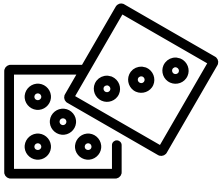
Sichere Passwörter

- Was macht ein Passwort stark?
  - Geheimhaltung

Sichere Passwörter

- Was macht ein Passwort stark?
  - Geheimhaltung

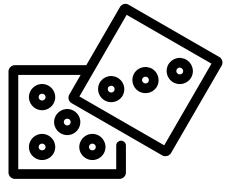
  - Zufall



Geheimhaltung

- gar nicht so einfach...
  - Abhören / Abfilmen
    - Keylogger, Überwachungskameras, Handys anderer Leute, Staatstrojaner, unverschlüsselte Emails (Google), der Herr hinter Ihnen
  - Schlechte Verstecke
    - Post-Its, Schreibtischunterseiten, Zettel in der Geldbörse, Streifen auf dem Handydisplay, dropbox, Klartextdateien
  - Social Engineering
    - Liebe Menschen: Kolleg.innen, Freunde, Familie, Vorgesetzte, vorgebliche Vorgesetzte
    - Nicht so liebe Menschen: Erpressung, Schmerzandrohung

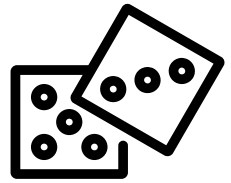
Zufall



- ebenfalls nicht so einfach...
  - Menschen sind nicht gut darin
  - https://www.expunctis.com/2019/03/07/Not-so-random.html
  - http://people.ischool.berkeley.edu/~nick/aaronson-oracle
- Helferlein:
  - ++: Cäsium-137, Quanten, Blitze
  - +: Würfel, Lavalampen[1], Münzen
  - ....
  - ?: Computer

[1]https://en.wikipedia.org/wiki/Lavarand

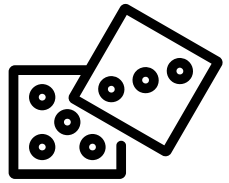
Zufall (mathematisch)



- Ziel: zu möglichst vielen Rateversuchen zwingen
  - Stärke Passphrase: Anzahl möglicher Kombinationen
- Anzahl Kombinationen
  - Größe des Zeichenvorrats (Alphabet)
  - Länge der Passphrase

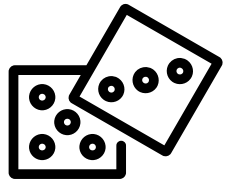
$$\textit{Größe Zeichenvorrat}^{\textit{Länge Passphrase}}$$

"123456789"



- Wie viele Rateversuche maximal?
  - Naiver Brute-Force-Ansatz
  - Länge: 9 Zeichen
  - Zeichenvorrat: 10 Ziffern
- 10^9 = 1.000.000.000 Versuche

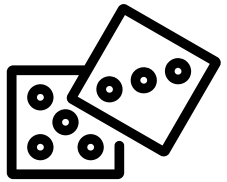
Schnellraten - Rechenzeit



- Rateversuche pro Sekunde
  - Einfacher älterer PC: 50 Millionen
  - Aktueller PC mit teurer Grafikkarte: 500 Millionen
  - Teures Mehrprozessor-System: 2-3 Milliarden
  - distributed.net-Netzwerk*: 570 Milliarden
  - NSA ?

* http://www.distributed.net/

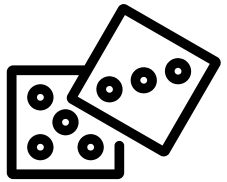
Schnellraten (naiv)



	Rateversuche/Sek.	Kombinationen	benötigte Zeit
Älterer PC	50 Mio.	1 Mrd.	20 Sek.
PC mit guter Grafikkarte	500 Mio.	1 Mrd.	2 Sek.
Starkes Multiprozessor-System	2,5 Mrd.	1 Mrd.	0,4 Sek.
distributed.net-Netzwerk	570 Mrd.	1 Mrd.	0,00175 Sek.
NSA	?	?	?

- Ratezeit für erschöpfende Suche nach "123456789"

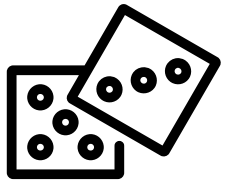
Stärke durch Länge



Passphrase	Entropie/Bits	Kombinationen	benötigte Zeit
10 Ziffern	33,22	1 Mrd.	0,0175 Sek.
12 Ziffern	39,86	100 Mrd.	1,75 Sek.
15 Ziffern	49,83	100 Billionen	29:14 Min.
20 Ziffern	66,44	10^{20}	> 5 Jahre
30 Ziffern	99,65	10^{30}	> 55 Mrd. Jahre

- Ratezeit für erschöpfende Suche nach
  - **zufälligen** Ziffernkombinationen (keine Buchstaben etc.)
  - über distributed.net
- Empfehlung: längere Passphrase, länger Freude

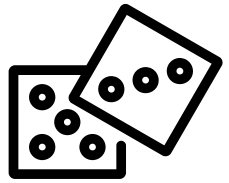
Stärke durch mehr Zeichen



Passphrase	Entropie / Bits	Kombinationen	benötigte Zeit
12 Ziffern	39,86	100 Mrd.	1,75 Sek.
12 Ziffern/[a-z]	62,04	36^{12}	> 96 Tage
12 Ziffern/[a-z]/[A-Z]	71,45	62^{12}	> 179 Jahre
12 [0-9]/[a-z]/[A-Z]/!“§...	76,29	82^{12}	> 5.141 Jahre
13 Ziffern/[a-z]/[A-Z]	77,40	62^{13}	> 11.127 Jahre

- Ratezeit für erschöpfende Suche nach
  - **zufälligen** Kombinationen bestimmter Zeichenvorräte
  - der Länge 12 (resp. 13)
  - über distributed.net
- Empfehlung: Buchstaben (groß, klein) + Ziffern

Starke Passphrasen

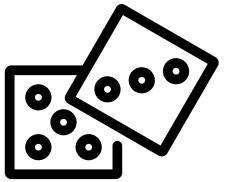


- durch
  - viele Zeichen (Länge, z.B. 12)
  - aus einem großen Alphabet (Zeichenvorrat: Ziffern, Groß-/Kleinbuchstaben)
  - zufällig ausgewählt (nicht: selbst ausgedacht)

- Beispiele*:
  - 9dhI9GXophxT5 UAVM3nKAEclSKDMaWhT2En9

* generiert mit: `pwgen -s 13` und `pwgen -s 23`

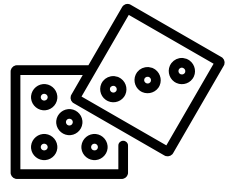
Passwörter Top 10



Passwort		Häufigkeit (in ‰)
1	**123456**	8,10
2	**123456789**	3,89
3	**password**	1,89
4	**qwerty**	1,85
5	**12345**	1,38
6	**12345678**	1,17
7	**111111**	1,17
8	**qwerty123**	1,02
9	**1q2w3e**	0,97
10	**123123**	0,85
,,,	**...**	…

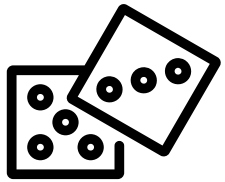
(Quelle: Hasso-Plattner-Institut, https://sec.hpi.de/ilc/statisics)

"123456789"



- Besserer Angriff: Häufigste 1000 Passwörter
- "Wörterbuchsuche"
- Wie viele Rateversuche maximal?
  - Länge: 1 Zeichen (jedes geratene Passwort ist ein Zeichen)
  - Zeichenvorrat: 1000 Wörter
- 1.000 Rateversuche

Schnellerraten (Top 1.000)

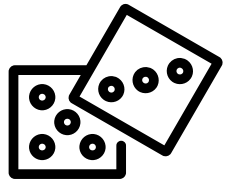


	Rateversuche/Sek.	Kombinationen	benötigte Zeit
Älterer PC	50 Mio.	1.000	0,00002 Sek.
PC mit guter Grafikkarte	500 Mio.	1.000	kaum messbar
Starkes Multiprozessor-System	2,5 Mrd.	1.000	kaum messbar
distributed.net-Netzwerk	570 Mrd.	1.000	kaum messbar
NSA	?	?	nicht messbar

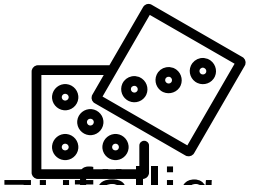
- Ratezeit für Wörterbuch-Suche nach "123456789"

Stärke durch Länge

- Übliche Methode: mehr Zeichen
- Tabelle: längere Zeichen, längeres Brute-Force
- ABER: Zufälligkeit ist wichtig



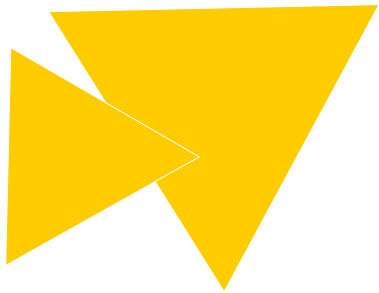
Stärke durch Listen statt Sonderzeichen



- Übliche Methode: mehr Zeichen
- Sätze mit Wortanfängen (sieht nur für Menschen zufällig aus)
- Sind diese wirklich zufällig, kann sie sich keiner merken
- Stattdessen: Diceware

Agenda

- Sichere Passwörter
  - Was macht ein Passwort sicher?
  - Passwortmanager
  - PINs, Gesten und TANs
- Spurenarmes & anonymes Surfen
  - Werbeblocker
  - Anonymes Surfen



Passwortmanager

- Speichern schwer zu merkender Passwörter
- Hilft Wiederverwendung von Passphrasen zu vermeiden
- Erzeugen starke Passwörter
- Brauchen ein Hauptkennwort
- Qualitätsmerkmale
  - OpenSource
  - Keine Online-Speicherung

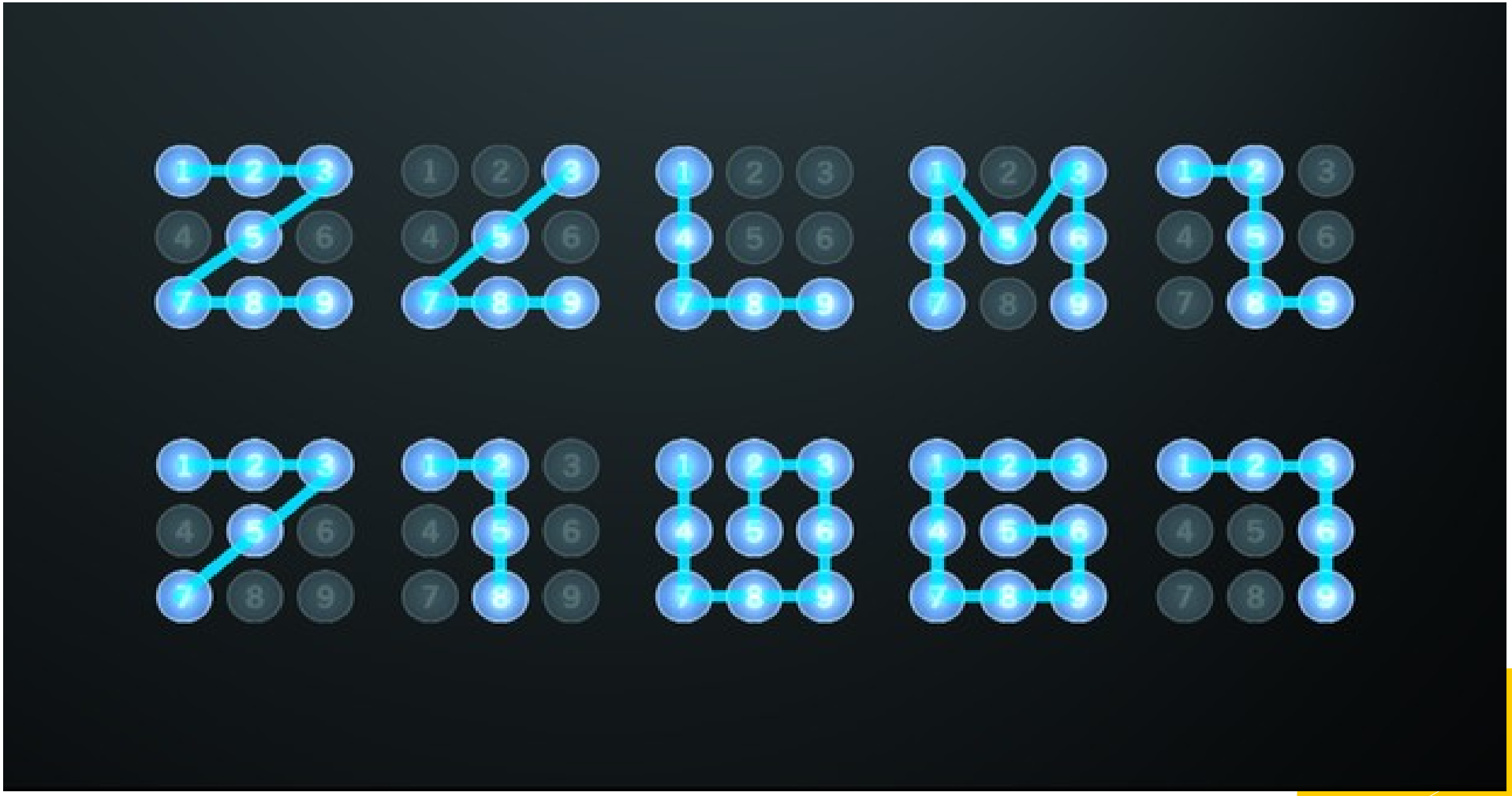
KeePassXC

- Unsere Empfehlung für den Alltagsgebrauch
  - https://keepassxc.org
  - Für Windows, Mac und Linux
  - Mit Browser-Integration
  - Quelloffen
  - Kostenlos

Agenda

- Sichere Passwörter
  - Was macht ein Passwort sicher?
  - Passwortmanager
  - PINs, Gesten und TANs
- Spurenarmes & anonymes Surfen
  - Werbeblocker
  - Anonymes Surfen

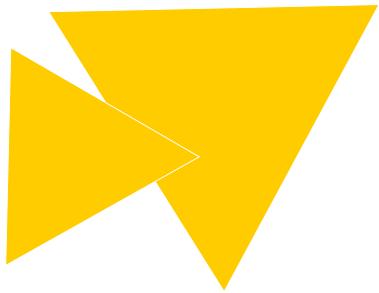
Typische Wischgesten



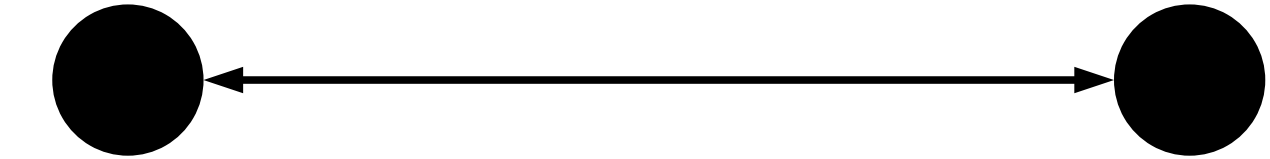
Agenda

- Sichere Passwörter
  - Was macht ein Passwort sicher?
  - Passwortmanager
  - PINs, Gesten und TANs

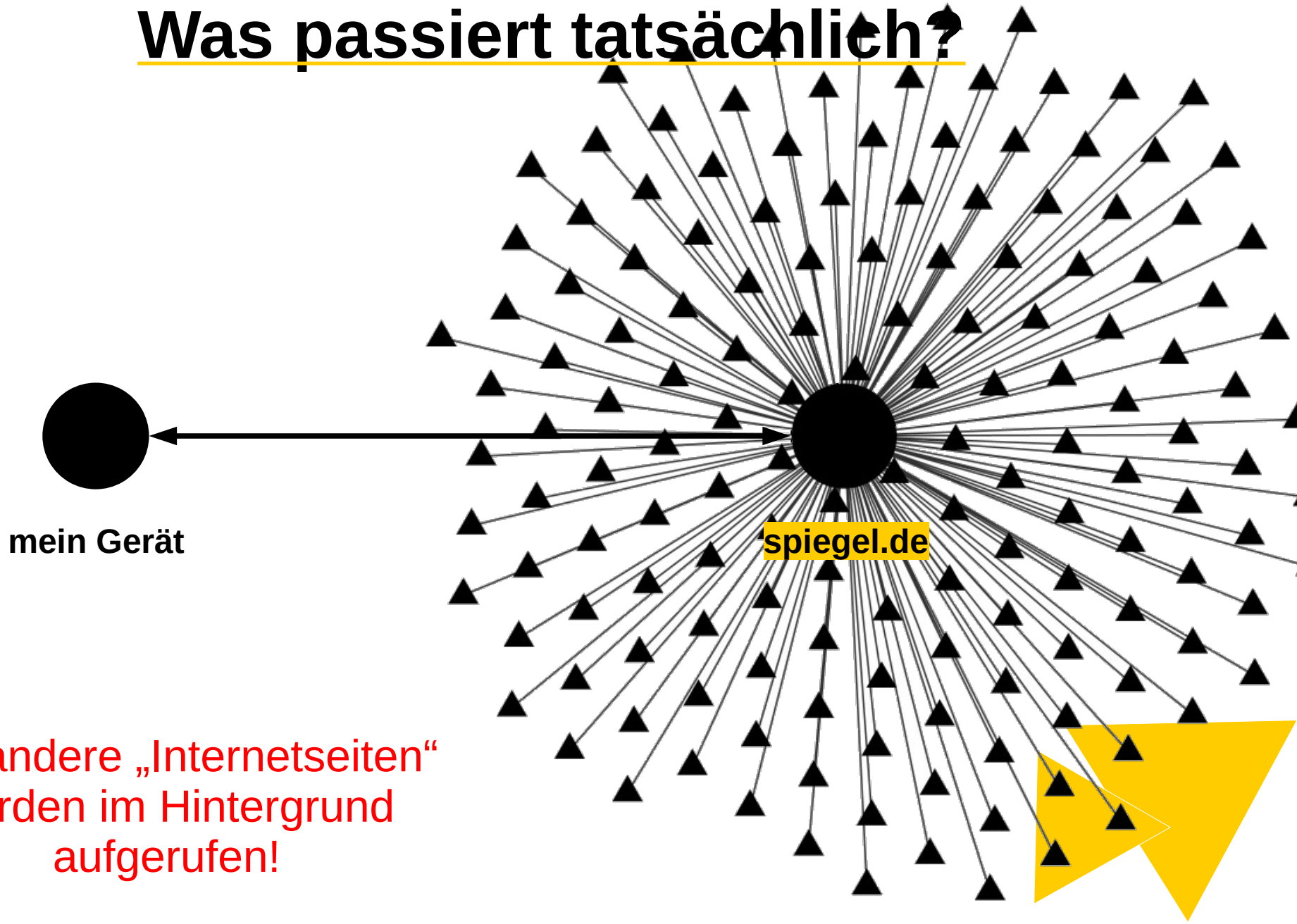
- Spurenarmes & anonymes Surfen
  - Werbeblocker
  - Anonymes Surfen



Wie funktioniert das Internet?



Was passiert tatsächlich?

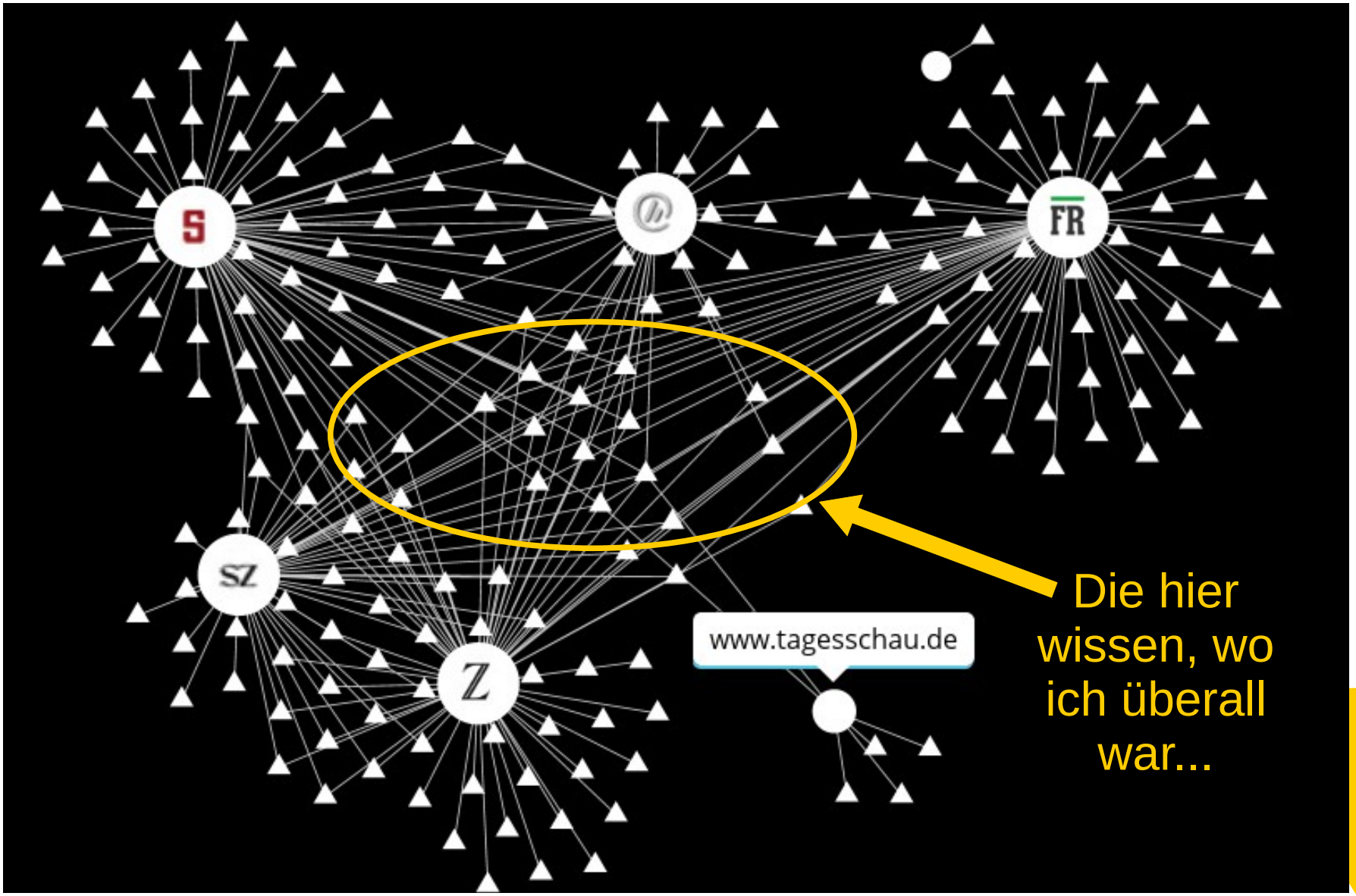


152 andere „Internetseiten“ werden im Hintergrund aufgerufen!

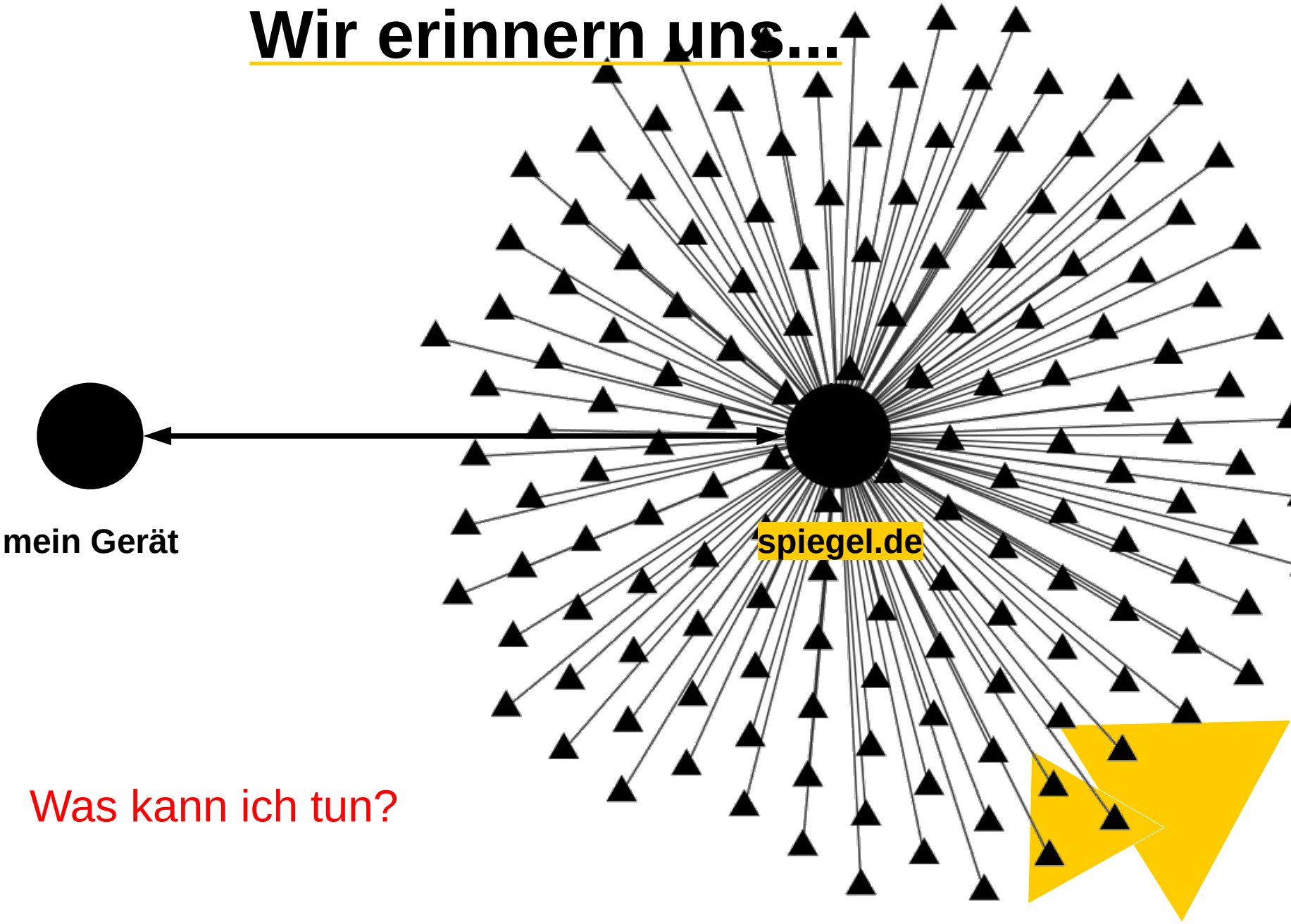
Wie schlimm ist es?

- ioam.de, **google**tagmanager.com, omny.fm, cloudfront.net, mxcdn.net, optimizely.com, soundcloud.com, demdex.net, adalliance.io, emsservice.de, emetriq.de, criteo.net, s79.research.de.com, meetrics.net, omtrdc.net, criteo.com, **doubleclick**.net, hotjar.com, **google**-analytics.com, **google**tagservices.com, yieldlab.net, everesttech.net, xplosion.de, **google**apis.com, ampcid.**google**.com, adservice.**google**.de, ampcid.**google**.de, srv-2019-06-13-05.pixel.parsely.com, theadex.com, newrelic.com, adrtx.net, nr-data.net, ligatus.com, ligadx.com, summerhamster.com, zemanta.com, scorecardresearch.com, outbrain.com, **google**syndication.com, csi.**gstatic**.com, ... (ohne Subdomains!)

Problem: Alles ist miteinander vernetzt!

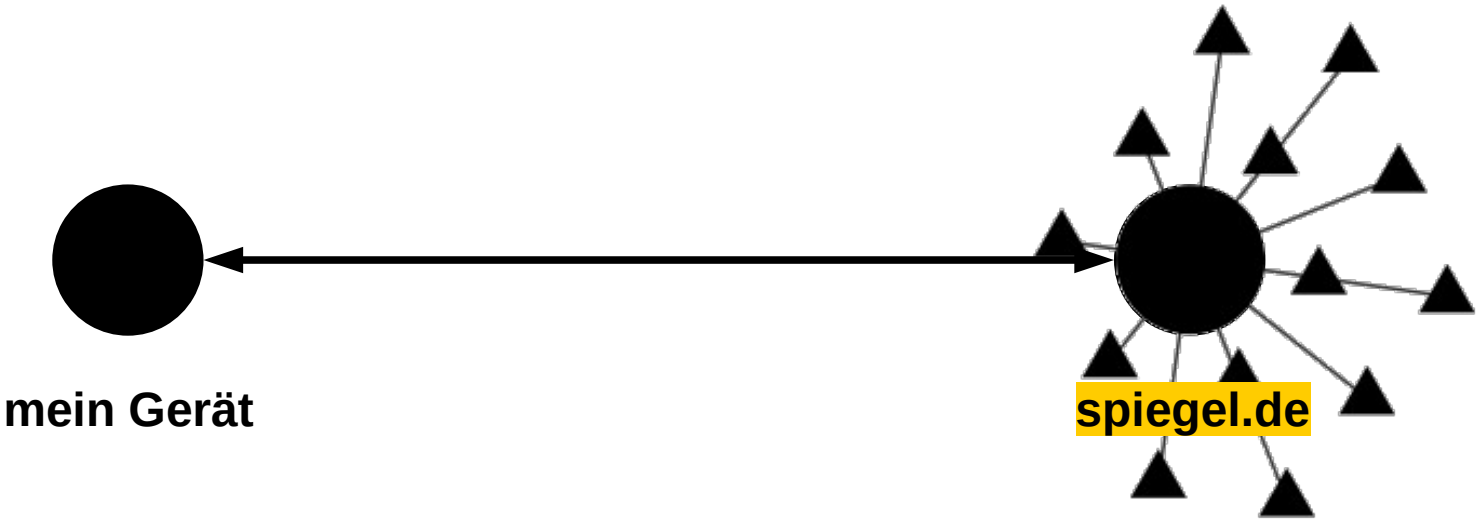


Wir erinnern uns...



Was kann ich tun?

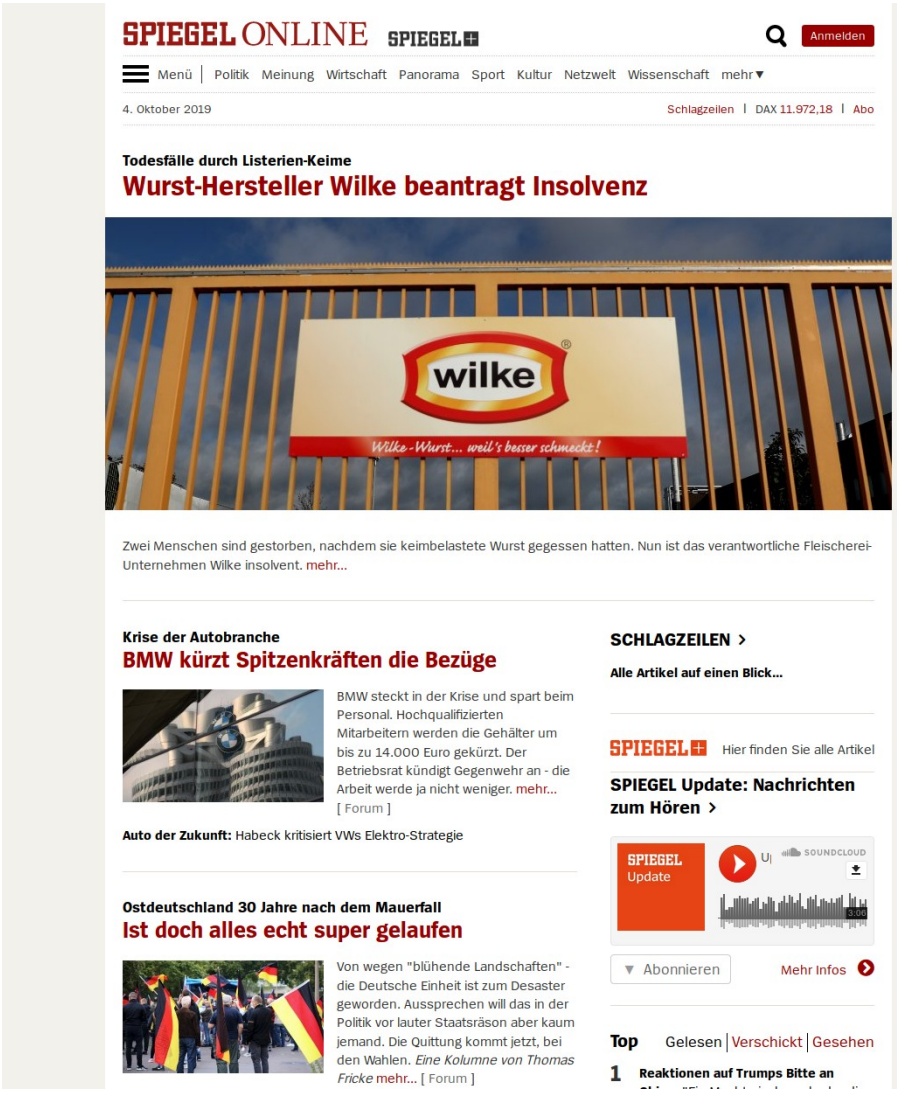
Wie sollte es sein?



Mit Werbeblocker:
nur noch 13 „externe“ Seiten!

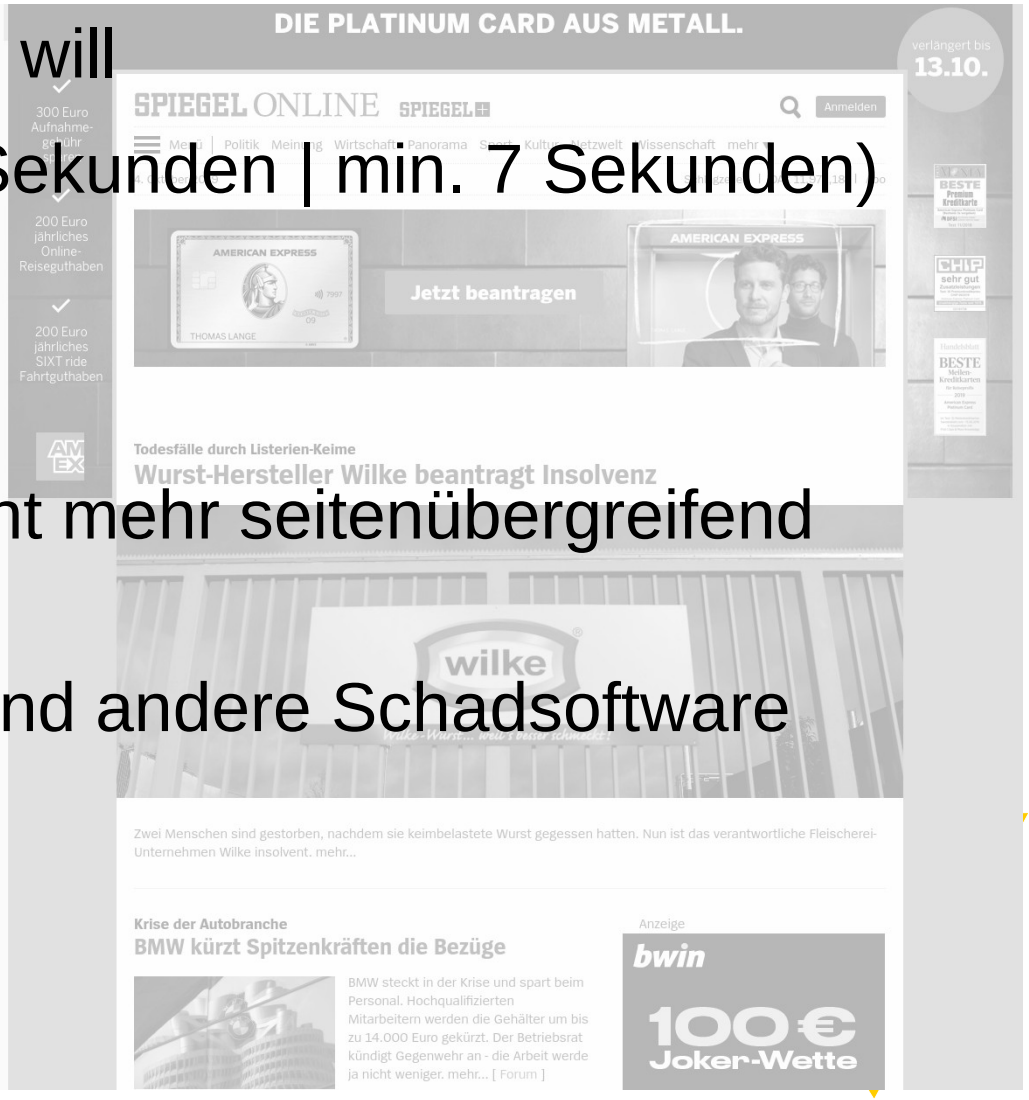
- mindestens 139 Drittseiten waren also „böse“

Vergleich
mit & ohne Werbeblocker



Vergleich
mit & ohne Werbeblocker

- Nur noch das, was ich sehen will
- Seite lädt schneller (max. 2 Sekunden | min. 7 Sekunden)
- Spart Datenvolumen
- Umweltschutz
- Werbenetzwerke können nicht mehr seitenübergreifend verfolgen (Tracking)
- Geringeres Risiko für Viren und andere Schadsoftware
- ...



Google weiß alles über dich!

- Suchanfragen nach Anfahrtswegen, Geschenk-ideen, Krankheiten, uvm.
- Profilbildung findet auch ohne Anmeldung statt
- Abrufbar über adssettings.google.com (Anmeldung notwendig)

Google sollte nicht alles wissen!

- Zahlreiche Alternativen verfügbar
- Eine davon: **MetaGer.de**
  - Wird vom SUMA-EV aus Hannover betrieben
  - Eigener Suchindex & Ergebnisse verschiedener Suchmaschinen
  - Freie Software
  - Arbeitet datensparsam
  - Kann als neue Standard-Suchmaschine im Browser eingerichtet werden
- Noch mehr Alternativen: StartPage.com, DuckDuckGo.com, Qwant.com

Praxisteil: Installation uBlock

- Voraussetzung: Computer, Tablet oder Smartphone mit Firefox
  - Ausnahme: iPhone
    Apples Firmenpolitik lässt Firefox mit Erweiterungen (Addons) nicht zu – und damit auch keine Werbeblocker
- Installation
  - Firefox: Menü ► Add-ons ► nach "ublock" suchen
  - "uBlock Origin" ► "+ Zu Firefox hinzufügen"
- Verwendung
  - Einfach wie bisher Surfen
  - Optional: weitere Filterlisten hinzuzufügen

Praxisteil: MetaGer als Standard-Suchmaschine

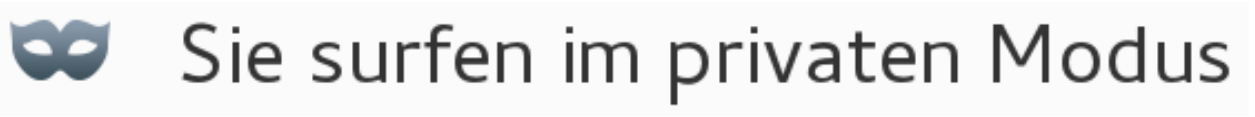
- Firefox (Computer)
  - MetaGer.de öffnen
  - Unter dem Suchfenster "MetaGer-Plugin hinzufügen" anklicken
- Firefox (Android)
  - MetaGer.de öffnen
  - lange auf Suchfeld tippen
    ► "als Suchmaschine hinzufügen"
  - Einstellungen ► Suche
    ► MetaGer als Standard festlegen

Ausblick

- Werbeblocker und alternative Suchmaschinen
  - Geringer Aufwand – großer Nutzen!
  - keine 100 % Lösung im Bezug auf Datenschutz
- Eigentlich müsste man noch viel mehr machen...
  aber: Benutzerfreundlichkeit sinkt leider spürbar
  - Cookies regelmäßig löschen / von Drittanbietern blockieren
  - JavaScript nur bei Bedarf aktivieren / Addon NoScript verwenden
  - Privaten Modus öfter verwenden (aber: nur lokale Spurenfreiheit!)

Weitere Firefox-Funktionen

- **Privater Modus**
- Keine Speicherung von Daten besuchter Webseiten **auf dem eigenen** Computer (insb. keine Chronik, keine URL-Vervollständigung, Cookies, etc.)
- Auf dem lokalen System verbleiben keine Spuren
- *Keine Anonymität* gegenüber dem Netz



Firefox-Add-ons

- Tracker und Werbung blocken: **uBlock origin**
- Aktive Inhalte blocken: **NoScript**
- Scripts Globally Allowed (vom Hersteller nicht empfohlen)
- Webseiten immer verschlüsseln: **HTTPS Everywhere**
- Cookies automatisch löschen: **Cookie AutoDelete**
- Adobe-Flash am besten entfernen oder deaktivieren!

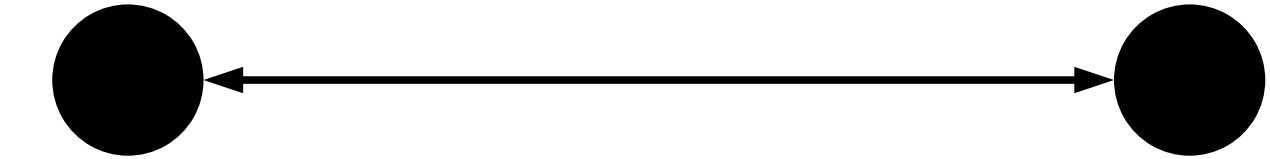
- Etwas komplizierter und aufwendiger:
- Alle Skripte blocken: **NoScript**
- Alle Drittanbieteranfragen blocken: **uMatrix**

Anonym Surfen mit Tor (The Onion Router)

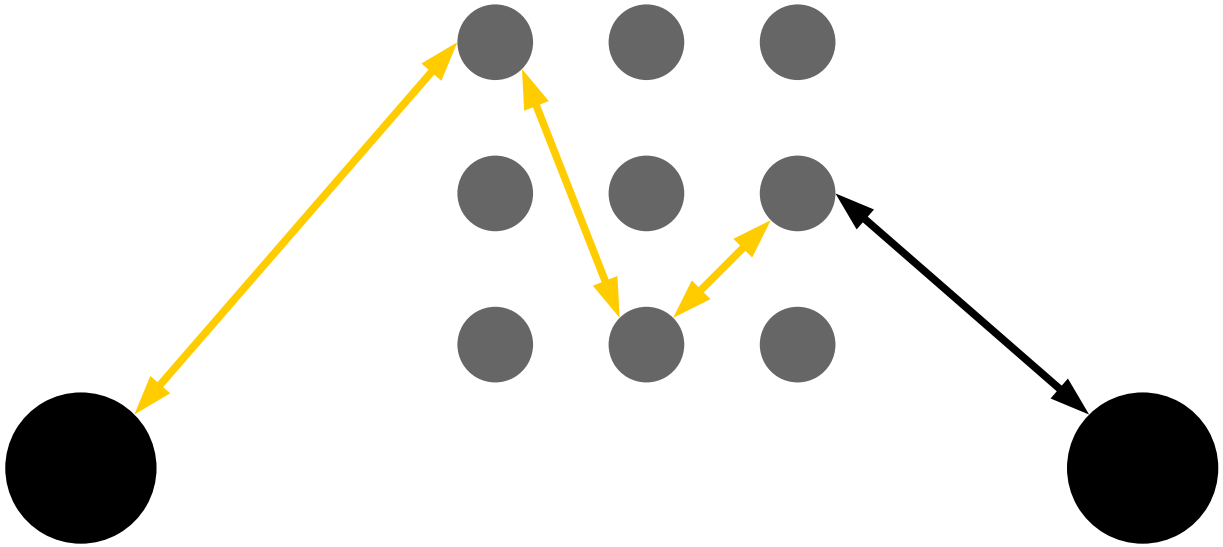
- Normales Surfen
  - Beide Seiten sehen ihr Gegenüber direkt
- Surfen mit Tor
  - Sämtlicher Datenverkehr geht über das Tor-Netzwerk
  - Nur der Einstiegsknoten des Tor-Netzwerks "kennt" mich
  - Die angesurfte Internetseite hat keine Möglichkeit, meine Herkunft (IP-Adresse) herauszufinden

- Vorteile
  - Quelloffen, freie Software
  - Anonymes Surfen
- Nachteile
  - Login bei personalisierten Seiten nicht sinnvoll
  - Langsamer

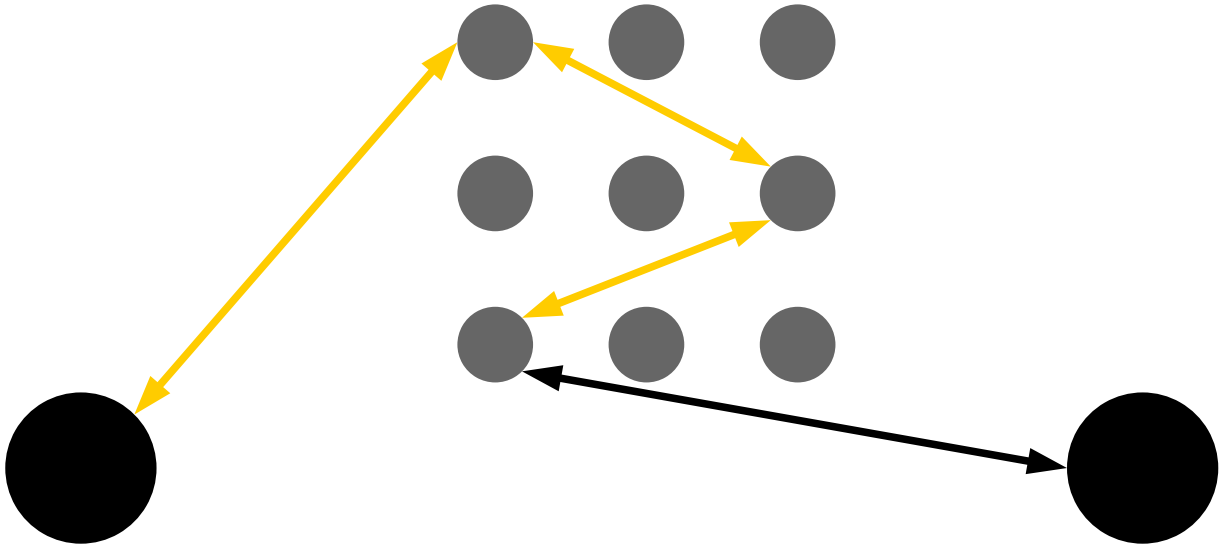
Wie funktioniert das Internet?



Wie funktioniert ~~das Internet~~ Tor?



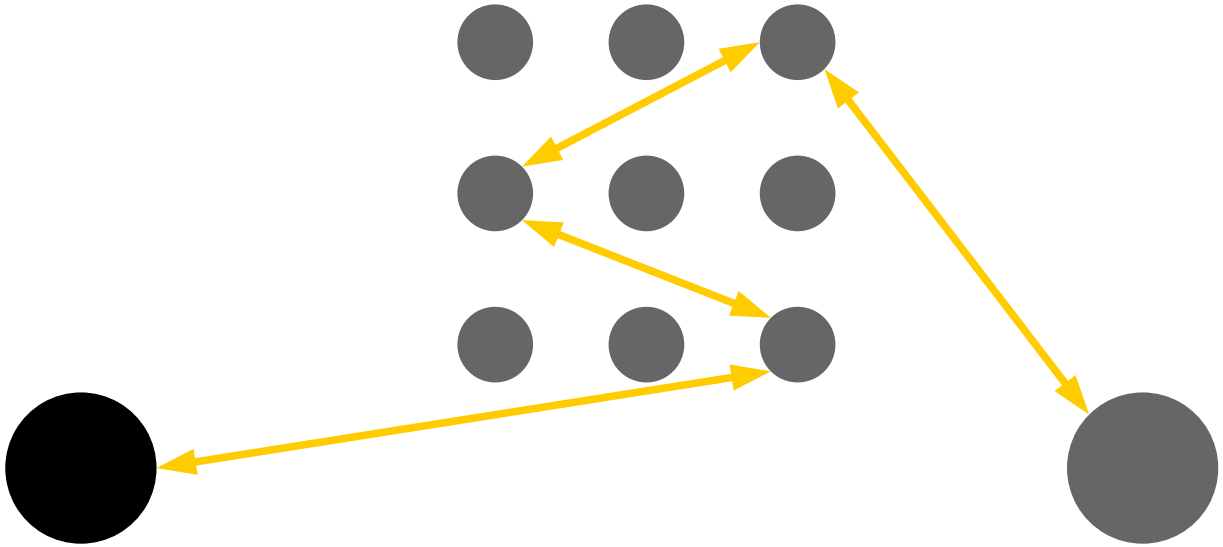
Wie funktioniert ~~das Internet~~ Tor?



mein Gerät

bnd.bund.de

Exkurs: Darknet



mein Gerät

pwoah7foa6au2pul.onion

- Mögliche Darknet-Seiten / Dienste:
  - Marktplätze
  - E-Mail-Anbieter
  - Filesharing
  - Foren
  - ...

Wie nutze ich Tor?

- Tor-Browser installieren
  - Modifizierter Firefox aus mehreren Addons (NoScript, HTTPS Everywhere, Torbutton und TorLauncher)
  - https://www.torproject.org/download/
- Hinweis zur Zielgruppe:
  - Nutzung ist vor allem bei exponierten Personen sinnvoll (Investigativjournalisten, innerhalb bestimmter Länder mit zensierten Internet oder anderweitiger Unterdrückung, ...)
  - Für den Normalanwender ist oftmals die Verwendung von Werbeblockern und ggf. weiteren Addons ausreichend

Vielen Dank fürs Mitmachen!

(Bild: CC-BY-2.0: EFF)

VIELEN DANK!

Gefördert durch:

Bundesministerium
der Justiz und
für Verbraucherschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

Impressum

Verbraucherzentrale
Niedersachsen e.V.

Herrenstraße 14
30159 Hannover

info@vzniedersachsen.de
www.verbraucherzentrale-niedersachsen.de