Selbstschutz-Konzepte im Wandel: Internetnutzung zwischen Krypto-Trojaner und Tracking-Krieg

Christian Krause, ULD

Sommerakademie 2017

Herausforderung „Informationelle Nichtbestimmung“

18.09.2017

Selbstschutz?

- IT ist traditionell dem Baumarkt näher als dem Supermarkt.
- Endgeräte-Sicherheit war lange eher Extra denn Standard:
- Entweder, weil bei der Konzeption Sicherheit nicht mitgedacht worden war (E-Mail, fehlendes Rechtekonzept in Windows),
- oder, weil Sicherheit zugunsten des Komforts zurücktreten musste (anfangs standardmäßig deaktivierte WLAN-Verschlüsselung)
- (manchmal war und ist Sicherheit auch nur lausig implementiert...)
- Und außerdem ist keine Software fehlerfrei.

Viren, Trojaner, Erpresser

- Windows-Nutzer waren bis Windows Vista (2007) als Administratoren unterwegs ...

- *Kindly check the attached LOVELETTER coming from me*
  (I Love You, vbs-Script, 4. Mai 2000)
- Einfallstor damals wie heute: Dateien und nervöse Zeigefinger:
- Locky (2016) nutzte ebenfalls infizierte Office-Dokumente: *"Bitte erlauben Sie die Ausführung von Makros"...*

- Die zwischenzeitlich verbesserte Rechtestruktur von Windows hilft wenig, da Dokumente und Fotos naturgemäß im Userspace liegen

Virenscanner

- Das Problem:
  - Eingehende Daten (früher Disketten, heute Downloads) können Schadcode enthalten
- Lösung:
  - Alles wird gegen Signaturen und/oder eine Heuristik gescannt.
- Das Dumme:
  - Signaturen prinzipbedingt nur zeitversetzt verfügbar
  - Schwellwert-Dilemma bei Heuristiken
  - Effektiver Scan nur mit weitreichenden Zugriffsbefugnissen und erheblichem Eingriff ins System möglich
  - Erfolgreicher Scan ist sichtbar, fehlgeschlagene Scans können nicht bemerkt werden

→ Was bedeutet also die Erkenntnis, dass der eigene Virenscanner gerade nichts meldet? Ist mein PC nach dem Entfernen eines Schädlings *wirklich* sauber?

Personal Firewalls

- Das Problem:
  - Anwendungen "telefonieren nach Hause"
- Die Idee:
  - Ausgehenden Datenverkehr nach Ursprungsanwendung filtern
- Das Dumme:
  - Wie entscheidet man denn zwischen legitimem und illegitimem Netzwerkverkehr?!?
- Und dann war da noch: Der Auto-Clicker

Patches

- Das Problem:
  - Komplexe Software enthält Fehler und Sicherheitslücken.
  - Immer.
  - Nutzer vergessen gern das Aktualisieren von Software.
- Die Lösung:
  - Updates und Patches werden vom Entwickler bereitgestellt, idealerweise von der Software automatisiert eingespielt.
- Das Dumme:
  - Jetzt entscheidet plötzlich der Softwareanbieter, was auf meiner IT läuft.
  - Oder (bei Profisoftware wie *PC-Wahl*) irgendjemand.
  - Geheimdienste mögen keine Patches und kaufen 0-Day-Exploits.

Was geschah am…

Am 1. Januar 1974 wurde die „Gurtpflicht“ für Neuwagen eingeführt

Die Einbaupflicht in Neuwagen ab 1. Januar 1974 wurde mit der Einführung einer neuen europäischen Typprüfung ECE und nach amerikanischen Vorbild mit der vorgeschriebenen Gurtöffnung durch Druck auf eine rote Taste kombiniert.

Die Einführung einer Gurtpflicht stieß in vielen Ländern auf heftigen Widerstand. Die nicht sanktionsbewehrte Gurtpflicht auf Vordersitzen in der Bundesrepublik im Jahre 1976 traf auf den großen Widerstand vieler Autofahrer.

Mond (zunehmend):
Aufgang: 11:11
Höchststand: 18:05
Untergang: 00:01
Aktuelle Entfernung: 387322km

Sonne:
Aufgang: 08:40
Höchststand: 12:22
Untergang: 16:05

Weitere Ereignisse:
Neujahr

DI
01
Jan
1974

The Times They Are a-Changin'

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Homepage ab Oktober 2014
Homepage Archiv
Wir über uns

Themen

Systemdatenschutz
Audit / Gütesiegel
Projekte
Informationsfreiheit

Gesetze
Presse
Veröffentlichungen
Mediathek
Vorträge

Infos für Bürger
Infos für Behörden
Infos für die Wirtschaft
FAQs

13. Juni 2003

Automatische Software-Installation durch Online-Updates unzulässig

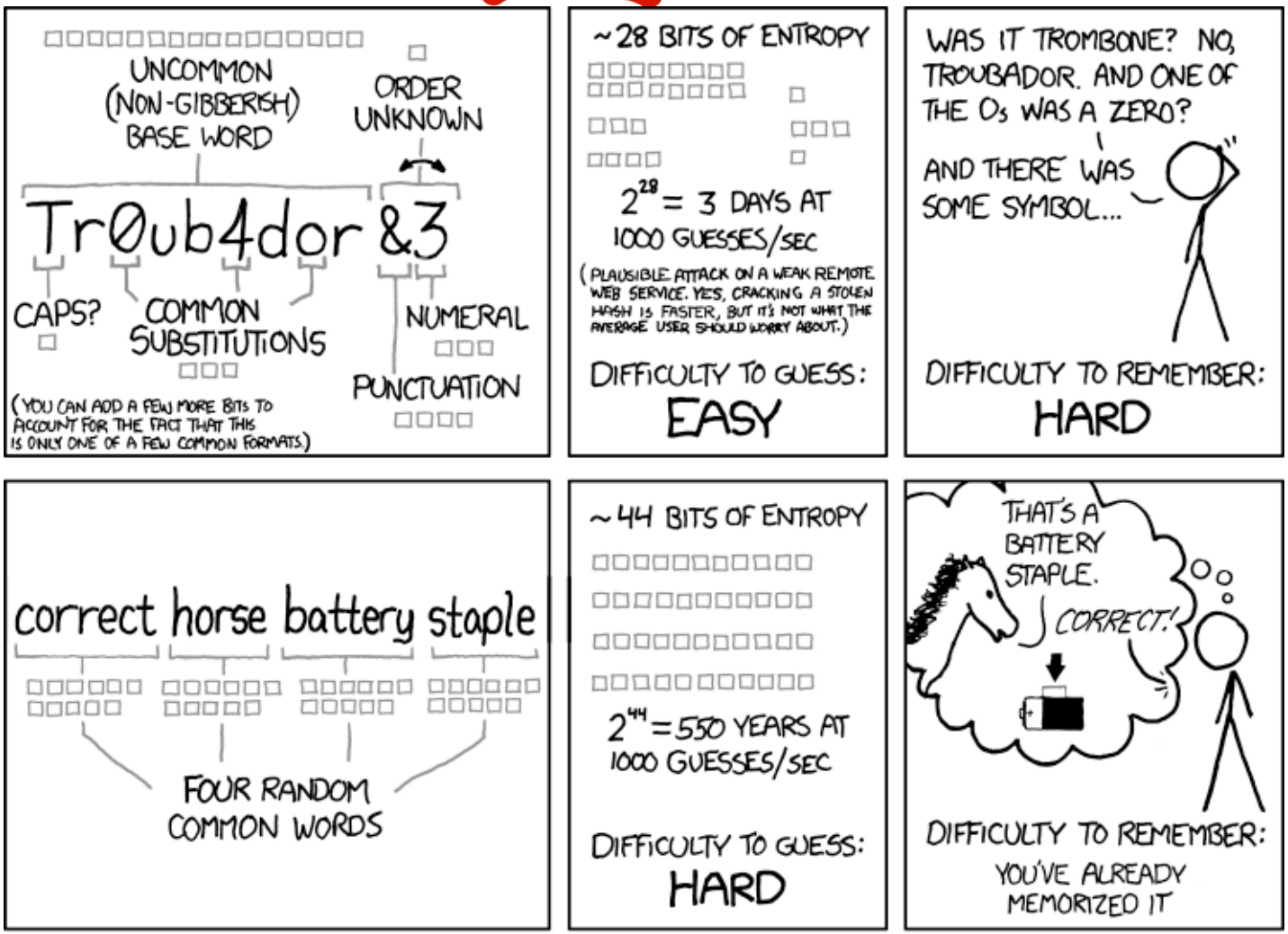
Ein vollautomatisches Betriebssystem-Update von Windows 2000/XP-Systemen über eine Internetverbindung ohne Eingriffsmöglichkeit der Administratoren verstößt gegen das LDSG.

Die Betriebssysteme Windows 2000 Servicepack 3 sowie Windows 2003 und Windows XP stellen eine neue Funktion zur Verfügung, die Betriebssystem-Updates und Patches von der Microsoft-Webseite herunterladen und automatisiert installieren kann.

Nach den in Schleswig-Holstein geltenden datenschutzrechtlichen Bestimmungen ist ein solches automatisiertes Update für IT-Systeme, mit denen personenbezogenen Daten verarbeitet werden, unzulässig: Ändernde Zugriffe an automatisierten Verfahren (und damit auch den Betriebssystemen) dürfen nur dazu ausdrücklich berechtigten Personen möglich sein; sie müssen getestet und protokolliert werden.

https://security.googleblog.com/2015/07/

~~Die~~ alte Passwortregeln



https://xkcd.com/936/

Passworte gehören abgeschafft?

- Alternative Biometrie?

DEUTSCHLAND ANTI-TERROR-KAMPF

Gesichtserkennung – die nächste Stufe der Überwachung

Von Ricarda Breyton | Veröffentlicht am 01.08.2017 | Lesedauer: 4 Minuten

Seit Wochen gehen 300 Berliner an einem Bahnhof ein und aus - im vollen Bewusstsein, dass sie unter besonderer Beobachtung stehen. Noch ist es ein Experiment. Doch Datenschützer sind in Sorge.

AUTOPLAY an

Quelle: N24/ Dagmar Boehning

Am Berliner Bahnhof Südkreuz setzt die Polizei erstmals Gesichtserkennungs-Software zur Kriminalitätsbekämpfung ein. Kritiker fürchten den Überwachungsstaat. Doch viele Passanten setzen ganz andere Prioritäten.

Sinneswandel auch beim Thema Verschlüsselung

- PGP erschien 1991 und hat bis heute keine Relevanz im Alltag.
- WhatsApp führt Ende-zu-Ende-Verschlüsselung 2016 für eine Milliarde Nutzer quasi "über Nacht" ein.
- Der Messenger DeltaCrypt setzt auf E-Mail-Infrastruktur: Mittels Autocrypt wird PGP erstmals völlig transparent implementiert – Nutzbarkeit auf Kosten sehr hoher Sicherheit. (Autocrypt für Thunderbird ist in Planung)

"Mobile Computing": Die Miniaturisierung von allem.

- Mini-Darstellung
- Mini-Eingabemöglichkeit
- Mini-Ressourcen
- Mini-Kontrolle
- Mini-Auswahl

- Mini-Risiko ...?

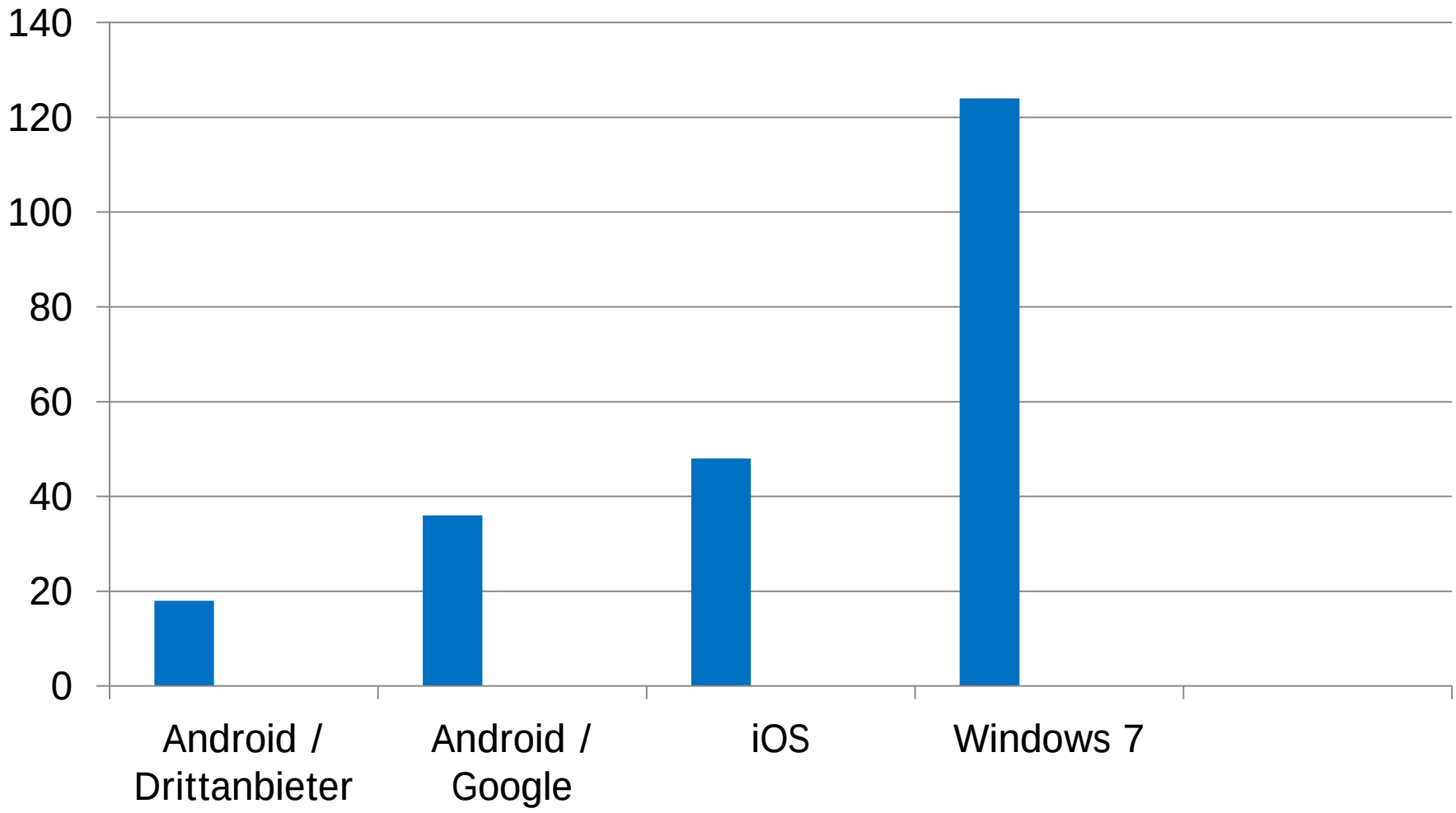
Vorteile(?) mobiler Betriebssysteme

- Anwendungs-Sandboxing
- Berechtigungsstruktur für Anwendungen
- Nutzer ohne Root-Rechte
- Weitgehend kontrolliertes Anwendungsangebot
- Vollautomatisierte Updates

Virenscanner auf Smartphones?

- Eine Smartphone-App kann kaum mehr als ihre eigene Sandbox scannen

Wie viele Monate gibt's Updates?



Nochmal in Worten:

- Hersteller von Android-Geräten versprechen 18 Monate (in der Praxis ist es manchmal mehr, oft jedoch nicht)
- Google unterstützt seine Nexus-Geräte bis KitKat 4.4.4 derzeit für über 36 Monate.
- Apple: Ältestes Gerät, das das neueste iOS bekommt: iPad Air (2013): derzeit über 48 Monate
- Zum Vergleich: Sicherheits-Patches für Windows 7 gibt es bis zum 14. Januar 2020: 124 Monate ...

Personal Firewalls (outbound) auf Mobilgeräten

- Weniger sinnlos als auf dem Desktop:
  - Auto-Clicker schwerer zu realisieren
  - Fremde Prozesse schwerer nutzbar
  - Deutlich größere Tracking-Aktivität der Anbieter
- Nachteile der eingeschränkten Mobilsysteme sind hier hilfreich

Werbung:
Das sind ja gleich zwei Gefahren auf einmal!

- Aushöhlung der informationellen Selbstbestimmung
- Gefährdung der eigenen IT

Das ist doch nur Werbung!

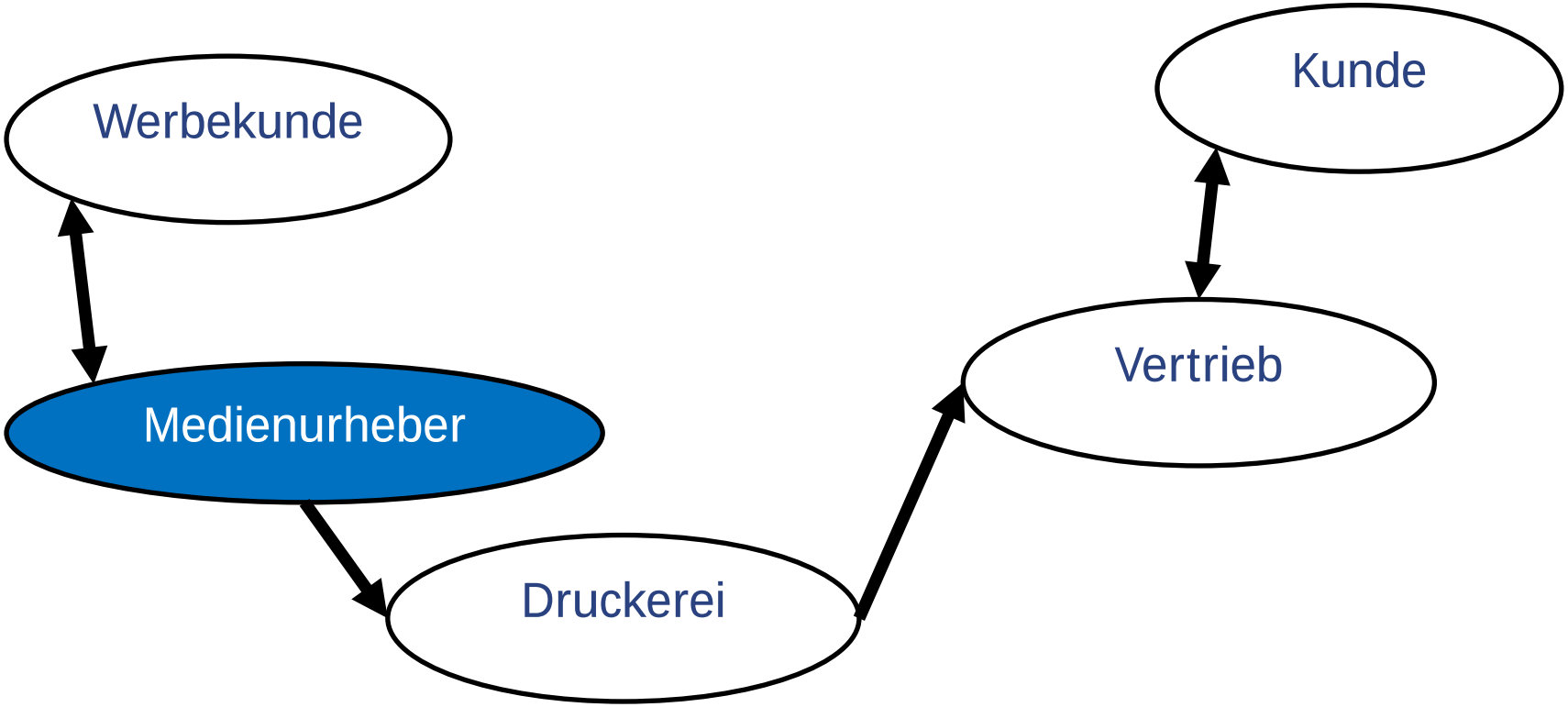
- Individuell zugeschnittene Inhalte erfordern eindeutige Erkennung des Nutzers:
  - Cookies
  - Font Fingerprinting
    (Individuelle Zusammenstellung installierter Schriftarten)
  - Canvas Fingerprinting
    (Individuelle Abweichungen der Bildschirmanzeige)
  - AudioContext Fingerprinting
    (Individuelle Abweichungen im Audio-Signalprozessor)
  - WebRTC Local IP Discovery
    (Individuelle Liste lokal erreichbarer IP-Adressen)

Massive Verkettung

- Durch Technologien wie Browser-Fingerprinting werden Online-Aktivitäten langfristig verkettbar.
- Im Unterschied zu aktiv geteilten Informationen im Web bleiben die gesammelten Tracking-Daten für den Nutzer ungewiss.
- Ohne Einblick in aggregierte Daten ist keine Korrektur oder gar Löschung dieser – womöglich falschen – Informationen möglich.
- Das Recht auf informationelle Selbstbestimmung wird auch hier zunehmend ausgehöhlt.

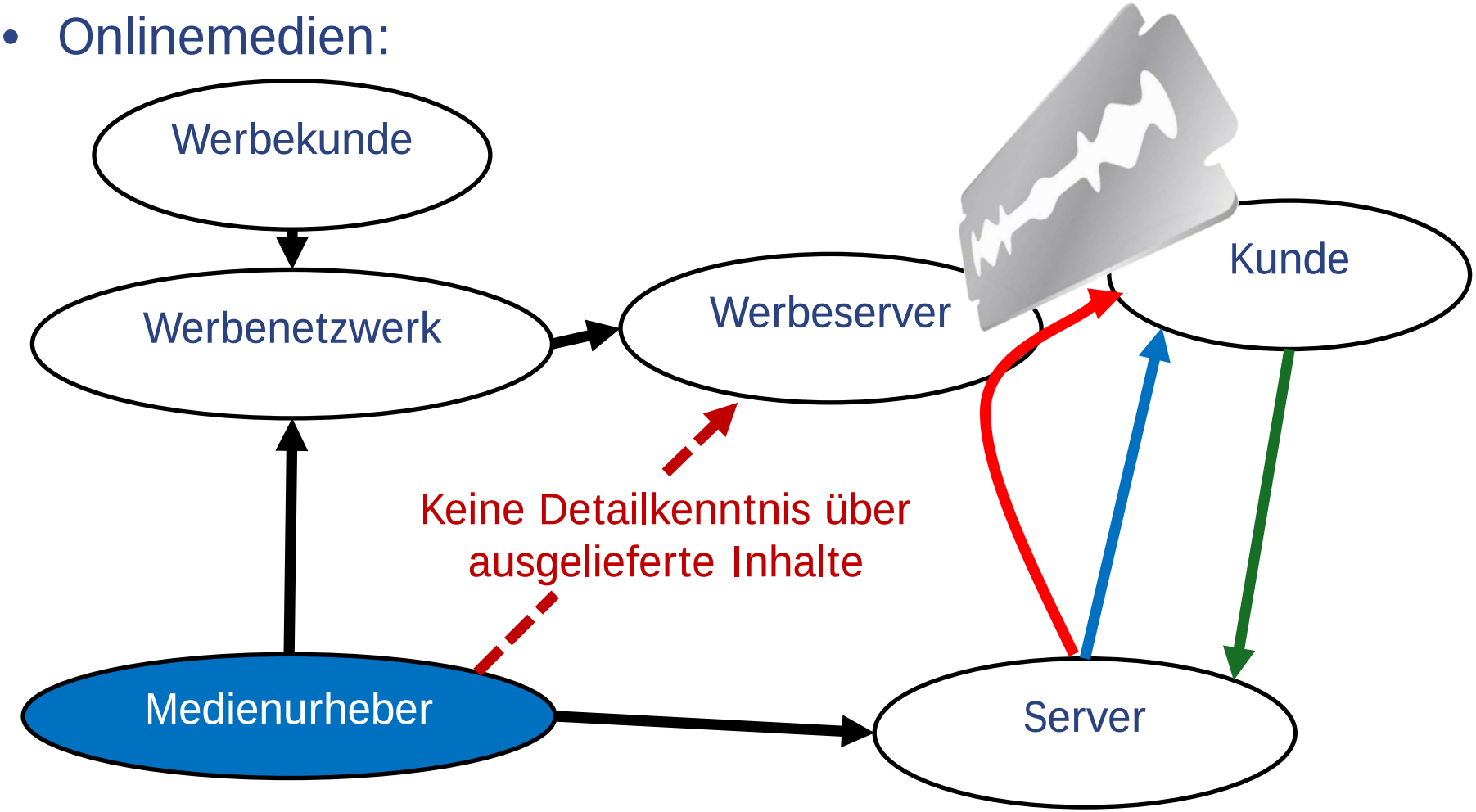
Werbung: Die Rasierklinge im Heft

- Klassische Werbung hat transparente Verantwortlichkeit
- Beispiel: Printmedien



Werbung: Die Rasierklinge im Heft

- Onlinemedien:



ATA GATHERED SINCE
EPT 15, 2017

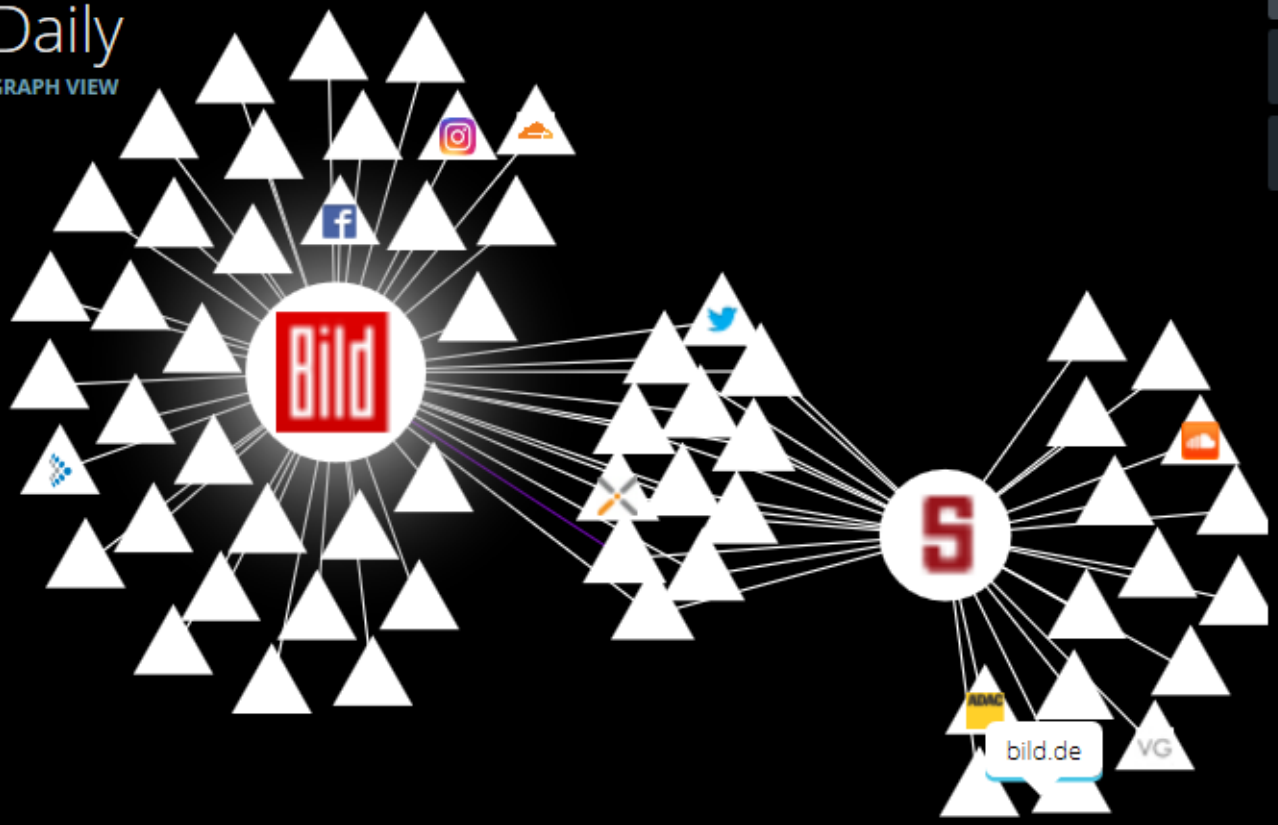
YOU HAVE VISITED
3 SITES

YOU HAVE CONNECTED WITH
76 THIRD PARTY SITES

TRACKING PROTECTION

Daily

GRAPH VIEW



TOGGLE CONTROLS

FILTER

Hide

- Visited Sites
- Watched Sites
- Cookies
- Third Party Sites
- Blocked Sites

Recent Site

Last 10 Sites

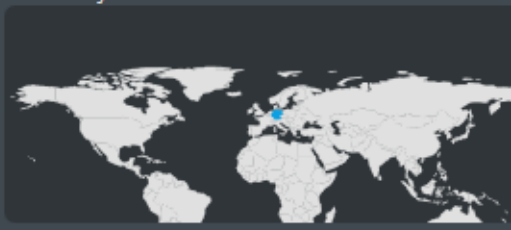
bild.de

FIRST ACCESS Fri, Sept 15, 2017 2:23PM
LAST ACCESS Fri, Sept 15, 2017 3:32PM

Block Site

Server Location

Germany



Connected to **46 sites** since first access.

- outbrain.com
- ioam.de
- bildstatic.de
- tiqcdn.com
- facebook.net
- smartadserver.com
- adnxs.com
- mookie1.com
- emetriq.de
- df-srv.de
- opecloud.com
- visualrevenue.com
- 71i.de

Wem gehört die Webseite?

re:publica TEN

	BILD.DE	SPON	SZ	ZEIT
Requests	2339	2514	1886	1130
Unique Hosts	**195**	**184**	**172**	**122**
3rd Party Hosts	182	172	160	113
Own Hosts (*)	**13**	**12**	**12**	**9**

(*) basiert auf augenscheinlich zum Verlag gehörenden Domains/Subdomains

Konsequenzen der Werbung durch Drittanbieter

- Neben Applikationen werden nun auch Inhalte zum Risiko:
  - Harmlose Inhalte werden durch Vermischung mit unkontrollierten Fremdinhalten potentiell gefährlich
  - Verantwortlichkeit für die ausgelieferten Inhalte ist weitgehend unklar

- Möglichst umfassende Inhaltsfilterung ist eine Maßnahme der IT-Sicherheit

Möglichkeiten der Inhaltsfilterung

- Browser-Erweiterungen
  z.B. uBlock Origin
  → können nicht verhindern, dass Fremdinhalte in Apps zur Anzeige kommen

- Lokale, systemweite Filter
  z.B. hosts-Datei oder Personal Firewall
  → müssen pro Gerät installiert und gepflegt werden

- Netzwerkweite Filter
  z.B. Pi-Hole

Risiken zunehmender Inhaltsfilterung

- Filterlisten werden in der Regel nicht individuell zusammengestellt, sondern aus zentraler Quelle abonniert

Ihre Fragen?

Christian Krause
ULD38@datenschutzzentrum.de
Tel. 0431-988 1247