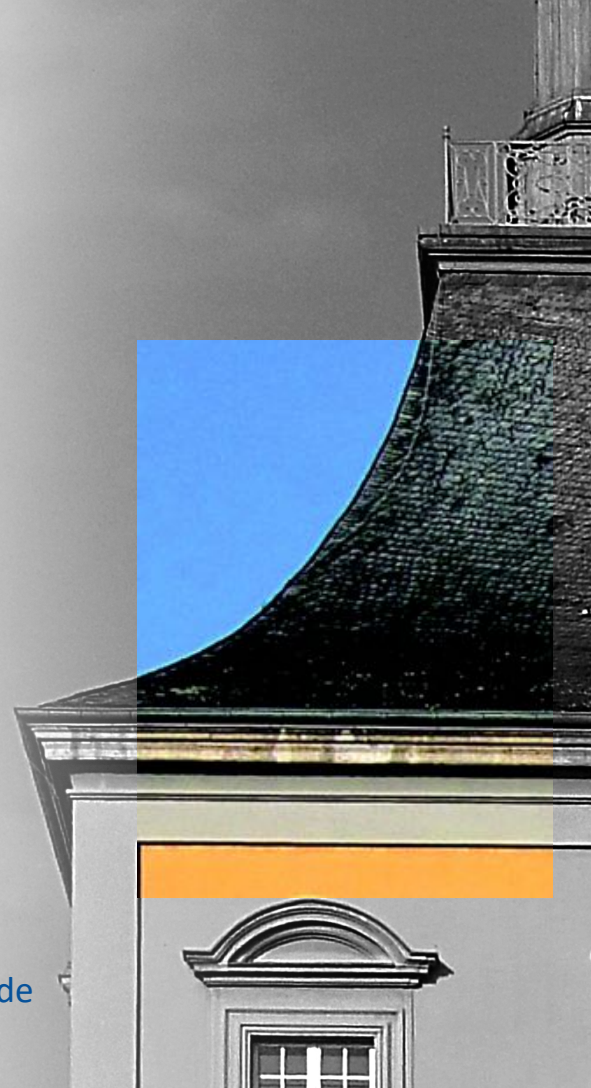
UNIVERSITÄT BONN

ULD
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

#DATALEAK

WIE MAN BETROFFENE INFORMIERT



Susan Gonscherowski
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein
uld611@datenschutzzentrum.de

Matthias Wübbeling
Universität Bonn
Arbeitsgruppe IT-Sicherheit
matthias.wuebbeling@cs.uni-bonn.de

UNIVERSITÄT BONN

MOTIVATION

- Identitätsdiebstahl verursacht:
  - Materielle Schäden
  - Gesellschaftliche Schäden
  - Persönliche Schäden
  - Vertraulichkeitsverlust
- Großes Dunkelfeld
  - Wird je nach Schadensart selten zur Anzeige gebracht.

=> Prävention durch Aufklärung und Warnung!

UNIVERSITÄT BONN

DATENSAMMLUNG

- Forschungsfragen:
  - Wie können Identitätsdaten (automatisch) gesammelt werden?
  - Wie werden diese Daten analysiert?
  - Wie werden diese Daten gespeichert?
  - Wie lässt sich (automatisch) warnen?
  - Wie häufig sollte gewarnt werden?
  - Wer sollte warnen?
  - Was können Betroffene tun?

UNIVERSITÄT BONN

IDENTITÄTS(DATEN)-DIEBSTAHL

- Angreifer erbeuten Daten von:
  - Unternehmen
  - Privatpersonen
  - Suchmaschinen
  - Sozialen Netzwerken
- Das Ziel der Angreifer ist zunächst einmal nicht der Identitäts-Diebstahl.

UNIVERSITÄT BONN

IDENTITÄTS(DATEN)-DIEBSTAHL

- Identitätsdaten
  - Name
  - Geburtsdatum
  - Adresse
  - …
- Digitale Identitätsdaten
  - E-Mail
  - Benutzerkonten (Amazon, eBay, XING, etc.)
  - …

UNIVERSITÄT BONN

IDENTITÄTS(DATEN)-DIEBSTAHL

- Online Marktplätze für Identitätsdaten
  - Angreifer verkaufen (Teil-)Datensätze
  - Betrüger kaufen Identitätsdaten
- Qualität von Datensammlungen
  - X% garantiert aktive E-Mailadressen
  - Pastebin zum Probieren vor dem Kauf
- Datenbroker kaufen Datensammlungen und reichern diese an (Klartextpasswörter, zusätzliche Informationen)

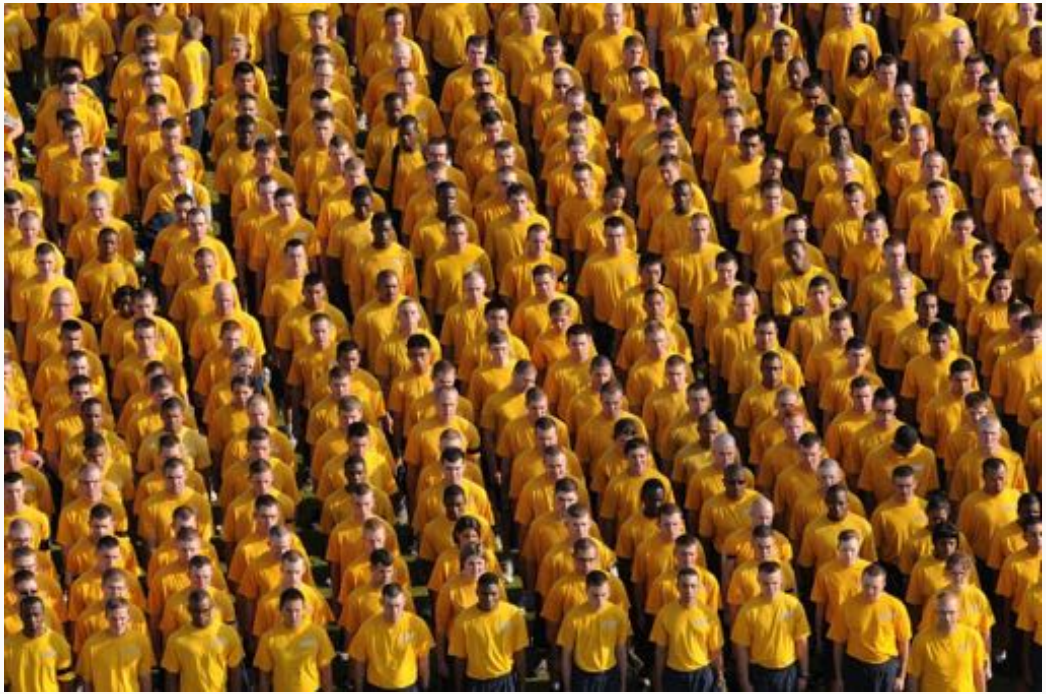
UNIVERSITÄT BONN

IDENTITÄTS(DATEN)-DIEBSTAHL

- Betroffene von Identitätsdaten-Diebstahl:
  - Unmittelbar nur der Betreiber des Geräts (PC / Server / Smartphone)
  - Identitätsinhaber nur mittelbar; bemerken den Diebstahl i.d.R. nicht
- Nach DSGVO Aufklärungspflicht von Kunden (z.B. Anschreiben / Zeitungsannonce) bei Bekanntwerden
- An dieser Stelle noch kein materieller Schaden für einen Identitätsinhaber

UNIVERSITÄT BONN

DATENSAMMLUNG



- Wie werden Identitätsdaten (Leaks) gesammelt?
  - Manuell (ca. 95% - 520 Dateien)
    - Foren
    - Untergrundseiten
    - Tauschbörsen
  - Automatisiert (ca. 5% - 18000 Dateien)
    - Paste-Sites

UNIVERSITÄT BONN

TECHNISCHE AUFBEREITUNG

- Leak-Daten sind
  - syntaktisch unterschiedlich
  - semantisch nicht dokumentiert

  => schwer automatisiert zu parsen

- Datenschutz-Aspekte
  - Leak Daten enthalten nicht benötigte / gewollte Informationen
  - Speicherung von Informationen?

UNIVERSITÄT BONN

TECHNISCHE AUFBEREITUNG

- Unterstützte Datentypen:
  - E-Mail-Adresse
  - Passwort
  - Hash (z.B. Passwort-Hashes)
  - Benutzernamen
  - Vornamen
  - Nachnamen
  - Postleitzahlen (API)
  - Adressen (API)
  - IBAN
  - Kreditkartennummern
  - Telefonnummern (API)

UNIVERSITÄT BONN

WARNUNG

- Gemeinsame Warnung mit einem vertrauenswürdigen Dienstanbieter
  - Entwicklung einer API
  - Datenschutzfreundlichkeit als Designziel
- Psychologische Unterstützung beim Warnungsdesign:
  - Enthaltene Information
  - Häufigkeit der Warnung
  - Rückfragemöglichkeiten
- Warnungen durch eine öffentliche Stelle?
  - Sammlung / Betrieb / Betroffenenhilfe

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

DATENSCHUTZ

- Wie können beide Ziele maximal datenschutz-freundlich erreicht werden?
- Wo liegen die rechtlichen Grenzen?
- Was fordert der Gesetzgeber im Rahmen der Umsetzung?
- Wer kann diese Aufgabe übernehmen?

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

IRRUNGEN UND WIRRUNGEN

„Schutzlücken“ in Art. 33 + 34 DSGVO

- Leaks können sehr resistent sein
- Folgen nur schwer absehbar
- Benachrichtigung nicht gesichert

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

EIN „BILD“ SAGT MEHR ALS 1000 WORTE

Konzeption eines Warnsystems

- Erhebung
- Datenanalyse
- Identifizierung Betroffener
- Benachrichtigung
- Abschluss

Risiken eines Warnsystems

- Fehlende Rechtmäßigkeit
- Mangelnde Zweckmäßigkeit bzw. Erforderlichkeit
- Warnsystem wird zum Datenleck
- Falschmeldungen

Anforderungen an die Datenverarbeitung eines Warnsystems

- Datenminimierung
- Transparenz
- Nicht-verkettung
- Integrität
- Vertraulichkeit
- Verfügbarkeit
- Intervernierbarkeit

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

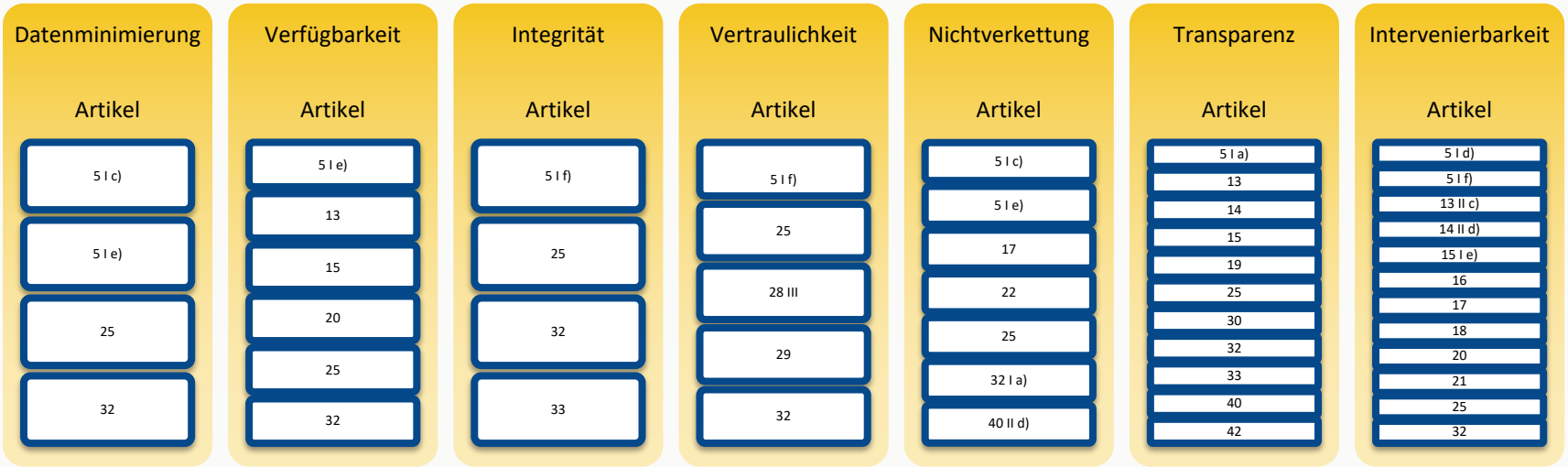
DER ZWECK HEILIGT DIE MITTEL

- Nein, auch für ein Warnsystem gilt: **Verbot mit Erlaubnisvorbehalt**
  - Verarbeitung durch öffentliche Stellen auf Grundlage eines Gesetzes (Art. 6 I e DSGVO)
  - Verarbeitung durch nicht-öffentliche Stelle auf Grundlage eines berechtigten Interesses oder einer rechtl. Verpflichtung (Art. 6 I f DSGVO oder Art. 6 I c DSGVO)

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

ES IST DER GEDANKE, DER ZÄHLT

- Nein, die Verarbeitung pb Daten fällt unter das Datenschutzrecht und die möglichen Risiken für die Betroffenen sind unabhängig vom Umstand des vorausgegangenen Leaks zu beurteilen



Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

ZU RISIKEN UND NEBENWIRKUNGEN…

- technische und organisatorische Maßnahmen müssen dem Risiko des Verarbeitungsverfahrens entsprechen
- Risikoanalyse obliegt Verantwortlichen
- Verantwortlicher zieht DSA-Muss-Liste (WP248); Art. 35; ErwGr 75 heran
- Hohes Risiko = hohe Anforderungen an TOM + verpflichtende DSFA
- Vorherige Konsultation

UNIVERSITÄT BONN

ERKENNTNISSE & DISKUSSION

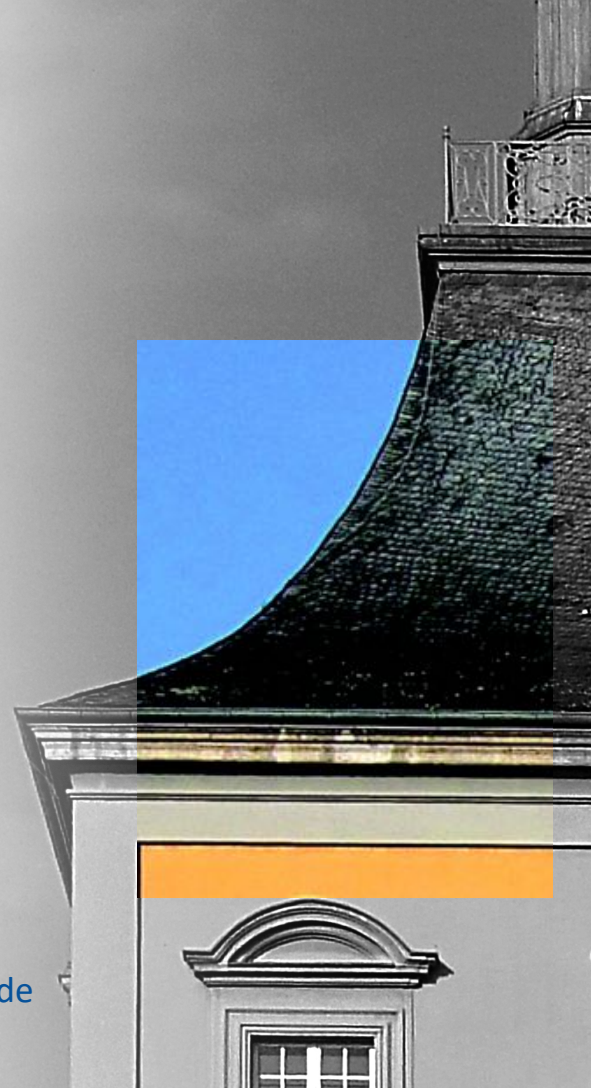
- Identitätsdatendiebstahl ist nicht Identitätsdiebstahl
  - Computerspionage
  - Datenhehlerei
  - Betrug
- Viele Identitätsdaten kursieren im Netz:
  - Nicht alle eignen sich für Identitätsdiebstahl
  - Nicht alle eignen sich für Warnungen
- Warnung müssen durchdacht und dürfen nicht zu häufig sein.
- Wer betreibt ein solches System?

UNIVERSITÄT BONN

ULD
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

#DATALEAK

WIE MAN BETROFFENE INFORMIERT



Susan Gonscherowski
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein
uld611@datenschutzzentrum.de

Matthias Wübbeling
Universität Bonn
Arbeitsgruppe IT-Sicherheit
matthias.wuebbeling@cs.uni-bonn.de