Wie wird die DSGVO umgesetzt und welche Lücken/Lügen gibt es?

Einführung

- Seit fast 6 Monaten muss die DSGVO von Firmen und Organisationen in der EU befolgt werden.
- Die folgende Präsentation zeigt erste Erfahrungen mit der DSGVO, Probleme und Lücken bei der Umsetzung…

Meine DSGVO-Anfragen

25. Mai 2018

- DSGVO-Anfragen wurden an ca. 50 Firmen und Organisationen gesendet, bei denen nach persönlichen Daten gefragt wurde.
- Je nach Firmen gab es unterschiedliche Ansätze und Strategien und die zurückgesendeten Ergebnisse reichten von lächerlich bis sehr detailliert.
- Ausgewählt waren diese Firmen / Organisationen nach dem persönlichen „Nerv-Faktor“ und Firmen, bei denen ich Kunde bin/ war.

Reaktionen

- Die Reaktionen lassen sich folgendermaßen einteilen
  - Nichts Tun
  - Leugnen
  - Nur Teile zurückliefen
  - Komplizierte Verfahren
  - Downloadlinks in Anwendung integriert
  - Verschlüsselter USB-Stick mit Passwort per Einschreiben

Reaktionen - Nichts Tun

- Einige der Angeschrieben habe nicht reagiert
  - CDU
  - Die Grünen
  - AFD
  - Die Linken
- SPD, CSU und FDP haben übrigens schnell geantwortet
- Beschwerden beim zuständigen Landesdatenschützer Berlin wurden per Webseite eingegeben. Dieser wollte zusätzlich alles schriftlich per Post (4 Mal)

Leugnen

- Einige Firmen hatten erst einmal keine Information.
- Erst beharrlich darauf bestanden wurde, fand man plötzlich meine Daten.
- Z.T. mussten weitere Email-Adressen angebenden werden (Identifikation über Email)

- Beispiel: REWE

Nur Teile zurückliefen

- Die Faulen lieferten einfach nur meine Adress-Daten und Bankverbindung zurück.
- 1&1 „versteckte“ sich hinter einem Link der Benutzeradresse und Bankverbindung zurückliefert
- Als (genervter) langjähriger Kunde von 1&1 stimmt das einfach nicht.
- Email-SPAM kann nicht einfach abbestellt werden, sondern erfordert POSTIDENT

Kompliziertes Verfahren

- Die meisten Firmen verifizieren keine Daten, sondern „glauben“ einer Email-Anfrage.
- Das (korrekte) Identifizieren (Postident, Kopie Ausweis/ Reisepass) des Anfragenden ist sehr selten.
- Video-Ident wurde bei mir nirgends angeboten
- Teilweise ist es schwierig, die Zuständigen zu finden (z.B. Microsoft, Bundeswehr).
- Große Konzerne wollen den Teilbereich wissen (ARD: Sind Sie Schauspieler, Laie, … DB: Welche der 1000 Konzerntöchter, …)

- Volkswagen sendet die Daten erst nach erfolgreichem Postident-Verfahren,
  Besitz an jedem einzelnen Fahrzeug muss nachgewiesen werden.

Integriert in Anwendung / Downloadlinks

- Integration in der Anwendung ist für die meisten Kunden der einfachste Ansatz
- Xing, Google, 1&1 folgen diesem Ansatz
- Daten meistens auf Daten des „Hauptsystems“ beschränkt.

XING

Ihre persönliche Datenauskunft

... und hier sind sie: Ihre Daten.

Hiermit erhalten Sie eine vollständige Kopie Ihrer bei XING gespeicherten personenbezogenen Daten in einem übersichtlichen Archiv. Nutzen Sie die Navigation links, um sich durch die verschiedenen Bereiche zu bewegen.

Das könnte Sie interessieren.

Verschlüsselter USB-Stick + Passwort per Einschreiben

- Einen sehr sicheren Ansatz verfolgte SKY.
- Dort wurden die Daten auf einem USB-Stick verschlüsselt und das Passwort separat (per Einschreiben) verschickt.

Email

- Zusenden der Daten per Email
- Der überwiegende Teil der angefragt Daten wurde per Email gesendet. Manchmal gab es Rückfragen („Wir haben eine namengleiche Person von 1989 mit abweichender Adresse“)
- Oracle, CSU, AVM, …

Post

- Zusenden der Daten per Post
- SPD, Bahn, Rewe, Payback, …

DSGVO-Workflow (einfach)

- Anfrage an die Firma/Org.
- Firma/Org. verifiziert Anfragenden
- Antwort der Firma

Lügen nachweisen

DSGVO Lügen nachweisen

- Lügen kann man sehr oft und sehr einfach nachweisen
- Möglichkeiten
  - Gewinnspiele
  - Newsletter
  - Kenntnisse der Business Prozesse

Bundeswehr
Wir. Dienen. Deutschland.

Suchbegriff

Aktuelles Einsätze Streitkräfte Verwaltung Gedenken Soziales Personal

Sie sind hier: Startseite > Gewinnspiel

Gewinnspiel

Hier können Sie gewinnen!

IHRE LÖSUNG

An: Zentrale Onlineredaktion

Betreff: Gewinnspiel

Ihre Antwort: *

IHRE ANGABEN

Anrede: * Frau Herr

Dienstgrad:

Vorname: *

Name: *

Straße und Nr.: *

Postleitzahl: *

Ort: *

E-Mail:

Telefon: *

* Pflichtfelder: Diese Angaben benötigen wir, um Ihre Mitteilung zu bearbeiten.

Gewinnspiele

- An Gewinnspiele (Via Suchmaschine oder auf der Webseite) teilnehmen und personenbezogene Daten eingeben.
- Das Gewinnspiel wird oft von Marketing-Firmen für den Auftraggeber organisiert.
- Anfrage stellen
- In der Regel bleiben solche Anfragen nicht berücksichtigt

Newsletter & User Account

- Auch an Newslettern kann man sich anmelden.
- Alternativ an irgendwelchen Web-Applikationen der Firma/Organisation (Shops, Demo-Seiten, …)
- Anfrage stellen
- Solche Anfragen werden z.T. berücksichtigt

Kenntnisse der Business Prozesse

- Auch an Newslettern kann man sich anmelden.
- Alternativ an irgendwelchen Web-Applikationen der Firma/Organisation (Shops, Demo-Seiten, …)
- Anfrage stellen
- Solche Anfragen werden z.T. berücksichtigt

Kenntnisse der Business Prozesse

- Anwort des Heise Verlags auf eine Anfrage
- Als gelegentlicher Autor für Heise, stehen mir Einnahmen von der VG Wort zu.
- Diese Daten müssen irgendwo gespeichert sein.
- Meine Anfrage danach wurde ignoriert…

Angriffe mit DSGVO

Angriffe mit DSGVO

- Die DSGVO kann auch für Angriffe auf Daten verwendet werden
- Die meisten Anfragen werden ohne genaue Identifikation oder mit einer Ausweiskopie beantwortet.
- Dies kann ausgenutzt werden, um Daten einer Zielperson zu erhalten.

Beispiel-Angriff

- Ehepartner bereitet Scheidung vor
- Um „Munition“ für die Scheidung zu bekommen, werden Anfragen an Banken/Versicherungen/… (wo sind welche Konten) gestartet.
  (Nicht unüblich im Versicherungsbereich)
- Als Ehepartner hat man normalerweise auch Zugriffe auf den Ausweis des Partners. Davon kann einfach eine Kopie erstellt werden, die für Anfragen verwendet werden kann.
- Die Post wird vor dem Ehepartner abgefangen.

GDPR-DDOS

- Ein GDPR-Distributed Denial of Service (DDoS) kann von politischen Gruppen dazu verwendet werden, Firmen mit einer großen Anzahl von Anfragen zu belasten.
- Beispiele:
  - Der Autohersteller AAA schädigt die Umwelt. Jeder soll bitte eine DSGVO-Anfrage an datenschutz@aaa.de stellen, die in 30 Tagen beantwortet werden muss.
  - Das Pharmaunternehmen CCC tötet arme Tiere in Tierversuchen. Jeder soll bitte eine DSGVO-Anfrage an datenschutz@ccc.de stellen, die in 30 Tagen beantwortet werden muss.
  - Die Partei DDD ist gegen FFF. Jeder soll bitte eine DSGVO-Anfrage an datenschutz@ddd.de stellen, die in 30 Tagen beantwortet werden muss.

Gehackte Email Accounts

- Gehackte Email-Accounts können auch für Anfragen verwendet werden, wenn keine zusätzliche Authentifizierung erfolgt.

Personenbezogene Daten in Tabellen

Datenbanken & Personenbez. Daten

- Bei Auswertungen über ca. 3000 Datenbankinstanzen (unterschiedlicher Kunden) enthielten ca. 0,5-2% aller Tabellen personenbezogene Daten (je nach Kundendefinition)
- Berücksichtigt werden die in der Regel jedoch nicht (viele Ausreden).
- Automatisierte Scans des Data Dictionaries liefert normalerweise die meisten Treffer von personenbezogenen Daten.

Personenbezogene Tabellen in der Realität

- **Mailingliste (%MAILING,% oder %NEWSLETTER%)**
- Zwischentabellen für Import von PBD, danach aber nicht gelöscht
- Kopien von Tabellen im selben Schemata (%_BACKUP, %_BAK, %_BACK, %_SIC, %_TMP, %_TEMP, %_HIST, %_SAVE, SIC_%, %_TB, TMP%, TEMP%, %_121205...)
- Kopien von Tabellen in unterschiedlichen Schemata
- Kopie eines ganzen Oracle Schemata
- Tabellen im Oracle Recyclebin
- Alte Tabellen mit Jahreszahlen
- Import von Daten in Tabellen (_IMP, _IMPORT, ...)
- Kopie von PBD aus anderen Systemen (Anhang DB-Kürzel oder APP-Kürzel)
- Export von PBD (_EXP, _EXPORT, EXP, ...)
- Tabellen in Kleinbuchtstaben oder Mixed-Case unüblich in Oracle (oft Export von anderen Plattformen
- PBD für Schulungen (Wurden diese anonymisiert?)
- Demouser bzw. Tabellen für Demouser vorhanden

Table Samples I

Zwischentabelle für Import, danach nicht gelöscht

- 160 APP1.T_SPARTNER_IMPORT(phone,email,adr_street_loc,adr_street)

Kopien von Tabelle im selben Schemata (%_BACKUP, %_BAK, %_BACK, %_SIC, %_TMP, %_TEMP, %_HIST, %_SAVE, SIC_%, %_TB, TMP%, TEMP%, %_121205...)

- 350 APP.PERSON_BACKUP(phone,mobile,mail,lastname,gender,firstname,fax,birthday)

Kopien von Tabellen in unterschiedlichen Schemata

- 450 APPDEV.USER_(screenname,password_,passwordencrypted, middlename,lastname, firstname,facebookid, emailaddressverified,emailaddress ,contactid)
- 450 APP.USER_(emailaddressverified,lastname,middlename,firstname,facebookid,emailaddress ,screenname,password_,passwordencrypted,contactid)

Kopie eines ganzen Oracle Schemata

- 160 APPTESTKOPIE.XMAUTHUSERGROUP(lastname,forename,email)
- 160 APPTEST.XMAUTHUSERGROUP(lastname,forename,email)

Table Samples II

Mailingliste (%NEWSLETTER% oder %MAILING%) Mailing hat fast immer Außenwirkung = kritisch, eventuell unabsichtliche Email an Kunde

- 160 APP1.NEWSLETTER_ORDER(user_lastname,user_firstname,user_salutation)
- 190 APP2.NEWSLETTEREINTRAG(vorname,nachname,geschlecht,email)
- 250 APP.MAILING(vorname,telefon_zentrale,telefon_ap,email,anrede,account_contact_id)

Alte Tabellen mit Jahreszahlen

- 380 APP.MARK_LESERUMFRAGE_2012(email,einverstaendnis_email,anrede,vorname,telefon,strasse_hnr,plz,ort,gewinn_etui_smartphone)

Kopien aus anderen Systemen (via DB-Kürzel oder APP-Kürzel)

- 160 APP.LIEFERANT_DB2(postleitzahl,strassenname,strassenname_erw,hausnummer)

Table Samples III

Import von Daten (_IMP, _IMPORT, ...)

- 160 APP.MITARBEITER_X500_IMPORT(vorname,nachname,email)
- 160 APP.T_SERVICEPARTNER_IMPORT(phone,email,adr_street_loc,adr_street)
- 1440 APP.IMP_OUTLOOK (weiterevornamen,weiterestelefon,weiteresrbundeslandkanton, weiteresfax,weiterepostleitzahl,webseite,vorname,telefonprivat2,telefonprivat,telefongeschaftlich2,telefongeschaftlich,telefonfurhorbehinderte,telefonfirma,telefonassistent,postleitzahlprivat,postleitzahlgeschaftlich,pager,ort,nachname,mobiltelefon2,mobiltelefon,geschlecht,geburtstag,…)

Export von Daten (_EXP, _EXPORT, EXP, ...)

- 400 APP.EXPORTPERSONSETTINGS(eps_salutation,eps_orgphonecurrent,eps_orgfaxcurrent,eps_organisationphone,eps_organisationfax,eps_lastname,eps_firstname,eps_email,eps_birthday)

Tip bei Ausweisanfragen

- Nicht notwendige Daten schwärzen
- Stempel mit Namen der angefragt Firma in das Bild einfügen
- Möglichst viele Information (alle Email-Adresse, Mitarbeiterdaten, …) angeben, das erspart Rückfragen.

Zusammenfassung

- Exakte Email-Adresse wird bei den meisten als Schlüssel verwendet. Falsche/Alte Email -> Keine Daten.
- Eine genaue Identifikation (Postident/Videoident) findet normalerweise nicht statt
- Daten ohne Email werden meistens ignoriert.
- Datenbanktabellen werde in der Regel ignoriert. Es werden maximal Daten von 1-2 Datenbanken verwendet.
- Der Nachweis von fehlenden Daten im DSGVO-Report ist meistens für Externe einfach.
- Abmahnung werden über kurz oder lang folgen…

Q & A

Thank you

- Contact:

Red-Database-Security GmbH
Eibenweg 42
D-63150 Heusenstamm
Germany