Datenschutz für Administratoren

Was ist meine Grundlage für Speicherung,
was darf ich speichern und
wie lange?

Hanno Wagner <froscon@rince.de>

Wer bin ich?

- Hanno Wagner, arbeite in Stuttgart
- Seit 3 Jahren Betrieblicher Datenschutzbeauftragter
- Bin mit dem Thema seit >10 Jahren vertraut (CCC, Fitug et al.)

Warum Administratoren? (1)

- Zugriff auf die komplette Infrastruktur – angefangen von den Desktoprechnern über Server im RZ bis hin zu den Datensicherungs- und Datenlöschungsmaßnahmen
- Wir haben viel mit Rohdaten zu tun – den Anwendern ist nicht bewusst was für Daten sich ansammeln.

Warum Administratoren? (2)

- Wir sind (theoretisch) in der Lage Daten zusammenzuführen – daher sind die Daten gefährdet (und wir mit ihnen!)
- Wir können „mal eben“ Statistiken erstellen die so gar nicht geplant waren
- Ebenfalls sollen wir oft “kurz mal” was nachschauen – wir haben ja Zugriff und den kurzen Dienstweg

Quintessenz

Wir sollten wissen was wir dürfen :)

Beispiele von pers.bezogenen Daten im Admin-Alltag

- Klassisch: Mailadressen im Maillog. Wenn man einen Mailserver für Kunden hat auch nicht-eigene Mails!
- Auch klar: IP-Adressen im Webserver-Log. Wunderbar für Statistiken die Marketing haben will.
- Im Proxy gibt es auch entsprechende Ips? Man kann erkennen wer sich welche Seiten anschaut

- Active Directory-Nutzung für verschiedene Applikationen, wie Berechtigungen im Content Scanner?
- Was ist mit dem LDAP-/NIS-/NIS+-Server für die Authentisierung?
- Datenbank-Logins?
- Fotos für die ID-Card der Firma?

Theorie: Welche Gesetze befassen sich mit dem Thema Datenschutz?

- Das bekannteste und weitestgehende ist das Bundesdatenschutzgesetz (letzte Änderung 03.07.2009)
- In den Ländern gibt es entsprechende Landesdatenschutzgesetze; aber was dort nicht geregelt ist wird über BDSG geregelt → Fallback
- Für uns weiter relevant sind andere Rechtsnormen wie TKG, TMG, Sozialgesetzbuch X, VDS

Was genau wird geregelt?

Der Umgang mit **personenbezogenen** Daten, in welchem Maße die Aufnahme und Verarbeitung von Daten erlaubt ist und welche Rechte und Pflichten der Datenerheber und Datenspeicherer hat.

Dieses ist in Europa inzwischen auch sehr einheitlich, es gibt einen Grundstandard

Was sind personenbezogene Daten?

Daten sind personenbezogen, wenn sie persönliche oder sachliche Verhältnisse einer natürlichen Person beschreiben. Dabei muss nicht der Name bekannt sein, es reicht die Bestimmungsmöglichkeit der Person

Unterschied USA ↔ Europa

In den USA gehören die Daten demjenigen der sie gesammelt hat. In Europa der Person die damit beschrieben wird

Es gibt in den USA deswegen eine Safe-Harbour-Regelung: Firmen die sich dieser Regelung unterwerfen verpflichten sich nach europäischem Datenschutzrecht zu agieren.

Welche Kontrollorgane gibt es?

- Für uns: den Datenschutzbeauftragten der Firma oder der Behörde.
- Eine Firma sollte einen DSB haben wenn mehr als neun Personen unmittelbar mit personenbezogenen Daten umgehen (oder 20 Leute mittelbar)
- Ansonsten: Gruppenleiter, Chef, bis hoch zum Vorstand

Und sonst?

- Bundesbeauftragter für Datenschutz und Informationsfreiheit: Öffentliche Einrichtungen des Bundes
- Landesdatenschutzbeauftragter: Öffentliche Einrichtungen des Landes
- Innenministerium (auch der Länder): Nicht-Öffentliche Einrichtungen. Können diese Aufgabe auch dem LDS übertragen

Arten von personenbezogenen Daten (gesetzlich)

- **Einfache Daten**: Name, Vorname, Geburtstag,Familienstand, aber auch Bankdaten
- **Persönlichkeitsdaten**: Einkommensverhältnis, Familienverhältnis, Lebensstil, Einkaufsverhalten
- **Sensible Daten**: Herkunft, politische Meinung, Religion, medizinische Daten

Was können wir tun?

- Generell gilt das Stichwort:

Datensparsamkeit.

Daten die nicht gebraucht werden müssen gelöscht werden. Es sollten möglichst wenig Daten überhaupt erst anfallen. Es muss eine Begründung geben, warum die Daten gesammelt werden sollen. Auch die Geräte zur Erfassung sollten nur das können wofür sie jetzt gebraucht werden.

- Wer keinen Zugriff auf die Daten braucht bekommt sie auch nicht (typischer Fall: Marketing und Webserver-Logfiles)
- Wir müssen sicherstellen dass die Daten auch nach der Benutzung gelöscht werden. Auch wenn wir selbst neugierig sind ;-)

Begründung zur Sammlung von Daten

- Prinzipiell gilt ein Erlaubnisvorbehalt. Laut dem BDSG gibt es vier Möglichkeiten, eine Erlaubnis zum Datensammeln zu haben / zu bekommen:
  - Gesetzliche Vorgaben
  - Öffentliche Quelle / bereits veröffentlicht
  - Abwägung
  - Einwilligung

Zweckbindung

- Es muss vorher bereits festgelegt sein zu welchem Zweck diese Daten gesammelt werden
- Einfach die Daten für weitere Zwecke zu nutzen ist nicht erlaubt

Weitergabe von Daten

- Wird gemacht wenn man Daten im Auftrag verarbeitet – dann findet eine Weitergabe an Dritte statt
- Dabei muß vorher bereits schriftlich festgehalten werden welche Daten zu welchem Zweck weitergegeben werden und was der Dritte damit machen darf.
- Der Dritte muß den hier geltenden Datenschutz einhalten, auch wenn er selbst in einem anderen Land sitzt.

Was machen mit den Logfiles?

- Datensparsamkeit heisst nicht dass sofort alle Logfiles gelöscht werden müssen. Für Debugging / Nachverfolgbarkeit ist es üblich 6 Wochen Logfiles zu behalten
- Es muß aber sichergestellt werden dass die Daten danach wirklich gelöscht werden
- Wie sensitiv die personenbezogenen Daten sind, die gelogged werden?

Die Daten werden aber länger gebraucht!

- Wenn für längerfristige Reports Daten gebraucht werden können die personenbezogenen Daten (IP-Adresse, Mailadresse, Login...) anonymisiert oder pseudonymisiert werden
- Beispiel: durch das aus-X-en von IP-Adressteilen (192.168.xx.xx)
- Anderes Beispiel: Statt einzelner Nutzer die Abteilung loggen.

Wie spreche ich mit meinen Kollegen darüber?

- Wichtig ist eine Sensibilisierung der Kollegen auf das Thema – ihnen bewusst machen worum es geht (Nothing to hide stimmt vielleicht jetzt aber auch in 5 Jahren?)
- Auch gemeinsames “Finden” von kritischen Logfiles ist wichtig
- Wir wollen niemanden vor den Kopf stoßen, nur aufmerksam machen

Wie gehe ich Änderungen an?

- Eine generelle Strategie für die Firma mit den Chefs besprechen (Best Practices) wie zum Beispiel loggen gemacht wird – viele Leute lassen bei Programmen die Defaulteinstellungen ohne weiter drüber nachzudenken

- Die Überprüfung dieser Einstellungen ist wichtig – nicht um “jemanden” bloßzustellen, sondern um gemeinsam den Konsens zu haben
- Dieses Wissen kann man bei neuen Programmen oder Projekten gleich anwenden

Verfahrensverzeichnis / TOMs

- Wenn es noch kein Verfahrensverzeichnis gibt, ist es sinnvoll eines zu erstellen: Dort wird unter anderem festgehalten, welche Verfahren es gibt die personenbezogene Daten loggen.
- Zusätzlich kann man generell technisch-organisatorische Maßnahmen (TOM) definieren in denen beschrieben wird wann und wie gelöscht wird

Und was ist mit Backup?

- Wenn Daten im Backup liegen und nicht ohne großen Aufwand (der Admins) herausgeholt werden können gelten sie als unkritisch. Natürlich gibt es Möglichkeiten, Daten 10 Jahre lang aufzubewahren. Der Zugriff darauf sollte aber für den normalen Nutzer sehr schwer sein.

Fragen?

- Wenn es Fragen gibt, bitte stellen!

- Ansonsten stehe ich gerne zur Verfügung unter <froscon@rince.de>

Viel Spass auf der FrOSCon 2009!!

Vielen Dank für die Aufmerksamkeit

- Dieser Vortrag wird unter der Creative Commons License veröffentlicht: