Sicherheit/Datenschutz

Datenschutz für den Administrator

Moderner und effektiver Einsatz von EDV ist in Betrieben und Verwaltungen heute eine Grundvoraussetzung für ökonomisches Arbeiten. Damit die Rechte und Freiheiten der betroffenen Personen durch die Verarbeitung ihrer Daten nicht beeinträchtigt werden, muss dabei aber dem Datenschutz Rechnung getragen werden. Gerade auch Administratoren, die auf „Alles" zugreifen können, sollten einige Grundbegriffe kennen.

Viele Administratoren glauben, mit dem Bundesdatenschutzgesetz (BDSG) wenig zu tun zu haben, da sie meinen, nur mit technischen, nicht aber mit personenbezogenen Daten umzugehen. Da aber Admins auf alles Zugriff haben, können sie auch auf personenbezogene Daten zugreifen. Außerdem haben sie Zugriff auf Protokoll- und Logdateien, in denen personenbezogene Daten enthalten sind. Selten wissen Admins auch, dass sie mit wenigen (Vor) Einstellungen bei einem erfolgreichen Datenschutz helfen können.

In den diversen Protokolldateien finden sich Daten aus drei unterschiedlichen Regelungsbereichen.

- BDSG: Protokollierung von Vorgängen, die nichts mit Kommunikation über Netzwerke zu tun haben: Passwortänderungen, Dateizugriffe o.ä.
- Telekommunikation: Protokollierung von Daten, die Auskunft über Kommunikationsvorgänge geben: Wer hat wann mit wem eine Netzverbindung aufgebaut? bspw. E-Mail-Protokolle, Anmeldevorgänge am Netz
- Telemedien: Protokollierung der Nutzung von Tele- und Mediendiensten: Wer hat welche Webseiten oder andere Datendienste abgerufen?

Bei der Beurteilung, ob ein Datensatz personenbezogen ist, muss man berücksichtigen, dass eine IP-Adresse als personenbezogen gilt, da Sie einer einzelnen Person zuordnbar ist.

Wichtige Grundsätze

Eine Verarbeitung personenbezogener Daten ist nur zulässig, wenn eine Rechtvorschrift diese Verarbeitung erlaubt oder anordnet, oder wenn der Betroffene eingewilligt hat. Die Einwilligung muss schriftlich erfolgen.

Personenbezogene Daten, die zur Sicherstellung des ordnungsgemäßen Betriebs gespeichert werden, unterliegen nach § 31

BDSG einer strengen Zweckbindung und dürfen **nur** für diese Zwecke verwendet werden.

Zudem sind personenbezogene Daten sofort zu löschen, wenn Sie für den Zweck, zu dem sie gespeichert wurden, nicht mehr benötigt werden. Daten, die zur Fehlereingrenzung gespeichert werden, müssen gelöscht werden, sobald eine Fehlersuche nicht mehr stattfindet. Hieraus ergeben sich kurze Speicherfristen (eine Woche bis ein Monat). Lediglich Daten, die zu Dokumentationszwecken benötigt werden (z.B. Buchungsprotokolle im SAP), dürfen im Rahmen der gesetzlichen Dokumentationsdauern gespeichert werden.

Dateizugriffsrechte regulieren

Der Administrator sollte Zugriffsrechte auf Dateien so einstellen, dass der freie Zugriff auf die Dateien eines Benutzers nicht möglich ist. So sollten z.B. in einem UNIX System die Dateiattribute auf

```
(rw- -- --)
```

voreingestellt sein, damit nur der Benutzer selbst auf die Dateien zugreifen kann. Jeder Benutzer kann dann im eigenen Ermessen und eigener Verantwortung diese Attribute ändern. Vergleichbares gilt auch für die Passwort-Policy einer Firma oder Behörde.

Ist bei Krankheit oder Nichterreichbarkeit eines Mitarbeiters unbedingt ein Zugriff auf Dateien erforderlich, so sollte ein Administrator dies nicht auf Zuruf erledigen, sondern immer nur mit schriftlicher Anordnung. Außerdem sollte der Zugriff auf Dateien nur mit Zeugen (z.B. Datenschutzbeauftragter, Betriebsrat, Personalabteilung) erfolgen. Es versteht sich von selbst, dass alle Daten dabei streng vertraulich behandelt werden müssen.

Fernwartung

Mit der Novellierung des BDSG im Jahre 2001 ist eine neue Regelung zum Thema Wartung geschaffen worden (§ 11 Abs. 5 BDSG). Wenn im Rahmen von Wartungsmaßnahmen auf personenbezogene Daten zugegriffen werden kann, gelten die Vorschriften für Auftragsdatenverarbeitung (§ 11 BDSG). Dies heißt, ein schriftlicher Auftrag muss erteilt werden, und es gibt Mindestanforderungen für den Inhalt des Auftrags. Auf den Webseiten der Beauftragten für den Datenschutz der Länder (Liste der Internet-Adressen unter http://www.rainer-gerling.de/links) findet man Musterverträge.

Technische Vorgaben des BDSG

Die acht Gebote des Datenschutzes in der Anlage zu § 9 BDSG machen abstrakte Vorgaben zu den Schutzzielen:

- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Auftragskontrolle
- Verfügbarkeitskontrolle
- Trennungsgebot

Die erforderlichen konkreten Umsetzungsmaßnahmen sind mit dem Datenschutzbeauftragen des Unternehmens abzustimmen.

Datenschutz und Telekommunikation

Das Telekommunikationsgesetz (TKG) regelt den Datenschutz für die technischen Kommunikationseinrichtungen (z.B. Kabel, Router oder Firewalls). Die Daten, wer wann mit wem kommuniziert, dürfen im Wesentlichen zum Aufbau, zur Abwicklung und zur Abrechnung der Verbindungen verarbeitet werden. Die eigentlichen Kommunikationsinhalte (was wurde kommuniziert) dürfen nur unter ganz engen Voraussetzungen ausnahmsweise verarbeitet werden.

Artikel 10 des Grundgesetzes schützt neben dem Briefgeheimnis auch das Post- und Fernmeldegeheimnis. Details dazu sind in § 85 TKG geregelt. § 85 TKG und § 206 Strafgesetzbuch (StGB) regeln die Vertraulichkeit der Kommunikationsinhalte. Danach ist es nicht erlaubt, dass der Betreiber des E-Mail-Systems die Inhalte der E-Mails kontrolliert. Eine entsprechende Regelung in einer Benutzungsordnung oder Betriebsvereinbarung wäre rechtlich nicht wirksam. E-Mails eines Benutzers dürfen nur mit dessen Zustimmung gelesen werden. Ist bei Abwesenheit eines Mitarbeiters unbedingt ein Zugriff auf seine E-Mails nötig, so sollte ein Admin nicht auf mündliche Bitte hin die Mails weiterleiten, sondern die gleichen Regeln wie bei Dateizugriffen einhalten.

Auch die Abwehr von Viren und Spam ist rechtlich nicht unkritisch, da § 206 Abs. 2 Nr. 2 StGB die Nachrichtenunterdrückung unter Strafe stellt. Wegen der starken Nähe zur Zensur ist dies prinzipiell eine richtige Regelung. Hier sollten die genauen Verfahrensweisen eng mit dem Datenschutzbeauftragten abgestimmt werden. Der Empfänger der E-Mail sollte dem Verfahren explizit zugestimmt haben. In der Praxis kann dies durch ein Einwilligungsformular oder die Aktivierung des Verfahrens durch den Empfänger geschehen.

Datenschutz bei Telemedien

Die Teledienstegesetze (TDG) und das Teledienstedatenschutzgesetz (TDDSG) sowie der Mediendienste-Staatsvertrag (MD-StV) wenden sich an Inhaltsanbieter (z.B. Anbieter von Webseiten oder Telefonansagediensten). Eine Inanspruchnahme der angebotenen Dienste kann kaum personenbezogen ausgewertet werden. Erlaubt ist lediglich eine Verarbeitung zu Abrechnungszwecken oder eine Verarbeitung zur Dienstermöglichung. Eine Missbrauchsbekämpfung ist nur beim Versuch des Umgehens von Bezahlmechanismen gestattet.

Es empfiehlt sich, die Protokolldateien nur anonymisiert zu schreiben. Das Ausblenden des letzten Bytes der IP-Adresse anonymisiert die Log-Datei weitgehend. Auswertungen, aus welcher Domain die Zugriffe erfolgten, sind auch mit diesen reduzierten Daten immer noch möglich. Eine detaillierte Analyse, wer das Webangebot wie nutzt, ist nur unter Pseudonym möglich (§ 6 Abs. 3 TDDSG). Die IP-Adresse ist **kein** Pseudonym.

Autor: Rainer W. Gerling

Informationen zum Autor: Rainer W. Gerling ist Datenschutzbeauftragter der Max-Planck-Gesellschaft und Honorarprofessor für IT-Sicherheit an der FH München