



4 Rechtliche Fragestellungen beim Einsatz eines IDS

Dieses Kapitel nennt die Gesetze, die bei einem Einsatz eines Intrusion-Detection-Systems in der Bundesrepublik Deutschland zu beachten sind. In anderen Ländern sind die entsprechenden Gesetze zu konsultieren. Die angesprochenen Gesetze sind grundsätzlich zu beachten, wenn Rechnersysteme zur Datenverarbeitung eingesetzt werden. Jedoch erfordert der Einsatz eines IDS eine zusätzliche Betrachtung dieser Gesetze.

4.1 Welche Gesetze sind anwendbar?

Bei der Betrachtung der rechtlichen Fragestellungen beim Einsatz eines IDS müssen zwei Aspekte besonders betrachtet werden. Hierbei handelt es sich um

- den Datenschutz und
- die Verwertbarkeit der Daten vor Gericht.

Diese beiden Aspekte sollen nun kurz beleuchtet werden. Hierbei kann nur die persönliche Erfahrung des Autors wiedergegeben werden. Es handelt sich dabei um keine vollständige oder gar rechtsverbindliche Aussage. Sämtliche Darstellungen dieses Kapitels sind immer im Lichte der speziellen Situation neu zu evaluieren und mit der Rechtsabteilung des eigenen Unternehmens/Behörde abzustimmen.

4.1.1 Datenschutz und IDS

Hier kommen die folgenden Gesetze zum Tragen (keine Gewähr für Vollständigkeit):

- Recht auf informationelle Selbstbestimmung (Art. 1 Abs. 1 GG)
- Zweckbindung der Daten (BDSG § 3, § 14 (4) und § 31)
- Innerbetriebliche Mitbestimmung (BtrVG § 87 (1))
- Gesetz über die Nutzung der Teledienste (TDG)
- Teledienstedatenschutzgesetz (TDDSG) (TDDSG § 4-6)

Ausführliche Ausführungen zu diesem Thema finden sich auch in dem Skript *Internetrecht* von Dr. Thomas Hoeren (<http://www.uni-muenster.de/Jura.itm/hoeren/>).

Das Bundesdatenschutzgesetz (BDSG) definiert in § 3 Abs. 1 den Schutz der personenbezogenen Daten. Dies begrenzt den Datenschutz auf natürliche Personen. Daten juristischer Personen werden nicht durch das BDSG geschützt. Das BDSG schützt alle Informationen, die eine Aussage über den Betroffenen machen (Name, Anschrift, Staatsangehörigkeit, Beruf etc.).

Sobald diese Daten anonymisiert oder aggregiert vorliegen, ist es herrschende Meinung, dass sie keine Einzelangaben mehr sind, wenn kein Rückschluss auf die einzelne Person möglich ist. Erfolgen Zuordnungen einzelner Benutzer zu diesen Gruppen, so wird jedoch der Personenbezug wiederhergestellt. Die Anonymität wird nach § 3 Abs. 7 BDSG als ausreichend angesehen, wenn die Daten »nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbar natürlichen Person zugeordnet werden können«. Anonyme oder pseudomisierte Speicherungen sind erlaubt, wenn nicht eine Auflösung der Anonymität oder der möglicherweise verwendeten Pseudonyme durch den Datenverarbeiter möglich ist. Hierzu kann es zum Beispiel sinnvoll sein, die Daten getrennt zu speichern, so dass Verbindungsdaten und Personendaten auf unterschiedlichen Systemen an unterschiedlichen Orten gespeichert werden. Der Datenverarbeiter ist dann nicht autorisiert, auf beide Quellen zuzugreifen.

Das BDSG schützt sämtliche Verarbeitungsphasen der Daten: Erhebung, Speicherung, Veränderung, Übermittlung, Sperrung und Löschung. Dieser Schutz ist in § 3 des BDSG definiert.

Grundsätzlich ist jede Verarbeitung personenbezogener Daten verboten. Eine Verarbeitung ist nur erlaubt, wenn

- a. die betroffene Person ihre Einwilligung schriftlich erklärt hat,
- b. die Erlaubnis in einem Tarifvertrag oder einer Betriebsvereinbarung enthalten ist oder
- c. eine gesetzliche Vorschrift existiert.

Die schriftliche Einwilligung durch den Betroffenen ist nach § 4a Abs. 1 BDSG nur möglich, wenn der Betroffene zuvor über den Zweck der Speicherung und die mögliche Übermittlung der Daten aufgeklärt wurde. Besteht nicht die Möglichkeit, eine schriftliche Einwilligung der Betroffenen (z.B. bei Online-Verträgen) einzuholen, so erlaubt § 3 des TDDSG eine elektronische Einwilligung, die so gestaltet ist, dass eine bewusste Handlung des Kunden vorliegt. Genaue Angaben sind dem Gesetz zu entnehmen.

Die Erlaubnis kann auch in einem Tarifvertrag oder einer Betriebsvereinbarung geregelt werden. Zunächst ist die Nutzung der Internetdienste in dienstliche und private Nutzung zu trennen. Eine Überwachung privater E-Mails fällt unter das Fernmeldegeheimnis (§ 85 TKG). Darf der Anwender nur dienstliche E-Mails versenden, so darf der Arbeitgeber wahrscheinlich den Ein- und Ausgang von E-Mails einschließlich

der Zieladressen festhalten. Er darf ferner bei Abwesenheit des Mitarbeiters E-Mails lesen, sofern diese nicht als privat zu erkennen sind. Ansonsten ist nur die Lektüre bei Nachweis eines berechtigten Interesses erlaubt (Verdacht auf strafbare Handlungen, Gefährdung des Betriebsfriedens oder Betriebsgeheimnisse).

Eine gesetzliche Vorschrift kann ebenfalls die Speicherung personenbezogener Daten erlauben. Sobald die Daten für die Rechnungsstellung benötigt werden oder für die Aufrechterhaltung des technischen Betriebes erforderlich sind, dürfen sie wahrscheinlich zweckgebunden gespeichert werden. Eine Löschung der Daten ist erforderlich, sobald sie nicht mehr benötigt werden.

Laut § 9 des Telekommunikations-Datenschutzgesetzes darf ein Telekommunikationsanbieter im Einzelfall die Bestandsdaten und Verbindungsdaten der Beteiligten erheben, verarbeiten und nutzen, wenn dies zur Erkennung, Eingrenzung und Beseitigung von Störungen dient.

Liegen Anhaltspunkte vor, so dürfen alle Bestands- und Verbindungsdaten erhoben, verarbeitet und genutzt werden, die zum »Aufdecken sowie Unterbinden von Leistungserschleichungen und sonstigen rechtswidrigen Inanspruchnahmen der Telekommunikationsnetze und -dienste erforderlich sind«. Hiervon sind jedoch unverzüglich die Regulierungsbehörde für Telekommunikation und Post und der Bundesbeauftragte für den Datenschutz in Kenntnis zu setzen.

Ein wahrscheinlich unproblematischer Einsatz eines IDS-Systems ist nur zu gewährleisten, wenn die schriftliche Einwilligung der Beteiligten bzw. eine Betriebsvereinbarung vorliegt oder das IDS nur bei einem Missbrauch im Einzelfall eine Protokollierung der Verbindungsdaten vornimmt. Dies ist jedoch kritisch, da das IDS falsch-positive Meldungen erzeugen kann. Es muss daher versucht werden, möglichst sämtliche falsch-positiven Meldungen zu unterdrücken.

§ 31 BDSG schreibt dann aber vor, dass die personenbezogenen Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, nur für diese Zwecke verwendet werden dürfen. Sie dürfen zum Beispiel nicht zur Leistungskontrolle ausgewertet werden.

4.1.2 Verwertbarkeit vor Gericht

Die Verwertbarkeit der Daten von Intrusion-Detection-Systemen vor Gericht wird in zwei verschiedenen Gesetzen geregelt: in der Strafprozessordnung (StPO) und in der Zivilprozessordnung (ZPO). Die Ergebnisse eines IDS sind vor Gericht so zu behandeln wie der Augenschein oder eine Zeugenaussage. Die Bewertung kann jedoch auch durch einen Sachverständigen vorgenommen werden. Es handelt sich nicht um ein rechtsverbindliches Beweismittel im Sinne von § 416 ZPO.

Von großem Nachteil ist die Tatsache, dass diese Daten üblicherweise sehr leicht modifiziert oder gänzlich künstlich erzeugt werden können. Hier ist es erforderlich, die

IDS-Daten mit einer automatischen Integritätssicherung zu versehen, die eine spätere Modifikation erkennen lässt. Dies kann eine Speicherung auf read-only-Datenträgern oder eine digitale Signatur sein. Ein weiteres Problem stellt die Authentizität der Daten dar. Es muss gewährleistet sein, dass die Daten so erhoben wurden, wie sie tatsächlich vorlagen und bei der Erhebung es nicht zu einer Verfälschung der Daten gekommen ist. Eine Nachvollziehbarkeit ist am wahrscheinlichsten beim Einsatz eines Open-Source-Systems oder der Verwendung zertifizierter Software gewährleistet.

4.1.3 Allgemeiner Hinweis

Die hier gegebenen Ausführungen und Zitate wurden nach bestem Wissen ohne jede Gewährleistung und ohne Anspruch auf Vollständigkeit gegeben. Eine Evaluierung muss immer vor Ort durch die entsprechende Rechtsabteilung des Unternehmens erfolgen. Einige weitere Hinweise diesbezüglich erfolgen im Kapitel 17, »Datenschutz-Aspekte in einem Unternehmensnetzwerk«.