ConSecur
GmbH

IT-Sicherheitsmanagement

Einführung von Intrusion-Detection-Systemen

Rechtliche Aspekte

31. Oktober 2002

Version 1.0

1 Inhalt und Zweck des Dokuments

In dem vorliegenden Dokument werden rechtliche Aspekte beim Einsatz von Intrusion-Detection-Systemen (kurz IDS) untersucht.

Die Darstellung der rechtlichen Vorgaben und zugehöriger Maßnahmen dient in erster Linie dem Zweck, Technikern und IT-Experten zu verdeutlichen, welche gesetzlichen Bestimmungen es gibt, die für den Einsatz von IDS relevant sind. In Kapitel 2 wird hierzu zunächst begründet, weshalb beim Einsatz von IDS sowohl datenschutzrechtliche Aspekte als auch Aspekte der Arbeitnehmer-Mitbestimmung zu berücksichtigen sind. Relevante bundesdeutsche Gesetzesvorgaben werden in Kapitel 3 beschrieben[1]. In Kapitel 4 werden beispielhaft Maßnahmen aufgeführt, die umzusetzen sind, um gesetzliche Anforderungen zu erfüllen. Für einen konkreten Einsatz von IDS sind Maßnahmen mit Rechtsexperten (Juristen, Rechtsabteilung) abzustimmen.

2 Rechtliche Aspekte beim Einsatz von IDS

Im Rahmen ihres Einsatzes zur Erkennung von Angriffen und Sicherheitsverletzungen zeichnen IDS eine Vielzahl von Daten auf. Diese Daten sind teilweise personenbezogen bzw. lassen die Zuordnung von Personen zu bestimmten Aktivitäten zu. Beispiele hierfür sind

- die Aufzeichnung unberechtigter Zugriffsversuche auf Daten,
- die Aufzeichnung unberechtigter Zugangsversuche zu Anwendungen,
- die Aufzeichnung der IP-Adressen oder Domain-/Rechnernamen, von denen aus Angriffe oder Angriffsversuche gestartet wurden.

Ein Grund des Einsatzes von IDS kann gerade darin bestehen, Angriffe zurückzuverfolgen und ihre Verursacher ermitteln zu können.

Ob und welche personenbezogenen Daten aufgezeichnet werden, hängt dabei stark von der Einsatzweise und Konfiguration bzw. Kalibrierung des IDS ab. Dies soll an den folgenden zwei Einsatzbeispielen verdeutlicht werden:

- **Einsatz des IDS zum ergänzenden Schutz des Internet-Übergangs**

  Beim Einsatz eines IDS als ergänzende Maßnahme zum Schutz des Internet-Übergangs, wie er im Vordergrund des Leitfadens steht, fallen typischerweise kaum personenbezogene Daten an. Für von außen initiierte Angriffe liegen im Allgemeinen lediglich IP-Adressen (als Pseudonyme) vor. Um einen Personenbezug herzustellen, ist sowohl die Auflösung der IP-Adresse durch den zugehörigen DNS-Namen erforderlich als auch die Ansprache des Unternehmens bzw. der Organisation, der dieser Name zugeordnet ist. Häufig ist diese Zuordnung aufgrund lediglich temporär zugeordneter oder gefälschter IP-Adressen nicht möglich.

  Interne Personenbezüge ergeben sich insbesondere, falls das IDS auch dazu eingesetzt wird, die IT-Systeme am Internet-Übergang vor unberechtigten Zugriffen aus dem internen Netz zu überwachen. In diesem Fall werden typischerweise Login-Namen oder IP-Adressen (als Pseudonyme) aufgezeichnet.

[1] Die Beschreibung erhebt keinen Anspruch auf Vollständigkeit. Zudem wurde EU-Recht im Rahmen der Ausarbeitung nicht berücksichtigt.

- **Einsatz des IDS zur Überwachung des internen Netzes**

  Eine weitergehende interne Überwachung verbunden mit einem höheren Aufkommen an personenbezogenen Daten ist gegeben, wenn IDS-Sensoren im internen Netz eingesetzt werden. Diese Einsatzweise kann z. B. dazu dienen, Angriffe und Sicherheitsverletzungen, die von Innentätern initiiert werden, oder Verstöße gegen interne Richtlinien zu erkennen.

Über die zweckgebundene Aufzeichnung - teilweise personenbezogener - Daten hinaus, können IDS dazu missbraucht werden, Verhaltensweisen von Mitarbeitern zu kontrollieren, da sie über weitgehende Protokollierungs- und Auswertungsfunktionen verfügen.

Beim Einsatz von IDS ist daher darauf zu achten, dass rechtliche Anforderungen sowohl des Datenschutzes als auch der Arbeitnehmer-Mitbestimmung geeignet berücksichtigt werden.

3 Relevante rechtliche Vorgaben

Bei der datenschutzrechtlichen Einstufung der gesamten vom IDS aufgezeichneten Daten über erkannte Ereignisse sind folgende bundesdeutsche Gesetze zu beachten[2]:

- Das Bundesdatenschutzgesetz (BDSG, Stand 19.7.2002), §§3a, 4, 4a, 5, 11, 14, 19a, 28 und 31.
- Die Telekommunikations-Datenschutzverordnung (TDSV, Stand 21.12.2000), §3.
- Das Betriebsverfassungsgesetz (BetrVG, Stand 10.12.2001), §§87 und 90 für nicht-öffentliche oder öffentlich-rechtliche Wettbewerbsunternehmen.
- Das Personalvertretungsgesetz des Bundes (BPersVG, Stand 9.7.2001) bzw. des zuständigen Landes, hier beispielhaft §75 BPersVG.
- Das Gesetz über den Datenschutz bei Telediensten (TDDSG, Stand 14.12.2001), §§4-6.
- Das Gesetz über die Nutzung von Telediensten (TDG, Stand 14.12.2001), §4.

In den folgenden Abschnitten werden die einzelnen Bestimmungen näher erläutert.

3.1 Bundesdatenschutzgesetz (BDSG)

Das BDSG bezweckt, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

Dazu sind zunächst die Grundsätze der Datenvermeidung und Datensparsamkeit zu beachten: Datenverarbeitungssysteme sollten derart konfiguriert und konzipiert sein, dass so wenig personenbezogene Daten wie möglich erhoben werden (§3a). Direkte Personenbezüge von Daten können dabei durch eine Pseudonymisierung vermieden werden. Funktionen zur expliziten Pseudonymisierung stellen marktverfügbare IDS derzeit typischerweise jedoch nicht bereit.

Die Zulässigkeit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten kann entweder durch andere Rechtsvorschriften oder durch die explizite Einwilligung der Betroffenen erteilt werden (§4 und 4a).

Zu beachten ist, dass den Personen, die mit der Bearbeitung der personenbezogenen Daten beauftragt sind, untersagt ist, diese Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Die aufgezeichneten

[2] Die Beschreibung erhebt keinen Anspruch auf Vollständigkeit. Zudem wurde EU-Recht im Rahmen der Ausarbeitung nicht berücksichtigt.

Daten unterliegen dem Datengeheimnis. Insbesondere sind Personen, die in nicht-öffentlichen Stellen beschäftigt sind und mit derartigen personenbezogenen Daten operieren, auf das Datengeheimnis zu verpflichten (§5).

Werden personenbezogene Daten im Auftrag durch andere Stellen, z. B. einem IT-Dienstleister, erhoben, verarbeitet oder genutzt, so ist der Auftraggeber für die Einhaltung der Bestimmungen des Gesetzes im Bezug auf den Datenschutz verantwortlich (§11).

Den von der Sammlung personenbezogener Daten betroffenen Personen ist auf Antrag Mitteilung darüber zu machen, welche Daten zur Person gespeichert wurden, an wen sie weitergeleitet wurden und zu welchem Zweck sie gespeichert wurden (§19).

Der Zweck der Erhebung personenbezogener Daten ist konkret festzulegen (§28).

Hinsichtlich der Speicherung personenbezogener Daten durch ein IDS sind insbesondere folgende Paragraphen relevant:

- §14 (2): Das Speichern, Verändern oder Nutzen [...] ist [...] zulässig, wenn es zur Verfolgung von Straftaten oder Ordnungswidrigkeiten [...] erforderlich ist.
- §14 (4), §31: Personenbezogene Daten, die ausschließlich [...] zur Sicherstellung eines ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage genutzt werden, dürfen nur für diesen Zweck verwendet werden.

Der Zweck des Einsatzes eines IDS besteht im erweiterten Sinn genau in der Sicherstellung eines ordnungsgemäßen Betriebs von DV-Anlagen bzw. IT-Systemen. Hierbei ist gemäß §14 (4) und §31 bei der Datenspeicherung die Zweckbindung sicherzustellen.

Falls Angriffe bzw. Sicherheitsverletzungen mit dem Charakter von Straftaten oder Ordnungswidrigkeiten durch das IDS erkannt werden, dürfen gemäß §14 (2) die aufgezeichneten Daten zu deren Verfolgung genutzt werden.

3.2 Telekommunikations-Datenschutzverordnung (TDSV)

Die TDSV regelt den Schutz personenbezogener Daten der an der Telekommunikation Beteiligten bei der Erhebung, Verarbeitung und Nutzung dieser Daten durch Unternehmen und Personen, die geschäftsmäßig Telekommunikationsdienste erbringen oder an deren Erbringung mitwirken.

In diesem Zusammenhang sind Diensteanbieter dazu verpflichtet, die durch den Einsatz von IDS entstehenden personenbezogenen Daten sowie deren Verarbeitung auf das Notwendigste zu reduzieren (§3).

3.3 Gesetz über den Datenschutz von Telediensten (TDDSG)

Das TDDSG regelt den Schutz personenbezogener Daten der Nutzer von Telediensten.

Im Falle der Datenerhebung durch einen Diensteanbieter ist der Nutzer zu Beginn eines Nutzungsvorganges über die Art, den Umfang und den Zweck der Erhebung sowie der Verarbeitung und Nutzung personenbezogener Daten durch den Diensteanbieter zu unterrichten. Dies kann einmalig oder individuell vor jeder Nutzung geschehen. Kann eine Einwilligung elektronisch erfolgen, so ist sicherzustellen, dass die Einwilligung auf einer eindeutigen und bewussten Handlung des Nutzers beruht. Darüber hinaus muss die Einwilligung protokolliert werden. Der Inhalt muss jederzeit für den Nutzer abrufbar sein (§4).

Dem Diensteanbieter ist es unter bestimmten Umständen erlaubt, Nutzerprofile zu erstellen (§6). Es ist jedoch auf keinen Fall zulässig, erstellte Nutzerprofile und Daten über Träger von Pseudonymen zusammenzuführen (§4).

3.4 Gesetz über die Nutzung von Telediensten (TDG)

Das TDG schafft einheitliche Rahmenbedingungen für die verschiedenen Nutzungsmöglichkeiten der elektronischen Informations- und Kommunikationsdienste.

Insbesondere wird der Schutz personenbezogener Daten auch für Diensteanbieter, die in der Bundesrepublik ihre Dienste anbieten, aber in einem anderen Staat innerhalb des Geltungsbereiches der Richtlinie 2000/31/EG niedergelassen sind, rechtlich verpflichtend (§4 (4)).

3.5 Betriebsverfassungsgesetz (BetrVG)

Das BetrVG regelt für nicht-öffentliche oder öffentlich-rechtliche Wettbewerbsunternehmen die Zusammenarbeit zwischen Arbeitgeber und Betriebsrat, der gewählten Vertretung der Arbeitnehmer.

Das BetrVG räumt dem Betriebsrat ein Mitbestimmungsrecht ein, wenn technische Systeme durch die Firmenleitung eingeführt werden sollen, die das Verhalten der Arbeitnehmer überwachen können (§87). Hierunter fallen grundsätzlich auch IDS.

Insbesondere hat die Firmenleitung den Betriebsrat über die Planung derartiger technischer Anlagen rechtzeitig und unter Vorlage der erforderlichen Unterlagen in Kenntnis zu setzen, damit eine sinnvolle Mitbestimmung gewährleistet werden kann (§90).

3.6 (Bundes) Personalvertretungsgesetz ((B)PersVG)

Das PersVG (Bundes- oder Landesrecht) regelt für öffentliche Stellen die Zusammenarbeit zwischen der Dienststellenleitung und der gewählten Personalvertretung.

Das PersVG legt fest, dass der Personalrat ein Mitbestimmungsrecht hat, wenn technische Einrichtungen oder Anwendungen, die dazu bestimmt sind, das Verhalten der Beschäftigten zu überwachen, eingeführt werden sollen (§75). Hierunter fallen grundsätzlich auch IDS.

Insbesondere ist der Personalrat durch den Dienststellenleiter von der beabsichtigten Einführung derartiger Systeme zu unterrichten. Der Dienststellenleiter muss die Zustimmung des Personalrates für die Einführung derartiger Systeme beantragen (§69).

4 Umsetzung gesetzlicher Anforderungen

Nachstehend werden beispielhaft Maßnahmen aufgeführt, die umzusetzen sind, um gesetzliche Anforderungen zu erfüllen. Unternehmensspezifisch festzulegende Parameter sind dabei als <*Parameter*> gekennzeichnet. Für einen konkreten Einsatz von IDS sind die Maßnahmen mit Rechtsexperten (Juristen, Rechtsabteilung) abzustimmen.

1. Datenschutzbeauftragte und Betriebs- bzw. Personalrat sind in den Prozess der Einführung des IDS mit einzubinden. Im Phasenplan der IDS-Einführung bedarf es ihrer Zustimmung zum entsprechenden Einsatz eines IDS insbesondere nach den Phasen „Bedarfsfeststellung“, „Entscheidungsvorlage“ sowie „Feinkonzept und Produktauswahl“.
2. Der Betriebs- bzw. Personalrat und der Datenschutzbeauftragte sollten Anforderungen an den IDS-Einsatz mit dem IDS-Manager abstimmen. Die Anforderungen sollten die nachstehend aufgeführten Punkte beinhalten.
3. Alle Mitarbeiter werden über den Einsatz des IDS und die Einsatzzwecke informiert[3].
4. Sämtliche Mitarbeiter, die das IDS administrieren oder Zugriff auf Daten des IDS-Ereignisprotokolls haben, sind auf das Datenschutzgesetz zu verpflichten.
5. Im Rahmen des IDS-Einsatzes erfolgt die Aufzeichnung personenbezogener Daten ausschließlich, um den ordnungsgemäßen Betrieb von Datenverarbeitungsanlagen sicherzustellen. Eine Aufzeichnung von Daten erfolgt in dem Umfang, wie es für die Erkennung von Angriffen, Angriffsversuchen und Sicherheitsverletzungen und ggf. deren Rückverfolgung erforderlich ist. Personenbezogene Daten werden zu keinem anderen Zweck aufgezeichnet.
6. Vom IDS aufgezeichnete Daten, die zur Zuordnung erkannter Ereignisse (etwa Angriffe oder Sicherheitsverletzungen) zu deren Verursachern dienen, dürfen von IDS-Mitarbeitern nur dann an <*befugte Dritte*> weitergegeben werden, wenn aufgrund des Ereignisses, dessen Auswirkungen oder sich ergebenden Gefährdungen vom <*Vorgesetzten*> entschieden wurde, den Verursacher des Ereignisses zu ermitteln, oder die Weitergabe der Daten gemäß <*Richtlinie*> vorgesehen ist[4].
7. Die aufgezeichneten Daten werden spätestens nach einem Zeitraum von <*2 Monaten*> gelöscht. Ausgenommen hiervon sind Daten, deren weitere Speicherung aufgrund von Beweis- oder Nachweiszwecken erforderlich ist.
8. Änderungen der Einsatzweise des IDS oder der IDS-Einsatzzwecke erfordern die Zustimmung des Betriebsrats bzw. Personalrats.

---

[3] Abhängig von der Einsatzweise des IDS bleibt zu prüfen, ob es erforderlich ist, dass jeder Mitarbeiter sein Einverständnis zum IDS-Einsatz erklärt.

[4] Im Rahmen einer Richtlinie kann festgelegt werden, ab welchem Gefährdungs- bzw. Schadensausmaß in jedem Fall versucht werden soll, den Verursacher zu ermitteln.