



17 Datenschutz-Aspekte in einem Unternehmensnetzwerk

Wenn ein Intrusion Detection-System in einem kleinen Heimarbeitsnetz eingesetzt wird, ist dieser Einsatz eigentlich unproblematisch. Es existiert dort normalerweise kein Bedarf für einen besonderen Schutz der personenbezogenen Daten. Administrator und Benutzer sind ein und dieselbe Person. Die Person, die das IDS installiert, protokolliert lediglich die eigenen Daten.

Dies ist nicht der Fall, wenn die ID-Systeme in Unternehmen mit fünf oder 5.000 Angestellten eingesetzt werden. Hier muss sehr wohl der Datenschutz beachtet werden. Das Kapitel hat bereits die Probleme zu skizzieren versucht, die beim Einsatz eines Intrusion Detection-Systems entstehen. Dieses Kapitel versucht nun einige Hilfsmittel an die Hand zu geben, die es ermöglichen, diesen Einsatz zu bewerten. Des Weiteren werden Ausschnitte von Benutzerordnungen vorgestellt, die die Verwendung eines IDS erlauben können.

Alle Schritte sollten jedoch mit dem Datenschutzbeauftragten des Unternehmens abgesprochen werden. Dieser sollte bei Fragen die erste Anlaufstelle darstellen.

17.1 IDS im Unternehmen

Bei jedem Einsatz von Computern werden Daten verarbeitet. Dies ist nicht erst der Fall beim Einsatz von Intrusion Detection-Systemen. Sobald hierbei personenbezogene Daten verarbeitet werden, ist der Datenschutz zu berücksichtigen. Damit dies gewährleistet werden kann, existiert das Bundesdatenschutzgesetz (BDSG). Dieses regelt den Datenschutz auf Bundesebene.

Um die Überwachung des Datenschutzes zu garantieren, verlangt das BDSG die Einsetzung eines Datenschutzbeauftragten. Dieser Datenschutzbeauftragte muss sowohl in öffentlichen als auch in nicht-öffentlichen Stellen, die personenbezogene Daten automatisiert erheben, verarbeiten oder nutzen, bestellt werden. Der § 4f (BDSG) defi-

niert im Weiteren einige Ausnahmen, die jedoch nur auf sehr kleine Firmen und öffentliche Stellen zutreffen.

Im Grunde muss jede Firma, die personenbezogene Daten (Personalakten, Kundendaten, Arbeitszeiterfassung) erhebt, speichert und verarbeitet, einen Datenschutzbeauftragten bestellen.

Diese Person muss die für die Aufgabe notwendige Fachkunde und Zuverlässigkeit besitzen. Es besteht die Möglichkeit, diese Aufgabe auf eine externe Person zu übertragen.

Diese Person sollte bei allen Fragen die erste Anlaufstelle darstellen.

Beim Einsatz des IDS sollte in Absprache mit dem Betriebsrat, der ein Mitbestimmungsrecht in diesem Punkt besitzt, der Anwender über die Tatsache der Protokollierung aufgeklärt werden. Dies erfolgt sinnvollerweise in einer Benutzerordnung (siehe Abschnitt). Hierbei sollte die private Nutzung der Internetdienste nicht erlaubt werden. Dies ermöglicht eine anschließende Überwachung durch das Unternehmen. Sobald eine private Nutzung erlaubt ist, ist das Unternehmen Diensteanbieter und muss das Fernmeldegeheimnis beachten!

Es existieren im Grunde die drei folgenden Möglichkeiten:

1. Das Unternehmen bietet keine Dienste für Dritte an. Die eigenen Benutzer dürfen die Dienste nicht privat nutzen. Alle Verbindungen, die von außen aufgebaut werden, werden entweder durch eigene Benutzer, die von einem Telearbeitsplatz auf das Unternehmen zugreifen, initiiert oder sind mögliche Angriffe. Die eigenen externen Benutzer werden ebenfalls von der Benutzerordnung über den Zweck und die Art der Protokollierung aufgeklärt und haben ihr zugestimmt. Der Angreifer hinterlässt üblicherweise keine personenbezogenen Daten. Selbst wenn dies der Fall sein sollte, so ist wahrscheinlich das Interesse des Unternehmens an der Früherkennung von Angriffen schutzwürdiger als das Interesse des Angreifers, unerkannt zu bleiben. Die grundsätzliche Speicherung dieser Verbindungsdaten ist dann wahrscheinlich zulässig.
2. Das Unternehmen erlaubt die private Nutzung des Internets durch die eigenen Anwender. Dann ist die grundsätzliche Protokollierung der Verbindungsdaten nicht erlaubt und durch das Telekommunikationsgesetz (TKG) als Fernmeldegeheimnis geschützt. Eine Protokollierung ist wahrscheinlich nur in Ausnahmefällen bei Verdacht einer Störung und bei einem begründeten Verdacht gegen einen Mitarbeiter möglich. Die letztere Variante muss jedoch mit dem Betriebsrat abgesprochen werden. Das bedeutet, das IDS darf lediglich die problematischen Netzwerkpakete protokollieren. Die Benutzerordnung sollte über die Art und den Umfang der Protokollierung aufklären.
3. Das Unternehmen bietet Dienste für Dritte im Internet an. Dies kann zum Beispiel in Form eines Webservers oder eines Internet News Servers erfolgen. Das Unternehmen darf erneut keine personenbezogenen Verbindungsdaten protokollieren. Die Speicherung der personenbezogenen Daten darf gemäß dem Telediensteda-

tenschutzgesetz nur in dem Maße erfolgen, in dem sie für die Aufrechterhaltung des Betriebes und die Abrechnung erforderlich sind. Diese Daten sind zweckgebunden. Um den Betrieb aufrechtzuerhalten, wird jedoch das IDS wahrscheinlich mögliche Angriffe protokollieren dürfen. Das bedeutet, dass das IDS nicht grundsätzlich sämtliche Daten protokollieren darf, wenn sie personenbezogene Daten enthalten.

17.2 Benutzerordnungen

Die einfachste Methode, den Anwender über die Art und den Umfang der Protokollierung und die Verwendung der personenbezogenen Verbindungsdaten aufzuklären, ist es, die entsprechenden Informationen in einer Benutzerordnung oder einer Betriebsvereinbarung niederzulegen. Es kann sich auch um eine Ergänzung des Arbeitsvertrages handeln.

Im Folgenden werden Auszüge aus Beispiel-Benutzerordnungen vorgestellt. Es werden einige URLs genannt, unter denen öffentliche Stellen ihre Benutzerordnungen oder Orientierungshilfen veröffentlicht haben.

Der Landesbeauftragte für den Datenschutz des Landes Saarland hat unter <http://www.lfd.saarland.de/dschutz/BRLInt.htm> eine Beispiel-Benutzerrichtlinie veröffentlicht.

Die wesentlichen Punkte dieser Benutzerordnung sind:

■ Unter Punkt 2:

- *Die Nutzung der erlaubten Dienste ist ausschließlich zu dienstlichen/geschäftlichen Zwecken und im ausdrücklich erlaubten Umfang zur Erledigung Ihrer Aufgaben gestattet. Die Nutzung der Dienste zu privaten Zwecken ist – auch aus Kostengründen – untersagt.*
- *Das Ausprobieren, ob weitere Dienste als die ausdrücklich erlaubten zur Verfügung stehen und evtl. genutzt werden können, ist unzulässig.*

■ Unter Punkt 6:

- *Jeder Datenverkehr innerhalb des Lokalen Netzes und zwischen dem Lokalen Netz und dem Internet kann/wird einer automatischen vollständigen/gezielten Protokollierung (Verbindungs- und Inhaltsdaten) unterzogen.*
- *Die Protokolle werden für den Zeitraum von wenigstens einem Jahr aufbewahrt und bei Verdacht auf einen Sicherheitsverstoß durch eigens hierfür Berechtigte ausgewertet. ...*

Diese Punkte definieren die Nutzung des Internets nur für dienstliche/berufliche Zwecke und erlauben die Protokollierung der Verbindungs- und Inhaltsdaten.

Der Hauptpersonalrat des Landes Berlin veröffentlicht unter <http://www.berlin.de/hpr/dv-8.html> die Dienstvereinbarung über die Nutzung des Internets und anderer elektronischer Informations- und Kommunikationsdienste in der Berliner Verwaltung.

Die wesentlichen Ausführungen dieser Vereinbarung sind in § 3:

- *Um unbefugte Eingriffe in das Berliner Verwaltungsnetz (Berliner Landesnetz BELA, Metropolitan Area Network MAN) und die lokalen Netze (z.B. durch Hacking, Viren, Ausspähen, Einschleusen trojanischer Pferde) verfolgen zu können, dürfen Zugriffe auf die Dienste mit den Daten Proxy, Zeit, Ziel beim zentralen Infrastrukturbetreiber protokolliert werden.*
- *Zum ordnungsmäßigen Betrieb der Brandmauer-Rechner (Firewalls) zwecks Durchlassens zulässigen oder Stoppens nicht zulässigen Netzverkehrs und der vermittelnden Rechner (Proxies) werden personenbezogene Daten wie Rechneradresse oder Nutzerkennung nur soweit und nur solange in Verbindung mit Kommunikationsinhaltsdaten wie Ziel unter Wahrung der gesetzlichen Zweckbindung gespeichert, wie dies für die Sicherstellung der Betriebsfähigkeit zwingend erforderlich ist.*

Des Weiteren veröffentlicht der Hauptpersonalrat des Landes Berlin auch eine Musterdienstanweisung. Diese enthält ein weiteres Mal den Hinweis auf die nicht erlaubte private Nutzung des Internets.

Der Datenschutzbeauftragte des Landes Nordrhein-Westfalen veröffentlicht unter http://www.lfd.nrw.de/fachbereich/fach_9_1_1.html eine Orientierungshilfe für datenschutzgerechte Nutzung von E-Mail und Internetdiensten am Arbeitsplatz.

Eine weitere Musterdienstanweisung wird vom Datenschutzbeauftragten des Landes Mecklenburg-Vorpommern unter http://www.lfd.m-v.de/download/mdv_intn.html veröffentlicht.

Weitere Quellen sind <http://hagen.tbs-nrw.de/aschwerp/download/a6.pdf> (Technologieberatungstelle Südwestfalen), www.lrz-muenchen.de/~rgerling/pdf/email97.pdf (Landesrechnungszentrum München), http://home.nikocity.de/schmengler/hbv/bv/bv_net.htm (Beispiel von Uwe Schmengler) und <http://www.arbeitsrecht.de/abisz/kommentare/kommentar9.htm> (Rechtsanwalt Thomas Adam, Rechtsreferendarin Silvia Pestke, Bremen).

Weitere Quellen lassen sich sicherlich leicht im Internet finden.

Wichtig bei einer derartigen Dienstanweisung oder Betriebsvereinbarung ist jedoch, dass die Benutzer diese Anweisung gelesen, verstanden und dies auch schriftlich quittiert haben.

Um dies einwandfrei nachvollziehen zu können, sollte die Dienstanweisung für jeden Beteiligten zweimal ausgedruckt werden. Nach dem Studium der Dienstanweisung sollte diese auf der letzten Seite vom Anwender unterschrieben werden.

Hierzu kann folgender Beispieltext verwendet werden:

Kennntnisnahme

Mit meiner Unterschrift bestätige ich den Erhalt und die Kenntnisnahme dieser Dienstanweisung. Ich verpflichte mich zu deren Einhaltung. Über die von mir zu verantwortenden Sicherheitsmaßnahmen bei der Nutzung des Internet und anderer Dienste bin ich informiert. Mir ist bewußt, dass bei Verstößen gegen diese Arbeitsanweisung entsprechende Maßnahmen eingeleitet werden können.

Name:

Personalnummer:

Ort:

Datum:

Unterschrift:

