Datenschutz in der Telekommunikation

Unternehmenskommunikation im Fokus des Datenschutzes

In Unternehmen boomen neueste, höchst unterschiedliche Telekommunikationsanlagen. Diese unterliegen allesamt dem Telekommunikationsgesetz (TKG) mit seinen detaillierten Vorgaben. Aber auch das Datenschutz- und selbst das Grundgesetz gilt es in diesem Umfeld zu berücksichtigen. Was es dabei zu beachten gilt, lesen Sie auf den folgenden Seiten.

Telekommunikationsanlagen sind *„technische Einrichtungen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können“* (§ 3, Nr. 23 TKG). Im Unternehmen sind dies die Netzwerk- und Telefonverkabelung, die Telefonanlagen, die Router, Switches und WLAN-Accesspoints (aktive Netzwerkkomponenten) sowie Firewalls und E-Mailserver.

Rechtsgrundlagen – TKG, GG, StGB

Momentan ist im Telekommunikationsbereich einiges im Umbruch, da gerade nach längeren Verhandlungen im Vermittlungsausschuss das TKG novelliert wurde. Das neue TKG ist am 26.6.2004 in Kraft getreten.

Neben dem TKG gibt es an zwei weiteren Stellen wichtige den Telekommunikationsbereich betreffende Rechtsvorschriften. Im Artikel 10 des Grundgesetzes wird das Fernmeldegeheimnis unter den Schutz der Verfassung gestellt. Im § 206 StGB sind Verletzungen des Fernmeldegeheimnisses konkret mit Strafe bedroht. In den §§ 88–107 der Abschnitte „Fernmeldegeheimnis“ und „Datenschutz“ im TKG wird detailliert festgelegt, welche Telekommunikationsdaten wie und wozu verarbeitet werden dürfen. Dies sind die für den Administrator wichtigen Regeln, da sie vorgeben, was er protokollieren darf und was nicht. Hier ist die Kritik angebracht, dass die Formulierungen des Gesetzes zu „telefonlastig“ sind und das Alltagsgeschäft der IT-Administratoren zu wenig berücksichtigen.

Telekommunikations- und Tele-/Mediendienstebereich unterscheiden sich durch die Anzahl der Beteiligten

Zur Unterscheidung und zur Abgrenzung zwischen dem Telekommunikationsbereich und dem Tele-/Mediendienstebereich kann folgender Sachverhalt betrachtet werden.

Wenn **zwei** Kommunikationspartner ihre Daten über eine technische Infrastruktur austauschen, schützt die Telekommunikationsgesetzgebung die ausgetauschten Daten vor Kenntnisname durch den Betreiber der Telekommunikationsinfrastruktur bzw. es wird geregelt, welche Datenverarbeitung erlaubt ist. Es gibt drei Beteiligte: die beiden Kommunikationspartner und den Betreiber der Infrastruktur.

Die Tele-/Mediendienstegesetzgebung regelt das Angebot von Inhalten, die von **einem** Kommunikationspartner über Telekommunikationseinrichtungen abgerufen werden. Der Abrufende wird davor geschützt, dass sein Ablauf des Abrufs der Inhalte beobachtet wird. Es gibt zwei Beteiligte: den Anbieter und den Abrufenden.

Private Telefonate sind nur nach vorheriger Zustimmung bzw. im Verdachtsfall kontrollierbar.

E-Mailserver gehören zum Bereich der Telekommunikation

Auch wenn es „E-Mail schreiben“ heißt, fällt ein E-Mailserver in den Bereich der Telekommunikation. Das heißt, das Fernmeldegeheimnis ist einschlägig. Soweit eine private Nutzung der Telekommunikation im Unternehmen gestattet ist, sind die gesetzlichen Schutzvorschriften unstrittig anzuwenden. Ob die Schutzvorschriften auch beim Verbot privater Nutzung gelten, ist allerdings strittig. Hierbei ist zu bedenken, dass eine private Nutzung nur bei ausgehender Telekommunikation sinnvoll verboten werden kann, da die Beschäftigten keine Kontrolle über die eingehende Telekommunikation haben können.

Inhalte sind tabu, Verkehrsdaten nicht

Es muss zwischen den eigentlichen Inhalten – das gesprochene Wort am Telefon; Inhalt und Betreff einer E-Mail – und den näheren Umständen der Telekommunikation – beim Telefon im Wesentlichen der Einzelverbin-

```
Mar 4 15:06:13 server.testnet.de sendmail[237]: PAA00237:
from=user1@testnet.de, size=1031, class=0, pri=31031, nrcpts=1,
msgid=<200403041400.PAA00237@server.testnet.de>,
relay=root@localhost
Mar 4 15:06:13 server.testnet.de sendmail[237]: PAA00237:
to=user2@testnet.de, ctladdr=root (0/0), delay=00:06:11,
xdelay=00:00:00, mailer=local, stat=Sent
```

Das Versenden einer E-Mail erzeugt auf dem Mailserver zwei Einträge in die entsprechende Protokolldatei.

dungsnachweis; ein typisches E-Mail-Protokoll siehe S. 7 – unterschieden werden. Während der Inhalt tabu ist, kann mit den Verkehrsdaten (§ 96 TKG) eine gewisse Verarbeitung vorgenommen werden (§§ 97, 99, 100 und 101 TKG). Dabei spielen die Abrechnung (§ 97 TKG) und die Störungsbeseitigung (§ 100 Abs. 1 TKG) sowie die Missbrauchsbekämpfung (§ 100 Abs. 3 TKG) eine Rolle. Diese ist in den engen Grenzen der Paragraphen des TKG unabhängig von der Erlaubnis der Privatnutzung möglich.

Private Telefonate sind nur nach vorheriger Zustimmung bzw. im Verdachtsfall kontrollierbar

Wenn private Telefonate erlaubt sind und bezahlt werden müssen, ist die Erstellung der Abrechnung natürlich möglich. Eine Kenntnisnahme der Zielnummern der privaten Gespräche ist unzulässig. Eine Erfassung der Kosten der dienstlichen Gespräche, um sie z.B. Kostenstellen zuzuordnen, ist zulässig. Besteht der begründete Verdacht eines Missbrauchs (z.B. teure Privatgespräche werden als Dienstgespräch geführt), ist eine Kontrolle nach vorheriger schriftlicher Dokumentation zulässig (§ 100 Abs. 1 Satz 1 TKG). Kostenfreie hausinterne Telefonate dürfen nicht erfasst und ausgewertet werden.

Auch virenverseuchte Mails dürfen nicht einfach gelöscht werden

Von Viren geht eine Gefahr für das Unternehmen aus, von Spam in aller Regel nicht. Deshalb muss die Messlatte auch unterschiedlich sein. Da die Unterdrückung einer anvertrauten Sendung nach § 206 Abs. 2 Nr. 2 StGB empfindlich mit Strafe bedroht ist, sollten die eingesetzten Verfahren zur Abwehr gut überlegt sein.

Viren können zentral gescannt und anschließend gekennzeichnet werden. Aufgrund dieser Kennzeichnung kann dann der Empfänger die E-Mail löschen. Mit Einwilligung des Empfängers darf auch das Rechenzentrum löschen. Sehr elegant ist es, eine virenverseuchte E-Mail nicht anzunehmen. (Damit ist die E-Mail nicht anvertraut.) Dazu muss während des laufenden SMTP-Protokolls das Virenscannen quasi in Echtzeit erfolgen.

Spam-Mails können nur gekennzeichnet, nicht gelöscht werden

Der Umgang mit Spam-Mail ist wegen des weichen Übergangs von erwünschter zu unerwünschter E-Mail und der Nähe zur Zensur sehr viel kritischer. Deshalb bleibt bei Spam-Mail nur die zentrale Kennzeichnung der E-Mail. Hierbei sollte allerdings nicht die Betreffzeile zur Kennzeichnung benutzt werden, da dies den Inhalt der E-Mail verändert. Eine eingefügte Headerzeile erfüllt den gleichen Zweck. Alternativ kann Spam-Mail in ein separates, dem Empfänger zugängliches Verzeichnis aussortiert werden.

Idealerweise finden diese Maßnahmen auf dem Mailserver statt, damit der Download der nicht erwünschten E-Mails unterbleibt.

Betriebsvereinbarung zur Nutzung des Internets über Firewalls

Router und Firewalls „sehen“ den Datenverkehr ziemlich vollständig. Soweit Protokolle anonymisiert

Schlüssel-Faktoren

- Welche Telekommunikationsanlagen gibt es im Unternehmern?
- Wie ist der physikalische Zugriff geschützt (z.B. abgeschlossene Räume)?
- Wie sind die Zugriffsberechtigungen realisiert? Wer ist zugriffsberechtigt?
- Was wird protokolliert? Wo werden die Protokolle gespeichert? Was ist der Verwendungszweck der Protokolle?
- Was sind die Rechtsgrundlagen der Protokollierung?
- Wie sind die Löschungsfristen?

(aggregierte Daten) erstellt werden, sind sie unkritisch. Da aber häufig IP-Adressen mitprotokolliert werden und diese in vielen Fällen Personen zugeordnet werden können, sind diese Protokolle als kritisch einzustufen. Zur Firewall sollte es wegen der damit möglichen Verhaltenskontrolle eine Betriebsvereinbarung geben. Damit ist die Transparenz hergestellt.

Soweit personenbezogene Daten im Unternehmen verarbeitet werden, gehört eine Firewall grundsätzlich zu den technischen Sicherungsmaßnahmen nach § 9 BDSG. Eine Auswertung, um einen Angriff gegen das Unternehmen zu erkennen und abzuwehren, ist zulässig. Eine Erkennung von Angriffen gegen Dritte, die von eigenen Beschäftigten ausgehen, ist im Rahmen der Regelungen der Betriebsvereinbarung möglich.

Eine separate Speicherung der TK-Protokolle vereinfacht den Datenschutz der Protokollierung

Es ist unbedingt notwendig, alle Telekommunikationsdaten getrennt von anderen Daten zu halten. Während Telefonanlagen in der Regel autonom sind, ist es in der EDV üblich, alle Protokolle in einer Log-Datei zu sichern. Da dies dazu führt, dass der Schutz dieser Log-Dateien an den TK-Daten zu orientieren ist, sorgt eine separate Speicherung der TK-Protokolle hier für eine Vereinfachung. Auf alle TK-Protokolle erhalten nur wenige Personen Zugriff, und der Speicherort wird entsprechend geschützt.

Fazit: TK-Daten separat speichern und mit restriktiven Zugriffen versehen

Prüfen Sie, obTelekommunikationsdaten von anderen Daten getrennt gespeichert und der Zugriff sehr restriktiv gestaltet wird. Leider fehlt es vielen Telekommunikationsanlagen an hinreichend fein einstellbaren und damit datenschutzfreundlichen Protokollierungsoptionen.

Meist besteht nur die Wahl zwischen ein- oder ausgeschaltetem Protokoll. Hier müssen datenschutzfreundlichere Möglichkeiten Einzug halten.

Autor: Prof. Dr. Rainer W. Gerling

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