DuD
Datenschutz und Datensicherheit

IT-Sicherheit und Datenschutz

Ein Widerspruch?

Rainer W. Gerling

Während es das oberste Ziel des Datenschutzes ist, keine oder so weinig personenbezogene Daten wie möglich zu nutzen, wird den für die IT-Sicherheit Verantwortlichen unterstellt, sie seien geradezu sammelwütig, wenn es um das Speichern von Daten gehe. Im diesem Beitrag wird dieser Widerspruch weiter untersucht.[1]

Prof. Dr.
Rainer W. Gerling

Datenschutzbeauftragter der Max-Planck-Gesellschaft, Honorarprofessor für IT-Sicherheit an der FH München.
Studium der Physik an der Universität Dortmund. Promotion und Habilitation an der Universität Erlangen-Nürnberg.
E-Mail: rgerling@gmx.de

1 Datenschutz

Im BDSG wird in § 3 a ein Ziel vorgegeben, das den Geist oder die Zielvorstellungen des Datenschutzes auf vortreffliche Art vorgibt: *„Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogen Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen.“*

Eine Datenverarbeitungsanlage in der keine personenbezogenen Daten gespeichert sind, kann durch die Datenverarbeitungsvorgänge das Grundrecht auf „informationelle Selbstbestimmung“ nicht verletzen. Zudem ist zu beachten, dass das Missbrauchsrisiko umso geringer ist, desto weniger personenbezogene Daten in einem System vorhanden sind. Vor diesem Hintergrund haben sich im Laufe der Zeit etablierte Verfahren zum Umgang mit personenbezogenen Daten gebildet. Es werden für einen vorgegeben Zweck nur die Daten erhoben, die zur Zweckerfüllung erforderlich sind. Eine Speicherung von Daten, die derzeit nicht benötigt werden, für den Fall, das diese später einmal benötigt werden könnten (Vorratsdatenspeicherung), ist nicht zu lässig.

2 IT-Sicherheit

Ein IT-Sicherheitsbeauftragter muss die Sicherheit der im Unternehmen eingesetzten Datenverarbeitungsanlagen optimieren. Dazu gehört nach allgemeiner Meinung auch die Aufklärung eventueller Missbrauchsfälle. Hierzu werden Kommunikationsvorgänge protokolliert und geloggt, insbesondere wird auf Servern das Nutzungsverhalten der Benutzer gespeichert.

In der Praxis lassen sich bei manchen Verantwortlichen immer wieder „eigenartige“ Vorstellungen über Art und Umfang ihrer rechtlichen Verpflichtungen zur Speicherung und Aufbewahrung von Log-Dateien feststellen. So sind manche Verantwortliche bspw. der irrigen Meinung, sie müssten alle Daten, die von einer Strafverfolgungsbehörde in der Zukunft irgendwann einmal angefordert werden könnten, bevorraten, da sich sonst strafbar machen würden.

3 Staatliche Sammelwut

Sowohl auf europäischer Ebene[2] als auch auf deutscher Ebene[3] wird die Vorratsdatenspeicherung im Bereich der Telekommunikation heftig diskutiert und geplant. Gesetzliche Vorschriften zur Telekommunikationsüberwachung sind bereits in Kraft. Seit dem 1. Januar 2005 sind die Übergangsfristen der TKÜV abgelaufen.[4]

3.1 Telekommunikationsüberwachung

Unterstellen wir einmal, dass eine E-Mail Überwachung etwa gleich häufig angeordnet wird, wie eine Telefonüberwachung, dann erlaubt dies eine Abschätzung des anfallenden Datenvolumens. Im Jahre 2004 wurden in Deutschland ca. 34.000 Telefonüberwachungen angeordnet. Bei durchschnittlich drei E-Mails pro Tag[5] und einer Überwachungsdauer von sechs Monaten würden pro Jahr 18,6 Millionen E-Mails anfallen, die ausgewertet werden müssten. Der Techniker wird einwenden, dies sei kein Problem, weil die E-Mails als elekronische Nachrichten automatisiert verarbeitet und ausgewertet werden können. Allerdings bestehen hier bereits erhebliche Zweifel: Alle Zeitgenossen, deren Systeme trotz

[1] Schriftliche Fassung des Beitrages, den der Verfasser auf dem Symposium „Der Datenschutz - eine kulturelle Herausforderung für Europa“ anlässlich der Verabschiedung von Prof. Dr. Marie-Theres Tinnefeld von der Fachhochschule München am 15. April 2005 gehalten halt.

[2] http://www.heise.de/newsticker/meldung/55743

[3] http://www.heise.de/ct/05/08/054/

[4] http://www.bmwa.bund.de/Redaktion/Inhalte/Pdf/TKUEV1,property=pdf.pdf

[5] Ende der Schonzeit?, Interview mit eco-Vorstand Prof. M. Rotert, <kes>, Heft 1/2005, Seite 6.

```
Mar 4 15:06:13 server.testnet.de sendmail[237]: PAA00237: from=user1@testnet.de, size=1031,
class=0, pri=31031, nrcpts=1, msgid=<200503041400.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
```

Abb. 1: Das Versenden einer E-Mail erzeugt auf dem Mailserver zwei Einträge in die entsprechende Protokolldatei. Hier ist ersichtlich wer (user1@testnet.de) wem (user2@testnet.de) wann (4. März. 2005 15:06) eine wie große (1031 Bytes) E-Mail geschickt hat.

SPAM-Filter unter den belästigenden E-Mails leiden, werden nicht wirklich glauben können, dass eine derartige elektronische Vorverarbeitung wirkungsvoll ist.

3.2 Mindest-speicherungsfrist

Die Regulierungsbehörde hat zur Vorbereitung auf die „Einführung einer Mindestspeicherungsfrist für Telekommunikationsverkehrsdaten“ einen Fragebogen an die Anbieter von Telekommunikationsdiensten und an Internet Access Provider verschickt, soweit diese Dienste für die Öffentlichkeit erbringen.[6]

Interessant an diesem Fragebogen ist die Anlage zu den „*Anforderungen der Sicherheitsbehörden an Datenumfang und Mindestspeicherungsfristen für Telekommunikationsdaten*“. In der ersten Fußnote werden die Ziele deutlich: „*Für erfolgreiche Ermittlungen der Sicherheitsbehörden ist weiterhin erforderlich, dass für den Bereich des Internets die IP-Adresse einer Rufnummer oder einem sonstigen Internetzugang (etwa DSL) und in einem zweiten Schritt ebenso wie für den Bereich der Telefonie die betreffende Rufnummer einer Person zugeordnet werden kann.*“

Es entspricht aktuellen Sicherheitskonzepten, das Unternehmen und Behörden, um die Netzstruktur vor potentiellen Angreifern zu verbergen, NAT[7] einsetzen. Hierbei werden *alle* IP-Adressen aus dem internen Netz zum Zugriff auf externe Ressourcen auf *eine* IP-Adresse umgesetzt. Ohne Kenntnis der Umsetzungstabellen kann ein Zugriff auf externe Ressourcen keinem Beschäftigten zugeordnet werden. Die Übersetzungstabellen werden heute gar nicht oder nur kurzfristig gespeichert, da sie ein erhebliches Datenvolumen darstellen.

Jede Internetverbindung erzeugt einen Log-Eintrag. Da insbesondere das http-Protokoll verbindungslos ist und außerdem eine Web-Seite aus einer Vielzahl graphischer Elemente bestehen kann, erzeugt gerade das Surfen eine große Zahl von Verbindungen und damit Log-Einträgen.

Die sich aus dem Fragebogen ergebenden Zielvorstellungen werden bei dem vorgesehnen Adressatenkreis insbesondere bei den auf Sicherheit bedachten Unternehmen und Behörden ins Leere laufen. Der Internet Access Provider hat keinen Zugriff auf die Übersetzungstabellen. Auch die zweite Fußnote des Dokumentes hilft nicht weiter: „*In Fällen, in denen die vom Internet-Access-Provider ursprünglich vergebene IP-Adresse durch Proxyserver oder Anonymisierungsdienste verändert wurde und die ursprünglich vergebene IP-Adresse nicht im Header mitgeliefert wird, sollen diese Proxyserver und Anonymisierungsdienste aus fachlicher Sicht ebenfalls zur Protokollierung verpflichtet werden.*“

Um ein Gefühl für den Umfang der Vorratsdatenspeicherung in einem Unternehmen zu bekommen, betrachten wir den E-Mailverkehr einer deutschen Universität. Der E-Mail-Server hat rund 12.400 Nutzer. Im Januar 2005 wurden 5.181.938 E-Mails verschickt und 5.105.282 E-Mails empfangen[8]. (Dies entspricht über 26 E-Mails pro Tag und Benutzer: die Intensität der E-Mail Nutzung ist im wissenschaftlichen Umfeld deutlich höher als bei Normalbürgern.)

Abbildung 1 zeigt den typischen Eintrag eines Mailversandes auf einem (Unix-) Mailserver. Der Umfang variiert etwas mit unterschiedlichen Parametern (z.B. Länge der E-Mail Adresse); im Mittel sind 256 Byte ein sinnvoller Wert. Damit ergibt sich auf Basis der obigen Januar-Werte ein Volumen von ca. 30 GByte nur für die Speicherung der Verkehrsdaten des Mailservers dieser Universität pro Jahr.

Da E-Mail nicht der einzige Dienst ist, müssen auch noch Web-Proxies, News-Server, Chat-Server sowie Firewalls betrachtet werden.

4 Lösung des Dilemmas

In einem Unternehmen dürfen alle die Daten gespeichert werden, die zur Aufrechterhaltung der IT-Sicherheit und zur Fehlersuche benötigt werden. Im Bereich der Telekommunikation ergib sich die Rechtsgrundlage aus §100 TKG. Bei der Auslegung des Begriffs „erforderlich“ sind strenge Maßstäbe anzulegen. Auf keinen Fall ist es zulässig, Daten zu speichern, die man „eventuell irgendwann einmal“ benötigt.

Bei der Fehlersuche auf einem Mail-Server reicht z.B. eine Speicherdauer von wenigen Tagen. Kein Nutzer geht nach einigen Monaten zum Administrator des Mail-Servers und beschwert sich, dass eine E-Mail nicht angekommen ist. Eine Speicherfrist von ein bis zwei Wochen ist, wie das Beispiel illustriert, völlig ausreichend.

Fazit

IT-Sicherheit und Datenschutz sind bei sachgerechter Anwendung der Protokollierung (Erforderlichkeit = Daten werden tatsächlich benötigt) kein Widerspruch.

Die Sicherheitsbehörden tendieren jedoch dazu mit der Begründung einer Bekämpfung von Terrorismus und Schwerstkriminalität dazu, umfangreichste Datenfriedhöfe zu fordern und damit der Wirtschaft Kosten auszubürden. Sie sollten sich hierbei aber einem Bild des amerikanischen Sicherheitsexperten Bruce Schneier über Sinn und Unsinn einer derartigen Sammelwut nicht verschließen. „*Wer eine Nadel im Heuhaufen sucht, sollte nicht den Heuhaufen vergrößern, sondern den Suchalgorithmus optimieren.*“[9]

[6] http://www.heise.de/newsticker/meldung/58509

[7] Network Address Translation, RFC 2663 http://www.ietf.org/rfc/rfc2663.txt

[8] Private Mitteilung des Administrators des E-Mail-Servers.

[9] Nach: Schneier, Bruce, *Beyond Fear*, Copernikus Books, 2003.