



Merkblatt: Übermittlung von Daten an Strafverfolgungsbehörden

Missbräuchliche Internetnutzung

Beim Einsatz der IT-Systeme der RUB sind einschlägige Gesetze, Vorschriften und Dienstvereinbarungen einzuhalten. Diese regeln unter anderem die Bereitstellung von Daten unter Gesichtspunkten des Datenschutzes, des Urheber- und Markenrechts und belegen die Verbreitung oder Verschaffung rechtswidriger Inhalte mit Strafe.

Besteht der Verdacht, dass IT-Systeme der Ruhr-Universität missbräuchlich genutzt werden, so sind keine Ermittlungen auf eigene Faust anzustellen, sondern

- es sollten Beweise gesichert werden (Ausdruck und Speicherung der Dateien, Ermittlung von Zeugen etc.).
- der Verstoß ist zeitnah zu melden, damit die Daten entfernt oder der Zugang zu ihnen gesperrt werden kann. Dies ist insbesondere besonders dann wichtig, wenn auf IT-Systemen gespeicherte personenbezogene Daten oder urheberrechtlich geschützte Inhalte von Unberechtigten eingesehen werden können oder rechtswidrige Inhalte auf IT-Systemen der RUB abgelegt sind oder über diese verbreitet werden.
- bei der Meldung sind die offiziellen Meldewege einzuhalten. Eine Beschreibung der Meldewege findet sich unter der am Ende angegebenen Internetadresse.

Vorgehensweise bei Auskunftersuchen Dritter

Häufig werden Auskunftersuchen an Einrichtungen der Ruhr-Universität gerichtet, um Informationen über Benutzer des Internets zu ermitteln. Dabei müssen die datenschutzrechtlichen Belange der Hochschulangehörigen berücksichtigt werden. Grundsätzlich sind ausschließlich Strafverfolgungsbehörden befugt, derartige Auskünfte unter bestimmten gesetzlichen Vorgaben einzuholen.

Werden Anfragen von Sicherheitsbehörden gestellt, so sollte nicht übereilt gehandelt werden und die folgenden Leitlinien berücksichtigt werden:

- **Die Übermittlung von Daten ist mit der IT-Sicherheitsbeauftragten der RUB abzustimmen. Diese wird gegebenenfalls das Justizariat und den Datenschutzbeauftragten einschalten.**
- Erfolgt das Auskunftersuchen telefonisch, so sollte um eine schriftliche Bestätigung der Anfrage gebeten werden. Dies dient in erster Linie dazu, im nach hinein Vorwürfe über datenschutzrechtliche Verstöße von Seiten der Nutzer auszuräumen.
- In der Anfrage muss die Rechtsgrundlage für die Auskunft genannt sein. Daraus ergibt sich, welche Daten überhaupt übermittelt werden dürfen (siehe unten).
- Vorhandene Daten sollten gesichert und nicht gelöscht werden.
- Gegenüber den betroffenen Nutzern und Dritten ist Stillschweigen zu wahren.

Rechtsgrundlagen

Bei Auskunftersuchen der Strafverfolgungsbehörden ist zwischen Bestands-, Verbindungsdaten

und Inhalten der Kommunikation zu unterscheiden:

- Bestandsdaten sind personenbezogene Daten wie Name und Anschrift eines Benutzers oder fest vergebene IP-Adressen. Gemäß § 113 TKG (Telekommunikationsgesetz) besteht eine Auskunftspflicht gegenüber den Ermittlungsbehörden auch ohne vorherige richterliche Anordnung, soweit dies zur Verfolgung von Straftaten, Ordnungswidrigkeiten oder zur Gefahrenabwehr erforderlich ist. Benutzern darf gemäß §113 TKG nicht mitgeteilt werden, dass eine Auskunftserteilung stattgefunden hat. Ergänzend sind gemäß § 161 StPO alle öffentlichen Einrichtungen bei staatsanwaltlichen Ermittlungen verpflichtet auf Verlangen Bestandsdaten an die Strafverfolgungsbehörden zu übermitteln.
- Verbindungsdaten sind Daten, die bei der Bereitstellung und Erbringung eines Dienstes erhoben werden. Beispielsweise Zeitpunkt des Beginns oder Endes einer Internetverbindung oder dynamisch vergebene IP-Adressen. Nach § 100 g StPO können Strafverfolgungsbehörden über einen Kommunikationsvorgang Auskunft verlangen. Es muss eine schriftliche richterliche Anordnung oder bei Gefahr im Verzug eine staatsanwaltliche Anordnung vorgelegt werden.
- Inhalte der Kommunikation beispielsweise Inhalte von Emails unterliegen dem Fernmeldegeheimnis. Wichtigste Rechtsgrundlage für eine Überwachung und Aufzeichnung der Inhalte einer Telekommunikation wird durch §100a StPO begründet. Die formale Voraussetzung für ein Auskunftersuchen setzt den konkreten Verdacht einer schweren Straftat voraus. Es muss ferner eine schriftliche richterliche Anordnung oder bei Gefahr im Verzug eine staatsanwaltliche Anordnung vorgelegt werden.

Welche Speicherpflicht besteht?

Es besteht *keine generelle Pflicht zur Erhebung und Speicherung von Daten* für eine mögliche Auskunftserteilung an Strafverfolgungsbehörden. § 111 TKG begründet nur eine Speicherpflicht für Rufnummern bei Telekommunikationsanbietern. Jedoch werden aus eigenem Interesse Bestandsdaten nach § 95 TKG zulässigerweise gespeichert, die nach § 113 TKG von Strafverfolgungsbehörden angefragt werden können. Die Speicherung von Verkehrsdaten unterliegen nach § 96 ff. TKG erheblichen Auflagen. Diese ist nur erlaubt, wenn sie aus technischen oder organisatorischen Gründen, zur Erhebung und zum Nachweis von Entgelten, zur Störungsbeseitigung oder zur Missbrauchsaufklärung unbedingt erforderlich ist. Bei der Erhebung, Speicherung und Verarbeitung von personenbezogenen Daten sind die datenschutzrechtlichen Bestimmungen einzuhalten (DSG NRW (Datenschutzgesetz Nordrhein-Westfalen), §§ 91ff. TKG) und der örtliche Datenschutzbeauftragte ist zu beteiligen. Erst nach einer richterlichen Anordnung besteht im Einzelfall eine Pflicht zur Vorratsdatenhaltung für die Übermittlung an Sicherheitsbehörden.

Referenzen:

„Internetrecht“, Prof. Dr. Thomas Hoeren, Universität Münster
<http://www.uni-muenster.de/Jura.itm/hoeren/INHALTE/lehre/lehrematerialien.htm>

Forschungsstelle Recht des DFN
<http://www.dfn.de/content/de/beratung/rechtimdfn/>

Meldewege: <http://www.ruhr-uni-bochum.de/itsb/Meldewege.htm>

Kontakt:

Brigitte Wojcieszynski, Stabsstelle IT-Sicherheit, Tel.: 23409,

E-Mail: itsb@rub.de

Anja John, Ass.‘in jur., Justizariat der Ruhr-Universität, Tel.: 22932,

E-Mail: Anja.John@uv.rub.de