Münster, den 31. Oktober 2012

Sehr geehrter Herr Speer,

vielen Dank für Ihre Anfrage und das damit der Forschungsstelle Recht im DFN entgegengebrachte Vertrauen. Vorab müssen wir Sie darauf hinweisen, dass wir eine Haftung für gegebene Hinweise nicht übernehmen können.

Gerne geben wir aber eine allgemeine Stellungnahme zu der von Ihnen aufgeworfenen Frage ab, ob im Zuge der Erneuerung eines netzwerkbasierten Intrusion Prevention Systems (IPS) im Netz der Westfälischen Wilhelms-Universität Münster (WWU) und im Netz des Universitätsklinikums Münster (UKM) die Stellungnahme von Januar 2006 mit der geplanten Erneuerung des IPS weiterhin als Grundlage für die Betriebsrahmenbedingungen betrachtet werden kann.

I. Sachverhalt

Im Netz der Westfälischen Wilhelms-Universität Münster (WWU) und im Netz des Universitätsklinikums Münster (UKM) soll eine Erneuerung eines netzwerkbasierten Intrusion Prevention Systems (IPS) vorgenommen werden. Dabei soll das vorhandene System (Produktfamilie "McAfee Intrushield") durch die "Stonegate" Produktfamilie des Herstellers Stonesoft ersetzt werden. Bei der Einführung des vorhandenen Systems wurde eine Stellungnahme der Forschungsstelle Recht im DFN von Januar 2006 als Grundlage für die Betriebsrahmenbedingungen betrachtet.

Es stellt sich nun die Frage, ob diese Stellungnahme von Januar 2006 im Hinblick auf die aktuelle Gesetzgebung und Rechtsprechung mit der geplanten Erneuerung des IPS weiterhin als Grundlage für die Betriebsrahmenbedingungen betrachtet werden kann.

II. Ergebnis

Die Stellungnahme aus dem Jahre 2006 bedarf nur in wenigen Punkten einer Aktualisierung.

Der Einsatz eines IPS ist grundsätzlich zulässig. Handelt es sich bei den abgefangenen Datenströmen um solche mit derartig schädigenden Inhalten, dass sie das TK-/IT-System der Hochschule tatsächlich negativ beeinflussen können, so ist eine Rechtfertigung eines Eingriffs in das Fernmeldegeheimnis gem. § 88 Abs. 3 S. 3 Telekommunikationsgesetz (TKG) i.V.m. § 100 Abs. 1 TKG mit Hilfe sogenannter Intrusion Prevention Systeme zu bejahen.

Eine anlassbezogene Speicherung von Verkehrsdaten ist für den Zeitraum der Abwehr- und Bearbeitungsmaßnahmen durch § 100 Abs. 1 TKG legitimiert, wohingegen bei einer anlasslosen Speicherung von Verkehrsdaten eine Speicherdauer von bis zu sieben Tagen angemessen zu sein scheint.

Im Hinblick auf den Personalrat ergibt sich eine Mitbestimmungspflicht aus § 72 Abs. 3 Nr. 1, 2 und 5 LPVG NRW, wenn die Änderung des IPS den jeweiligen speziellen Tatbestand erfüllt.

III. Rechtliche Begutachtung

Im Rahmen einer rechtlichen Begutachtung sind vor allem das Fernmeldegeheimnis, das Datenschutzrecht und die Einschaltung der Personalvertretung von Bedeutung.

1. Einordnung der Hochschulen

Die Hochschulen bieten ihren Nutzern einen kostenlosen Internetzugang und einen E-Mail-Account an, wobei die private Nutzung grundsätzlich nicht untersagt ist. Durch die Gestattung der privaten Kommunikation und Internetnutzung (die Duldung der privaten Nutzung steht dieser gleich) treten die Hochschulen den Nutzern gegenüber als Anbieter von Telekommunikationsdiensten auf, da sie damit den Internetzugang für fremde Zwecke zur Verfügung stellen (vgl. § 3 Nr. 6 TKG). Ihre Stellung ist dabei vergleichbar mit der Leistung eines Access-Providers gegenüber seinen Kunden. Durch diese Einordnung der beteiligten Hochschulen als Diensteanbieter im Sinne des Telekommunikationsgesetzes müssen sie die

datenschutzrechtlichen Verpflichtungen des Telekommunikationsgesetzes (TKG) und ggf. auch des Telemediengesetzes (TMG) beachten.

2. Fernmeldegeheimnis

Nach § 109 Abs. 1 TKG bzw. des inhaltsgleichen § 10 Datenschutzgesetz NRW (DSG NRW) ist jeder Diensteanbieter dazu verpflichtet, die erforderlichen technischen Vorkehrungen und sonstigen Maßnahmen zum Schutz des Fernmeldegeheimnisses (§ 88 TKG) und gegen die Verletzung des Schutzes personenbezogener Daten zu treffen. Hierunter kann auch die Filterung oder Unterdrückung von Datenströmen und Inhalten fallen, wenn diese eine Störung oder einen Schaden in dem TK-/IT-System des Empfängers auslösen können. Ziel der Vorschrift ist es, den Betrieb eigener Kommunikationssysteme von äußeren und inneren Einflüssen freizuhalten, ohne dafür das Einverständnis vom Betroffenen einholen zu müssen. Durch das Filtern bzw. die Unterdrückung von schädlichen Datenströmen wird die Gefahr stark reduziert, dass die Netzwerkperformance des TK-/IT-Systems der Hochschule reduziert oder vollständig gehemmt wird. Beim IPS handelt es sich um eine technische Vorkehrung im Sinne dieser Vorschrift. Darunter sind nämlich alle Maßnahmen zu verstehen, die sich auf die Funktionsweise der technischen Einrichtung beziehen. Dazu gehört auch die Überwachung des eigenen Netzes mittels IPS auf verdächtige Muster (Signaturen) im IP-Verkehr, die auf einen Hacker-Angriff aus dem äußeren Netz (oder innerhalb des eigenen Netzes), Spyware, Würmer oder Peer-to-Peer Programme hindeuten. Der Einsatz dieser Systeme ist damit grundsätzlich zulässig.

Durch die Einordnung als Diensteanbieter im Sinne des Telekommunikationsgesetzes ergibt sich darüber hinaus die Besonderheit für eine Hochschule, dass auch sie zum grundrechtlichen Schutz des Fernmeldegeheimnis verpflichtet ist (§ 88 TKG). Diesen Diensteanbietern ist es nach § 88 Abs. 3 S. 1 TKG untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Das Fernmeldegeheimnis schützt dabei die Vertraulichkeit der unkörperlichen Übermittlung von Informationen an individuelle Empfänger. Nach § 88 Abs. 1 S. 1 TKG unterliegen dem Fernmeldegeheimnis der Inhalt der

Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Darüber hinaus erstreckt sich das Fernmeldegeheimnis auch auf die näheren Umstände erfolgloser Verbindungsversuche (§ 88 Abs. 1 S. 2 TKG). Das Fernmeldegeheimnis wird schon durch die bloße Kenntnisnahme der Umstände oder des Inhalts der Kommunikation verletzt. Geschützt ist die Kommunikation unabhängig von ihrem Inhalt.

Der Zugriff in Form der Informationserhebung darüber, mit welcher IP-Adresse zu welchem Zeitpunkt etwa eine Peer-to-Peer-Plattform angesteuert wurde oder Würmer bzw. Spyware in das System gelangten, betrifft nähere Umstände eines Kommunikationsvorganges und fällt damit unter das Fernmeldegeheimnis. Eine Kenntnisnahme über das erforderliche Maß hinaus ist wie oben erwähnt nach § 88 Abs. 3 S. 1 TKG unzulässig. Es kann damit zwar zum Schutz der Systeme eine Einschränkung des Fernmeldegeheimnisses vorgenommen werden, allerdings unterliegt diese einer strengen Zweckbindung und darf nur bei absoluter Erforderlichkeit angewandt werden.

Im Zusammenhang mit dem Fernmeldegeheimnis ist hervorzuheben, dass die Einsichtnahme in den Inhalt der Kommunikation (z. B. Inhalt von E-Mails, Inhalte von VoIP-Gesprächen) wegen der Intensität des Eingriffs nur dann in Betracht kommen kann, wenn eine Störung von einiger Erheblichkeit vorliegt, kein anderes Mittel zur Behebung der Störung in Betracht kommt und die Einholung einer Einwilligung bei den Betroffenen nicht möglich ist. Die Betroffenen sind in diesem Fall jedoch sobald als möglich hierüber zu informieren. Die genannten Voraussetzungen sind eng zu interpretieren. Eine Einsichtnahme ohne Einwilligung der Betroffenen kann daher nur als allerletztes Mittel in Erwägung gezogen werden kann.

Eingriffe in den Schutzbereich des Fernmeldegeheimnisses könnten aber gerechtfertigt sein. Als Rechtfertigung für Eingriffe in das Fernmeldegeheimnis kommen jedoch nur Erlaubnissätze in Betracht, die in einer gesetzlichen Vorschrift niedergelegt sind und sich ausdrücklich auf TK-Vorgänge beziehen (vgl. § 88 Abs. 3 S. 3 TKG). Als ein solcher Rechtfertigungsgrund kommt insbesondere die Vorschrift des § 100 Abs. 1 TKG in Betracht. Danach darf der Diensteanbieter zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen die Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer erheben und verwenden, soweit dies erforderlich ist. Demzufolge ist

eine Einsichtnahme in den Kommunikationsvorgang zur Gefahrenabwehr dann zulässig, wenn es hierzu einen konkreten Anlass gibt. Dies wird in der Regel die entsprechend voreingestellte Warnmeldung des IPS sein im Hinblick auf schädliche Inhalte. Warnt das IPS dagegen auch bei objektiv ungefährlichen Datenströmen oder unschädlichen Inhalten, ist die notwendige Erforderlichkeit nicht gegeben und der Eingriff in das Fernmeldegeheimnis damit unzulässig.

3. Datenschutz

Datenschutzrechtlich relevant wird die Nutzung des IPS dann, wenn personenbezogene Daten betroffen sind. Dies ist bei einer Erhebung, Verarbeitung oder Nutzung von Daten der Fall. Das IPS speichert zu keinem Zeitpunkt den Namen des Nutzers bzw. des Nutzer-Rechners oder vergleichbare „klassische“ personenbezogene Daten. Lediglich die IP-Adressen von Quelle und Ziel des abgefangenen Datenstroms werden mit Datum und Uhrzeit registriert. Bei diesen handelt es sich einerseits um dynamische IP-Adressen und andererseits um statische IP-Adressen. Im Rahmen der dynamischen IP-Adressen kann ein tatsächlicher Personenbezug nur über die Verbindung mit den Login-Daten und eines Zeitstempels hergestellt werden. Anders ist dies bei statischen IP-Adressen, die bestimmten Rechnern dauerhaft zugewiesen sind. Die Login-Daten, die bei dynamischen IP-Adressen zur Ermittlung der tatsächlichen Person erforderlich sind, befinden sich in einem anderen System.

Personenbezogene Daten i. S. d. Datenschutzgesetzes sind solche Daten, die Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person enthalten (§ 3 Abs. 1 Bundesdatenschutzgesetz (BDSG)). Bei statischen IP-Adressen handelt es sich unproblematisch um personenbezogene Daten. Aber auch dynamische IP-Adressen sind als personenbezogene Daten anzusehen. Die Information, dass der Nutzer einer bestimmten IP-Adresse zu einer bestimmten Zeit bestimmte Inhalte angerufen hat, stellt eine solche Einzelangabe über den Nutzer dar. Die Person des Nutzers kann anhand der Merkmale IP-Adresse und Uhrzeit mit Hilfe der Login-Daten bestimmt werden. Entscheidend ist insoweit die abstrakte Möglichkeit einer Verknüpfung der Verbindungsdaten mit den „klassischen“ personenbezogenen Daten (z.B. des Namens).

Während diese Möglichkeit für außenstehende Dritte i. d. R. nicht besteht, kann die Hochschule als Provider die Verknüpfung herstellen. Die Erschwerung der Ermittlung der natürlichen Person durch rein organisatorische Hindernisse hat keine Auswirkungen auf die Eigenschaft der dynamischen IP-Adressen als personenbezogene Daten. Kürzlich hat der Bundesgerichtshof in einem Urteil festgestellt, dass es sich bei dynamischen IP-Adressen um Verkehrsdaten handelt (Beschluss v. 19.04.2012, Az. I ZB 80/11). Nach § 3 Nr. 30 TKG sind dies solche Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden. Diese Einordnung hat aber nicht zur Konsequenz, dass es sich bei dynamischen IP-Adressen nicht mehr um personenbezogene Daten handelt. Vielmehr sind dynamische IP-Adressen Verkehrsdaten im Sinne des Telekommunikationsgesetzes und gleichzeitig personenbezogene Daten im Sinne der Datenschutzgesetze.

Die Speicherung der IP-Adresse im Zusammenhang mit dem Zeitpunkt der Verwendung stellt damit eine datenschutzrechtlich relevante Handlung dar. Dies hat zur Folge, dass die Universität Münster durch den Einsatz des IPS an die Vorgaben des Datenschutzrechts gebunden ist, sofern sie IP-Adressen im Zusammenhang mit dem Zeitpunkt der Nutzung speichert.

a. Anlassbezogene Speicherung

Der Diensteanbieter darf nach § 96 Abs. 1 TKG für bestimmte Zwecke Verkehrsdaten erheben. Diese Zwecke liegen vor allem im Bereich der Entgeltabrechnung für erbrachte Telekommunikationsdienste. Eine über § 96 Abs. 1 TKG hinausgehende Erhebung oder Verwendung der Verkehrsdaten ist nach der spezialgesetzlichen Datenschutzregelung in § 96 Abs. 2 TKG zunächst unzulässig. Einen Erlaubnistatbestand hierfür stellt jedoch § 100 Abs. 1 TKG dar. Danach ist die Erhebung und Verwendung von Verkehrsdaten der Teilnehmer und Nutzer zum Erkennen, Eingrenzen und Beseitigen von Störungen bis zur Grenze der Erforderlichkeit zulässig. Entscheidend ist daher, dass eine Speicherung nur dann erfolgt, wenn tatsächlich ein konkreter Anlass dafür besteht, dass dem System Gefahr droht. Denn nur in diesem Fall ist die vom Gesetz geforderte „Erforderlichkeit“ gegeben.

Liegt eine konkrete Gefahr vor und bedarf die Abwehr einer weiteren Bearbeitung, so ist die Speicherung der entsprechenden Daten auch über die normale Lebensdauer der Verkehrsdaten hinaus zulässig. Wie lange die normale Speicherung der Verkehrsdaten zulässig ist, hängt davon ab, wie viel Zeit tatsächlich erforderlich ist, um entsprechende Überprüfungen der Vorgänge durchzuführen. Dies wird in der Regel einen Zeitraum von wenigen Tagen umfassen.

Sobald das IPS ein Protokoll für eine Peer-to-Peer-Verbindung oder einen anderen objektiv ungefährlichen Datenstrom anfertigt, obwohl für das System keine konkrete Gefahr besteht, wird dies vom Erlaubnistatbestand des § 100 Abs. 1 TKG nicht mehr umfasst sein. Die Datenspeicherung wäre damit in diesem konkreten Fall unzulässig. Daher sind die erhobenen Daten unverzüglich wieder zu löschen, wenn keine Störungen oder Fehler auftraten. Die Voreinstellungen bei der Verwendung von IPS sind demzufolge so vorzunehmen, dass eine Protokollierung nur bei tatsächlich gefährlichen Datenströmen erfolgt.

b. Anlasslose Speicherung

Setzt man voraus, dass die Speicherung zur Erreichung des angestrebten Zweckes notwendig ist, so stellt sich im Weiteren die Frage, wie lange Verkehrsdaten anlasslos gespeichert werden dürfen. Stellt der Diensteanbieter das Vorliegen eines Fehlers oder einer Störung fest, so darf er die Verkehrsdaten wie soeben erwähnt speichern und verwenden, bis der Fehler oder die Störung behoben ist. Zur Speicherdauer bei der sogenannten anlasslosen Speicherung, also der Speicherung um Fehler oder Störungen erst zu erkennen, hat sich zu Beginn des Jahres 2011 der Bundesgerichtshof (BGH) geäußert (Urteil v. 13.01.2011, Az. III ZR 146/10). In dem zugrunde liegenden Verfahren ging es um die Speicherdauer in Bezug auf die Speicherung von IP-Adressen. Es ist allerding zu berücksichtigen, dass in diesem Verfahren kein Urteil über die Speicherfrist gefällt wurde. Das Verfahren wurde vielmehr an das Oberlandesgericht Frankfurt a. M. zurückverwiesen. Nach Meinung des BGH scheint allerdings eine Speicherdauer von bis zu sieben Tagen angemessen zu sein. Eine längere Speicherdauer ist darüber hinaus möglich, muss aber im Einzelfall begründet werden. An diese Begründung im Einzelfall sind aufgrund des Eingriffs in das Fernmeldegeheimnis hohe

Anforderungen zu stellen. Diese Beurteilung der Rechtslage ist jedoch zurzeit – wie soeben bereits ausgeführt worden ist – noch nicht durch höchstrichterliche Rechtsprechung belegt.

4. Personalvertretung

Zuletzt ist noch das Personalvertretungsgesetz für das Land Nordrhein-Westfalen zu beachten. In § 72 Abs. 3 LPVG NRW sind einige beteiligungspflichtige Fälle in Rationalisierungs-, Technologie- und Organisationsangelegenheiten angeführt, in denen der Personalrat mitzubestimmen hat, soweit eine gesetzliche oder tarifliche Regelung nicht besteht.

Zunächst ist § 72 Abs. 3 Nr. 1 LPVG NRW zu nennen, der sich mit der Einführung, Anwendung, wesentlichen Änderung oder wesentlichen Erweiterung von automatisierter Verarbeitung personenbezogener Daten der Beschäftigten außerhalb von Besoldungs-, Gehalts-, Lohn-, Versorgungs- und Beihilfeleistungen sowie Jubiläumszuwendungen befasst. Wie oben geschildert werden im Zuge eines IPS personenbezogene Daten automatisch verarbeitet. Sobald durch die Erneuerung dieses Systems eine wesentliche Änderung bzw. wesentliche Erweiterung dieser Verarbeitung erfolgt, ist eine Personalratsanhörung erforderlich.

Nach § 72 Abs. 3 Nr. 2 LPVG NRW hat der Personalrat mitzubestimmen bei der Einführung, Anwendung und Erweiterung technischer Einrichtungen, es sei denn, dass deren Eignung zur Überwachung des Verhaltens oder der Leistung der Beschäftigten ausgeschlossen ist. Sobald also durch die Auswertung der vom System festgestellten Daten in irgendeiner Weise eine Überwachung der Beschäftigten möglich erscheint, ist der Personalrat im Voraus bei der Änderung des Systems anzuhören.

Schließlich besteht noch nach § 72 Abs. 3 Nr. 5 LPVG NRW eine Beteiligungspflicht des Personalrates bei der Einführung, wesentlichen Änderung oder wesentlichen Ausweitung betrieblicher Informations- und Kommunikationsnetze. Sollte die Umstellung auf das neue IPS eine deutliche Änderung bzw. Ausweitung der Arbeitsweise des Systems bedeuten, ist auch aufgrund dieser Vorschrift der Personalrat im Voraus anzuhören.

Ich hoffe, dass wir Ihnen mit dieser Stellungnahme weiterhelfen konnten. Für weitere Fragen stehen meine Kollegen und ich Ihnen gerne zur Verfügung.

Mit freundlichen Grüßen

Kevin Kuta

Forschungsstelle Recht im Deutschen Forschungsnetz