„Intrusion Prevention“ an Hochschulen

Die Intrusion-Prevention-Systeme (IPS) der Firma McAfee sollen als Teil des umfassenden Sicherheitssystems für die Universität Münster eingesetzt werden. Durch diese Systeme sollen Angriffe durch Würmer, Viren, Trojaner, Denial-of-Service-Attacken usw. die zu erheblichen Störungen der IT der Universität, zu Schädigungen der Rechnerkonfigurationen sowie Datenverfälschungen und -verlusten führen können, abgewehrt werden.

Hierzu lesen die Systeme den Datenverkehr mit und überprüfen ihn auf vorgegebene Muster und Signaturen, um bekannte Angriffe abwehren zu können. Die Signaturen werden fortlaufend aktualisiert. Darüber hinaus ermöglichen eine intelligente Protokollanalyse und verhaltensbasierte Algorithmen auf Applikationsebene, weitere, bisher noch nicht bekannte Angriffsformen zu erkennen und abzuwehren.

Es sind zwei Arten von IPS zu unterscheiden, netzwerkbasierte und Host-basierte Lösungen. Letztere werden auf potentiell gefährdeten Systemen wie Servern oder Notebooks installiert. Im Datennetz der Universität Münster sind bisher nur netzwerkbasierte IPS im Einsatz, die an genau auszuwählenden Stellen im Netzwerk integriert werden. Die Lösung von McAfee gestattet dabei die Administration über ein gemeinsames Managementsystem.

In einem ersten Arbeitsschritt findet der Abgleich der Signaturen innerhalb des Systems statt. Erkennt das System insoweit eine Besonderheit, die auf einen schädlichen Angriff hinweist, zeigt es diese an und erstellt ein Protokoll, aus dem ersichtlich wird, welche IP-Adressen zu welchem Zeitpunkt an welchem gefährlichen Datentransfer beteiligt waren. Das Protokoll ermöglicht anschließend eine Analyse der aufgetretenen Warnung und ggf. ein Einschreiten seitens der Systemadministration.

Nach einer zuvor festgelegten Zeitdauer – in der Regel reichen hier wenige Tage – werden die Protokolle automatisch vollständig gelöscht.

Fraglich ist, in welchem Umfang und ggf. mit welchen Einschränkungen bzw. Dienstanweisungen „Intrusion Prevention“ für das Uni-Netz an der Hochschule eingesetzt werden kann.

1. Datenschutz

Datenschutzrechtlich relevant wird die Nutzung des Programms dann, wenn personenbezogene Daten erhoben, d.h. in irgendeiner Form gespeichert werden. Das Programm speichert zu keinem Zeitpunkt den Namen des Nutzers/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, bei denen ein tatsächlicher Personenbezug nur über die Verbindung mit den „Login“-Daten hergestellt werden kann und andererseits um feste IP-Adressen, die bestimmten Rechnern dauerhaft zugeteilt sind. Die Login-Daten zur Ermittlung der tatsächlichen Person befinden sich in einem anderen und unter normalen Umständen nicht verknüpfbaren System.

Fraglich ist damit, ob es sich auch bei den dynamischen IP-Adressen um personenbezogene Daten handelt. 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 BDSG). 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, der anhand der Merkmale Uhrzeit und IP-Adresse mit Hilfe der „Login“-Daten bestimmt werden kann. Entscheidend ist insoweit die abstrakte Möglichkeit einer Verknüpfung der Verbindungsdaten mit den „klassischen“ personenbezogenen Daten (z.B. der Name). Während diese Möglichkeit für außen stehende Dritte i. d. R. nicht besteht, kann die Hochschule als Provider die Verknüpfung herstellen. Zumindest für die Hochschule selbst ist die dynamische IP-Adresse eines damit ein personenbezogenes Datum (vgl. hierzu etwa *Roßnagel*, Recht der Multimediadienste, § 1 TDDSG Rn. 35 f.).

Wenn die Ermittlung der natürlichen Person durch rein organisatorische Hindernisse erschwert ist, hat das keine Auswirkungen auf die Eigenschaft als personenbezogenes Datum. Es ist daher bei einer dynamischen IP-Adresse von einem personenbezogenen Datum auszugehen.

Das Speichern der IP-Adresse im Zusammenhang mit dem Zeitpunkt der Verwendung stellt damit eine datenschutzrechtlich relevante Handlung dar.

Dies hat zur Folge, dass die Hochschule als Benutzerin des Programms „Intrusion Prevention“ an die Vorgaben des Datenschutzrechts gebunden ist, sofern sie IP-Adressen im Zusammenhang mit dem Zeitpunkt der Nutzung speichert.

Das Speichern der vom Programm ermittelten Verkehrsdaten über die Dauer der Verbindung hinaus ist nach der spezialgesetzlichen Datenschutzregelung in § 96 Abs. 2 TKG zunächst unzulässig. Einen Erlaubnistatbestand hierfür stellt jedoch § 100 Abs. 1 TKG dar, wonach die Erhebung und Verwendung von Verkehrsdaten zum Erkennen, Eingrenzen und Beseitigen von Störungen bis zur Grenze der Erforderlichkeit zulässig ist. Entscheidend ist daher, dass eine Speicherung nur dann erfolgt, wenn tatsächlich ein konkreter Anlass dafür besteht, dass dem System Gefahr droht, da nur dann eine „Erforderlichkeit gegeben ist.

Sollte das IPS auch dann ein Protokoll anfertigen, wenn es etwa eine P2P-Verbindung oder einen anderen objektiv ungefährlichen Datenstrom aufspürt, obwohl für das System keine konkrete Gefahr besteht, wird dies vom Erlaubnistatbestand des § 100 Abs. 1 TKG nicht mehr umfasst sein. Diese Datenspeicherung wäre damit unzulässig. Die Voreinstellungen bei der Verwendung von IPS sind daher so vorzunehmen, dass eine Protokollierung nur bei tatsächlich gefährlichen Datenströmen erfolgt.

Liegt dagegen eine konkrete Gefahr vor und bedarf die Abwehr einer weiteren Bearbeitung, so ist es dann zulässig, die entsprechenden Daten auch über die normale Lebensdauer der Protokolldaten hinaus zu speichern. In einem solchen Fall kann dann etwa eine Kopie angefertigt werden, bevor das betreffende Protokoll turnusmäßig gelöscht wird. Wie lange die normale Speicherung der Protokolldaten 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.

2. Fernmeldegeheimnis

Als Anbieterin von Telekommunikationsdienstleistungen i. S. d. TKG ist die Hochschule zur Einhaltung des Fernmeldegeheimnisses aus Art. 10 GG, das in § 88 TKG konkretisiert wird, verpflichtet. Dieses umfasst gem. § 88 Abs. 1 TKG den Inhalt der Kommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Kommunikationsvorgang

beteiligt ist oder war. Darüber hinaus erstreckt sich das Fernmeldegeheimnis auch auf die näheren Umstände erfolgloser Verbindungsversuche.

Die Information, darüber, mit welcher IP-Adresse zu welchem Zeitpunkt etwa eine Peer-to-Peer-Plattform angesteuert wurde, betrifft nähere Umstände eines Kommunikationsvorganges und fällt damit unter das Fernmeldegeheimnis. Gem. § 88 Abs. 3 TKG ist es dem Diensteanbieter untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung ihrer Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis zu verschaffen. 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 (vgl. hierzu Beck'scher TKG-Kommentar 2. Aufl. 2000, § 85 Rn. 5). Damit gilt insofern das oben gesagte: eine Einsichtnahme in den Kommunikationsvorgang ist zur Gefahrenabwehr dann zulässig, wenn es hierzu einen konkreten Anlass gibt. Dies wird in der Regel die entsprechend voreingestellte Warnmeldung des IPS sein. Warnt das IPS dagegen auch bei objektiv ungefährlichen Datenströmen (z.B. Peer-to-Peer) ist keine Erforderlichkeit gegeben und der Eingriff in das Fernmeldegeheimnis damit unzulässig.

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 sobald als möglich hierüber zu informieren. Die genannten Voraussetzungen sind eng zu interpretieren, so dass eine Einsichtnahme ohne Einwilligung der Betroffenen nur als allerletztes Mittel in Erwägung gezogen werden kann.

Münster, den 27.01.2006
Forschungsstelle Recht im DFN