International Working Group
on Data Protection
in Telecommunications

675.41.20 7. September 2010

Arbeitspapier zur Nutzung von Deep Packet Inspection zu Marketing-Zwecken

48. Sitzung, 6.-7. September 2010, Berlin, Deutschland

-Übersetzung-

Deep Packet Inspection (DPI) ist eine Technologie, die die Untersuchung[1] des Headers und von Teilen des Inhalts von Datenpaketen, die über Netzwerke übertragen werden, in Echtzeit oder annähernder Echtzeit erlaubt.

Ein Internet-Paket oder „Datagramm" besteht gewöhnlich aus einem „Datagramm-Kopf" und einem „Datagramm-Daten-Bereich". Der Datagramm-Kopf ist der Teil des Pakets, der Informationen wie Quell- und Ziel- IP-Adresse enthält sowie andere Details, die notwendig sind, um das Paket dorthin zu leiten, wo es hin soll, während es das Netz durchquert. Der Datagramm-Daten-Bereich wird als „Nutzdaten" bezeichnet, weil er den Inhalt dessen bildet, was der Datagramm-Kopf (den „Umschlag") gewöhnlich zustellt. „Paketkopf" bezeichnet jegliche Information, die ein Dienstleister benötigt, um eine Telekommunikations-Nachricht zustellen zu können; die Nachricht selbst wird als der Inhalt oder die Nutzdaten dieser Telekommunikations-Nachricht bezeichnet.

Während DPI nicht als eine neue Technologie angesehen werden kann, da sie schon seit Jahren im Bereich der Intrusion Detection und -Prevention-Systeme wie auch in Firewall-Systemen eingesetzt wurde, wurden in jüngerer Zeit zusätzliche Nutzungen – ermöglicht durch leistungsfähigere Computer und effizientere Algorithmen – für das Netzverkehrsmanagement, zur Kontrolle der Verbreitung illegaler oder unerwünschter Inhalte – einschließlich urheberrechtsgeschützten Materials – und sogar für die Auslieferung benutzerspezifischer Werbung an Internetnutzer diskutiert und einzuführen begonnen.

Die Anwendung dieser Technologie kann die Privatsphäre von Internetnutzern Risiken aussetzen. Insbesondere können bestimmte Nutzungsarten von DPI-Technologien durch Internet-Zugangsdiensteanbieter zu erheblichen Beeinträchtigungen der Privatsphäre von Internetnutzern führen. Zugangsdiensteanbieter sind das „Eingangstor in die virtuelle Welt"; ihnen ist es technisch möglich, den Inhalt der gesamten Kommunikation eines Internetnutzers zu überwachen. Es ist daher unerlässlich, dass Internet-Zugangsdiensteanbieter das Fernmeldegeheimnis respektieren, wie es in vielen Rechtsordnungen festgelegt ist. Darüber hinaus bieten Internet-Zugangsdiensteanbieter in vielen Fällen nicht nur Internetzugang an, sondern auch Internettelefonie und Zugang zu Medien, wie Kabelfernsehen. Anbieter solcher „triple-play"-Dienste können – technisch gesehen – ein noch

[1] In der Computertechnik werden Firewalls verwendet, um legitime Datenpakete für verschiedene Typen von Verbindungen zu unterscheiden. Nur Datenpakete, die einer vordefinierten Regel genügen, werden durch die Firewall durchgelassen, andere werden zurückgewiesen. Paketfilterung, oder „normale" Packet Inspection, arbeitet auf der Vermittlungsschicht (Schicht 3) und betrachtet nur den Header eines Pakets wie die Quell- und Ziel- IP-Adresse. Deep Packet Inspection (DPI) ist eine Firewall-Technologie, die auf der Anwendungsschicht (Schicht 7) des OSI-Modells arbeitet. DPI ermöglicht die Untersuchung des Inhalts von übertragenen Datenpaketen, wie der Kommunikation über HTTP und von Internet-Telefonie (VoIP)- Inhalten.

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
An der Urania 4- 10
D-10787 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

detaillierteres Profil des Kommunikationsverhaltens ihrer Kunden erlangen. Mit dem Entstehen neuer und innovativer Dienste wie Telemedizin können darüber hinaus mehr und mehr besonders sensible personenbezogene Daten (wie Gesundheitsdaten) über Einrichtungen übertragen werden, die von Internet-Zugangsdiensteanbietern angeboten werden.

Die Arbeitsgruppe hat erhebliche Vorbehalte gegen den Einsatz von DPI für jegliche Zwecke außer der Gewährleistung der Sicherheit von Informationssystemen und- Netzen innerhalb einer Organisation[2], oder soweit es sonst durch das anwendbare Recht erlaubt oder gefordert wird.

Die Arbeitsgruppe insbesondere besorgt, dass jegliche zusätzliche Anwendung von DPI durch Internet-Zugangsdiensteanbieter und andere Internetdiensteanbieter in einer weiteren Erosion des Fernmeldegeheimnisses münden wird. Sie wird auch die Vertrauensbeziehung zwischen diesen Anbietern und ihren Kunden beschädigen.

Die Anwendung von DPI bei Internet-Zugangsdiensteanbietern kann in der Informationsgesellschaft auf das Äquivalent des Abhörens von Telefongesprächen hinauslaufen. Die Gruppe unterstreicht ihre Position, die bereits in früheren Veröffentlichungen niedergelegt ist, dass Netzwerk- und Diensteanbieter (einschließlich Internet-Zugangsdiensteanbieter) prinzipiell jegliche Inhalte einer Kommunikation nicht abhören oder stören dürfen, außer wo dies durch das anwendbare Recht ausdrücklich erlaubt oder gefordert wird[3] (informationelle Gewaltenteilung). Dies wird heutzutage auch unter der Überschrift „Netzneutralität“ diskutiert.

Empfehlungen

Im Lichte des oben gesagten fordert die Arbeitsgruppe Internet-Zugangsdiensteanbieter auf, insbesondere die Nutzung von DPI-Technologie für zielgerichtete beziehungsweise verhaltensbasierte Werbung zu unterlassen.

Zusätzlich fordert die Arbeitsgruppe die vermehrte Anwendung sicherer Ende-zu-Ende-Verschlüsslungsmechanismen. Das (optionale) Angebot solcher Technologien sollte gesetzlich vorgeschrieben werden wo dies nicht bereits der Fall ist, wenigstens für Anbieter, deren Dienste die Verarbeitung besonders sensitiver Daten beinhalten (z.B. Online-Banking, Nutzungen, die Kreditkarteninformationen beinhalten, Gesundheitsdaten, usw.) wie auch für Anbieter von Kommunikationsdiensten (wie E-Mail, Chat, Internettelefonie – VoIP, usw.)[4].

---

[2] Vergleiche Arbeitspapier zu Intrusion Detection–Systemen (IDS) (Berlin, 02./03.09.2003); http://www.datenschutz-berlin.de/attachments/229/enum_de.pdf

[3] Vergleiche gemeinsamer Standpunkt zur Aufnahme telekommunikationsspezifischer Prinzipien in multilaterale Abkommen zum Datenschutz – zehn Gebote zum Schutz der Privatheit im Internet (Berlin, 13./14.09.2000); http://www.datenschutz-berlin.de/attachments/215/tc_de.pdf

[4] Vgl. Bericht und Empfehlungen zu Datenschutz und Privatsphäre im Internet (Budapest-Berlin Memorandum) (Berlin, 19.11.1996), Punkt 7 auf Seite 2; http://www.datenschutz-berlin.de/attachments/137/bbmen_de.pdf