Allzu sorglose Weitergabe von IP-Adressen?

Joerg Heidrich
Heise Zeitschriften Verlag

Dr. Christoph Wegener
Horst Görtz Institut für IT-Sicherheit

DFN-Cert Workshop 2010
Hamburg, 10. Februar 2010

Heise Zeitschriften Verlag

Zur Person: Joerg Heidrich

- Justiziar Heise Zeitschriften Verlag
- Rechtsanwalt in Hannover
- Fachanwalt für IT-Recht

- Autor zahlreicher Fachpublikationen und Referent
- Sachverständiger für IT-Produkte (ULD SH/rechtlich)

Zur Person: Dr. Christoph Wegener

- Mitarbeiter am Horst Görtz Institut für IT-Sicherheit (HGI)
- Gründungsmitglied "Arbeitsgruppe Identitätsschutz im Internet" (a-i3)
- Gründer der **wecon.it**-consulting

- CISA, CISM, CBP
- Auditor und Sachverständiger
- Fachautor/-lektor/-gutachter, verschiedene Lehrtätigkeiten

hgi
Horst-Görtz Institut
für IT Sicherheit

Was werden wir heute vorstellen?

- Motivation und Einführung in die Problematik
  - Wann werden IP-Adressen gespeichert bzw. weitergegeben?
- Einordnung von IP-Adressen bzgl. des Datenschutzes
  - Sind IP-Adressen personenbezogen?
  - Welche Konsequenzen ergeben sich daraus?
- Lösungsansätze
  - Anonymisierung von IP-Adressen
  - Auftragsdatenverarbeitungsregelung
  - Nutzung lokaler Datenquellen
- Fazit

Wann werden IP-Adressen gespeichert?

- Meist im Zusammenhang mit Logging-Mechanismen
  - Zu Abrechnungszwecken (vgl. etwa TKG und TMG)
  - Zu Datenschutzzwecken (vgl. etwa Anlage zu §9 BDSG)
  - Zu forensischen Zwecken ("Einbruchsaufklärung")
- Oft werden die Daten aber nicht (regelmäßig) gelöscht
  - Teilweise "dauerhafte" bzw. "langfristige" Aufbewahrung
  - Speicherplatz ist heute kein Problem mehr
- Speicherdauer aber (gesetzlich) begrenzt
  - "*Nur so lange wie zu [...] notwendig.*"
  - Vgl. dazu etwa BDSG, TKG und TMG

Wann werden IP-Adressen weitergegeben?

- Viel, viel häufiger als man zunächst denkt ;)
- Gängige Praxisbeispiele sind
  - Weitergabe im Rahmen von "Blacklisting"-Verfahren
  - Weitergabe im Rahmen von GeoIP-Verfahren
  - Weitergabe im Rahmen von "reverse DNS"
- Besonders problematisch insbesondere bei Nutzung
  - Einer externen Quelle
  - Eines ausländischen Anbieters

Wann werden IP-Adressen weitergegeben? Beispiel: DNS-based Blacklists (DNSBL)

- Anwendung vor allem zur Spam-Bekämpfung
- Bekannter Anbieter: THE SPAMHAUS PROJECT
- Funktionsweise
  - DNSBL-Verfahren basieren auf DNS-Abfragen
  - Exemplarisches Beispiel für die IP-Adresse 12.34.56.78
    - Frage nach "87.65.43.21.dnsbl.example.net."
    - Positive Antwort liefert: "A" record
    - Negative Antwort liefert: "NXDOMAIN"
- In jedem Fall wird aber die IP-Adresse des einliefernden (E-Mail-)Servers an den DNSBL-Anbieter übertragen!

Wann werden IP-Adressen weitergegeben? Beispiel: GeoIP

- Anwendungsfelder
  - Anti-Fraud-Mechanismen
  - Angebote in passender Sprache
  - Lastverteilungsmechanismen
- Bekannter Anbieter: MaxMind®
- Funktionsweise
  - Übertragen der IP-Adresse an Geo-IP-Anbieter
  - Auswertung anhand einer Datenbank und des Routing
  - Rückgabe der Geodaten (Land, Stadt, ...)

Wann werden IP-Adressen weitergegeben? Beispiel: Google Analytics

- Anwendungsfelder
  - Analyse der Webzugriffe
  - Optimierung des Webcontent
  - Optimierung der Marketingstrategien
- Bekannte Anbieter: Google Analytics
- Funktionsweise
  - Auf Webseite wird JavaScript-Code eingebettet
  - Übermittlung von Nutzerdaten und IP-Adresse an Google
  - Google erstellt detaillierte Statistiken

Wann werden IP-Adressen weitergegeben? Beispiel: reverse DNS (rDNS)

- Anwendungsfelder
  - Anti-Spam-Bekämpfung
  - Erkennen von DSL-IP-Adressen
- Bekannte Anbieter: Jeder DNS-Server-Betreiber ;)
- Funktionsweise
  - Umgekehrtes DNS-Verfahren
  - Exemplarisches Beispiel für den Rechner mit der IP-Adresse 12.34.56.78
    - Frage: "78.56.34.12.in-addr.arpa."
    - Antwort: "server.example.net."

Einordnung von IP-Adressen
Sind IP-Adressen personenbezogen?

- Definition in § 3 BDSG: "*Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer* ***bestimmten oder bestimmbaren natürlichen Person***"
- Bestimmte Person: (-)
- Bestimmbare Person: Höchst umstritten!

Meinungsstreit IP-Adressen Bestimmbar im Sinne von § 3 BDSG?

- **1. Ansicht** (Google, AG München, Literatur)
  - Bei der Bestimmbarkeit ist nur auf die Kenntnis der jeweiligen Person abzustellen
  - Diese hat keine Möglichkeit, auf Providerdaten zuzugreifen

- **2. Ansicht** (LG Berlin, BMJ, Literatur, Datenschutzbeauftragte)
  - Abzustellen ist auf die objektive Möglichkeit, auf Daten von Dritten zuzugreifen
  - Daher auch Zurechnung der Providerdaten
  - Zudem: Möglichkeit der Verknüpfung mit weiteren Daten
  - Vergleichbar Autokennzeichen, Kontonummer, u.ä.

Einordnung von IP-Adressen
Statische vs. dynamische IP-Adressen

- Es gibt verschieden Arten von IP-Adressen
  - *Private IP-Adressen* (nach RFC 1918)
    - Spielen hier im weiteren keine Rolle, sie werden nicht geroutet
  - *Dynamische IP-Adressen*
    - Können nur mit Hilfe des vergebenden Providers einer bestimmten Person zugeordnet werden
  - *Statische IP-Adressen*
    - Lassen sich aber von Jedermann durch die Registry Datenbank (beispielsweise beim RIPE-NCC) einer Person zuordnen

- Problem: IP-Adressart lässt sich nicht direkt erkennen
  - Statische IP-Adressen „infizieren“ die dynamischen!
  - Alle Adressen sind wie statische IP-Adressen zu behandeln!

Folgen der Einordnung

- IP-Adressen sind personenbezogene Daten
- Nach § 4 BDSG gilt: *"Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit ein Gesetz dies erlaubt oder anordnet oder der Betroffene eingewilligt hat."*
- Für IP-Adressen gelten folgende Vorschriften:
  - Bei Websites: Telemediengesetz (TMG)
  - Bei E-Mail: Telekommunikationsgesetz (TKG) und BDSG (str.)
- Einwilligung des Betroffenen?
  - Muss ausdrücklich erfolgen (Unterschrift, Checkbox)
  - Muss vor der Nutzung erfolgen
  - Daher bei Web und E-Mail i.d.R. (-)
  - Möglich z.B. bei Foren, Registrierung

IP-Adressen bei Websites

- § 15 TMG Nutzungsdaten

  (1) Der Diensteanbieter darf personenbezogene Daten eines Nutzers nur erheben und verwenden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen (...)

  (4) Der Diensteanbieter darf Nutzungsdaten über das Ende des Nutzungsvorgangs hinaus verwenden, soweit sie für Zwecke der Abrechnung mit dem Nutzer erforderlich sind (Abrechnungsdaten). Zur Erfüllung bestehender gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsfristen darf der Diensteanbieter die Daten sperren.

- Herausgabe nach § 14 TMG nur gegenüber Behörden und Rechteinhabern

IP-Adressen bei E-Mails

- Nach hM Anwendung TKG und BDSG
- Anwendung der allgemeinen Vorschrift des § 28 BDSG

(1) Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig

1. *wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist,*
2. *soweit es zur **Wahrung berechtigter Interessen** der verantwortlichen Stelle **erforderlich** ist und kein Grund zu der Annahme besteht, dass das **schutzwürdige Interesse** des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung **überwiegt**, oder*

Einordnung von IP-Adressen Weitergabe an ausländische Anbieter

- Probleme bei der Weitergabe an ausländische Stellen (§ 4b BDSG)
- Erlaubt bei Stellen innerhalb der EU oder solche mit vergleichbarem Datenschutzniveau

- Höchst problematisch bei Weitergabe an „unsichere Drittstaaten“, insbesondere USA, China, Indien
- Bei Weitergabe in USA:
  - „Safe Harbour“ Regelung erforderlich oder
  - Vertragliche Vereinbarung nach EU-Muster
  - Ansonsten: Gesonderte Einwilligung des Betroffenen erforderlich

- Problematisch auch bei Cloud Computing

Einordnung von IP-Adressen Zwischenfazit

- Ergebnis der Einordnung
  - IP-Adressen sind nach hM als personenbezogenen Daten zu betrachten
  - Speicherung und Weitergabe nur bei bestehender gesetzlicher Erlaubnis oder Einwilligung des Betroffenen
  - Im Web: Anwendung TMG
  - Bei E-Mails: Interessenabwägung nach BDSG

- Konsequenzen
  - Speicherung und insbesondere Weitergabe von IP-Adressen an Dritte ohne Einwilligung ist rechtswidrig
  - Nutzung von rechtlichen oder technischen Maßnahmen zur Vermeidung der Speicherung oder Weitergabe

Lösungsmöglichkeiten Einwilligung des Nutzers

- Problematisch aus diversen Gründen
  - Zeitliche Korrelation zwischen Einwilligung und Nutzung
    - Einwilligung müsste vor jeglichem Logging erfolgen
  - Mechanismen existieren nicht
    - Keine "Nutzerinteraktion" beim E-Mail-Protokoll
  - Nutzer wird abgeschreckt
    - Meine Daten werden benutzt?
  - Nutzer versteht Problem nicht
    - Nutzer willigen in alles ein
- Dies Lösung lässt sich nicht sinnvoll ein- bzw. umsetzen!

Lösungsmöglichkeiten Auftragsdatenverarbeitungsregelung

- Auftragsdatenverarbeitung im Sinne des § 11 bzw. § 4a BDSG
  - Möglicher Ausweg bzgl. der Einwilligung des Betroffenen in eine Datenübermittlung
- Vorteile
  - Keine Einwilligung des Betroffenen notwendig
  - Klare Regelung bzgl. des Datenschutzes
- Nachteile
  - In jedem Fall "umfangreiche" vertragliche Regelungen
  - In einigen Fällen definitiv nicht machbar, da der Anbieter sich nicht darauf einlassen wird

Lösungsmöglichkeiten Anonymisieren von IP-Adressen

- Durch "Nullen" des/der letzten Oktetts einer IP-Adresse werden die IP-Adressen entsprechend anonymisiert

- Vorteile
  - Bei ausreichender Nullung Keinerlei Personenbezug mehr herstellbar
  - Beim Geo-IP-Verfahren bringt die Nullung des letzten Oktetts keine wesentlichen Nachteile (vgl. Kühn, DuD 2009, 747ff)

- Nachteile
  - Bei Antispam-Lösungen sehr kontraproduktiv
  - Reverse DNS funktioniert schlichtweg nicht mehr

Lösungsmöglichkeiten
Verwendung einer lokalen Datenbank

- Anstelle eines externen Anbieters kann etwa im Falle des DNSBL auch eine lokale Datenbank verwendet werden

- Vorteile
  - Keine Weitergabe von IP-Adressen an DNSBL-Anbieter
  - Benötigt keine dauerhafte Verbindung zum DNSBL-Anbieter

- Nachteile
  - Erhöhter personeller Aufwand (etwa für Betrieb des DNS-Servers)
  - Erhöhte Kosten
    - Bei Spamhaus Mehrkosten von etwa 10% ggb. Abrufverfahren
    - Bei Spamhaus aber erst ab 5000 Nutzern möglich

Fazit

- IP-Adressen sind personenbezogene Daten
  - Keine Speicherung und Weitergabe von IP-Adressen ohne Einwilligung des Betroffenen
- Ausweichverfahren sind teilweise vorhanden
  - Nutzung lokaler Datenbanken
  - Anonymisierung der IP-Adressen
  - Auftragsdatenverarbeitungsregelungen
- ... und sollten auch genutzt werden
  - Rechtliche Risiken
  - Besseres Gewissen ;)

Einige Literatur zum Thema

- Amtsgericht Berlin (AZ 5 C 314/06) vom 27. März 2007
  http://medien-internet-und-recht.de/pdf/VT_MIR_2007_378.pdf
- Amtsgericht München (AZ 133 C 5677/08) vom 30. September 2008
  http://medien-internet-und-recht.de/pdf/VT_MIR_2008_300.pdf

- Schreiben des Bundesjustizministeriums vom 2. Februar 2009
  http://www.daten-speicherung.de/data/bmj_2009-02-02.pdf
- Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 26./27. November 2009
  http://www.datenschutz-mv.de/dschutz/beschlue/Analyse.pdf

- Kühn, DuD 2009, 747ff

Danke für Ihre Aufmerksamkeit :)

Joerg Heidrich

Christoph Wegener

- Kontakt per E-Mail: joerg.heidrich@heise.de
  wegener@wecon.net

- Mehr Infos im Web: www.heise.de
  www.wecon.net