International Working Group
on Data Protection
in Telecommunications

675.52.16

Arbeitspapier: Aktualisierung zu Datenschutz und Datensicherheit in der Internettelefonie (Voice over IP - VoIP) und verwandten Kommunikationstechnologien

59. Sitzung, 24. – 25. April 2016, Oslo (Norwegen)

- Übersetzung -

Einleitung

Im September 2006 veröffentlichte die Arbeitsgruppe ein Arbeitspapier zu Voice over IP (VoIP) - Anwendungen[1] in dem Bestreben, mögliche Datenschutz- und Datensicherheitsrisiken zu antizipieren. Dieses Papier schilderte die Situation, wie sie von der Arbeitsgruppe zu dieser Zeit gesehen wurde: Es beschrieb die sich entwickelten Dienste sowie mögliche zukünftige Datenschutz- und Datensicherheitsrisiken und enthielt eine Reihe von datenschutz- und datensicherheitsbezogenen Empfehlungen für Geräteherstelle, Softwareentwickler und Anbieter von VoIP-Diensten.

In den nachfolgenden zehn Jahren hat VoIP weitverbreitete Anwendung in Organisationen und bei Endnutzern gefunden. Darüber hinaus ist die Sprachtelefonie mit einer Reihe anderer Kommunikationstechnologien zusammengeführt worden, wie Instant Messaging und Text- und Videoübertragung. In einigen Regionen haben bereits Diskussionen über die Ausmusterung des „Plain Old Telephone System“ (POTS) begonnen, das jetzt von einigen als „veraltete Infrastruktur“ bezeichnet wird.

[1] Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation: „Arbeitspapier zu Datenschutz und Datensicherheit bei der Internet-Telefonie (VoIP)“, verabschiedet auf der 40. Sitzung am 5. – 6. September 2006 in Berlin (Deutschland); http://www.datenschutz-berlin.de/attachments/101/WP_VoIP_de.pdf

Secretariat
Berliner Beauftragte für
Datenschutz und Informationsfreiheit
Friedrichstr. 219
D-10969 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

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

Die Empfehlungen in diesem Arbeitspapier gelten für alle Arten von Multimedia-Diensten, einschließlich Instant Messaging, Real-Time Text und Videodienste.[2] Darüber hinaus unterscheidet dieses Arbeitspapier nicht zwischen einem VoIP-Dienst, der von einem Telekommunikationsdiensteanbieter angeboten wird und dem Angebot eines „Over-the-Top"-Anbieters. Auch wenn sich die von den verschiedenen Unternehmen verwendete Technologie unterscheidet, bleiben die Datenschutz- und Datensicherheitsrisiken gleich und deswegen richten sich die Empfehlungen an all diese Unternehmen. Zusätzlich zu Standardlösungen existieren viele proprietäre Produkte und Dienste, die einen unterschiedlichen Grad an Sicherheit, Datenschutz und Schutz der Privatsphäre bieten. Unglücklicherweise bleiben nicht-technische Nutzer über den gebotenen Schutz oft uninformiert, oder ihnen werden keine datenschutzfreundlichen Standardeinstellungen geboten.

Mit diesem zusätzlichen Arbeitspapier aktualisiert die Arbeitsgruppe die Empfehlungen, die in der ursprünglichen Veröffentlichung enthalten sind, auf Basis einer Neuevaluierung des heutigen Entwicklungsstandes (2016). Die folgenden Überlegungen motivieren die Neuevaluierung dieser Thematik:

- Die Enthüllungen von Edward Snowden deuten darauf hin, dass Strafverfolgungsbehörden und Geheimdienste rund um den Erdball in nie dagewesener Weise Zugriff auf VoIP-Verbindungen und auch auf die damit zusammenhängenden Verkehrsdaten haben – mit oder ohne Kooperation von Unternehmen, die diese Dienste im Internet anbieten (einschließlich Anbietern von VoIP-Diensten). Diese globale Überwachung stellt das Vertrauen sowohl in Entwickler als auch in Dienstanbieter in Frage. Informationslecks bei Verkehrsdaten, wie IP-Adressen, DNS-Anfragen und Adressköpfen der Anwendungsschicht (Signalling Header), stellen in gleicher Weise eine Herausforderung für die Vertraulichkeit der Kommunikation dar.[3] Zwar werden durch Verkehrsdaten keine Kommunikationsinhalte bekannt, sie liefern aber oft genügend Informationen über die kommunizierenden Partner, um deren Privatsphäre zu gefährden.

- Die Standardisierung im Bereich von VoIP hat Fortschritte gemacht und der Markt ist heutzutage weiter entwickelt als 2006, als das ursprüngliche Papier veröffentlicht wurde. Die Standardisierung des Session Initiation Protocol (SIP) und der verschiedenen Erweiterungen ist

[2] Wir nutzen die Begriffe „Sprache und Video" und „Multimedia" synonym, da sich der Inhalt dieser Empfehlungen auf das allgemeinere Konzept von Multimedia-Kommunikation bezieht. Aus historischen Gründen und um die Lesbarkeit zu verbessern wird häufiger der Begriff Sprachtelefonie benutzt.

[3] R. Barnes, et al., „Confidentiality in the Face of Pervasive Surveillance: A Threat Model and Problem Statement" (RFC 7624), August 2015, abrufbar unter http://tools.ietf.org/html/rfc7624

abgeschlossen und viele Produkte sind nunmehr auf dem Markt erhältlich. Zusätzlich ist mit Web-Real-Time-Communication (WebRTC)[4] ein neuer Standardisierungsversuch gestartet worden, der darauf zielt, eine bessere Harmonisierung mit Web-Technologien (und besonders mit Browsern) zu ermöglichen. Erste Anwendungen sind verfügbar. Das Ziel von WebRTC ist, die einfachere Integration von Echtzeitkommunikation in den Browser zu ermöglichen. Dies führt zu neuen Herausforderungen für Datenschutz und Datensicherheit[5].

- Der Einsatz von breitbandiger Mobilfunktechnologie und WiFi-Netzwerken hat substantiell zugenommen. Nutzer können diese Netzwerke für verlässliche VoIP- und Video-Verbindungen von hoher Qualität verwenden. Außerdem ist einfach zu bedienende VoIP-Software auf Endgeräten vorinstalliert, oder sie kann über App-Stores heruntergeladen werden. Wurde VoIP In den frühen 2000er Jahren überwiegend von Unternehmen und technisch versierten Nutzern verwendet, ist dies heute unter normalen Endnutzern weit verbreitet.

- Datenschutz- und Datensicherheitspraktiken der verschiedenen Angebote unterscheiden sich erheblich. Unglücklicherweise werden Nutzer über diese Praktiken nicht ausreichend informiert.

- POTS wurden traditionell von einem einzigen – in der Regel staatlichen – Anbieter installiert und verwaltet. Im Gegensatz dazu entwickelt sich die jetzige VoIP-Umgebung zu einer Zusammensetzung vieler Teile (z.B. Netzwerkdienste, Betriebssysteme, Anwendungssoftware). Diese „Teile“ werden häufig von unterschiedlichen Einrichtungen entwickelt und verwaltet (z. B. dem Netzanbieter, dem Entwickler der Hard- oder Software und dem Hersteller des Geräts), die unabhängig voneinander und in den meisten Fällen ohne jegliche Koordination handeln. Während diese Vermehrung der Rollenden den Nutzern eine größere Auswahl ermöglichen könnte, führen die Anreize für die Beteiligten und ihre Ziele nicht notwendigerweise zu einer Verbesserung des Schutzes der Privatsphäre, da jeder Teilnehmer auf seinen Teil in der Kette fokussiert ist.

[4] W3C, WebRTC 1.0: Real-Time Communication Between Browsers, abrufbar unter http://www.w3.org/TR/webrtc/

[5] E. Rescorla, "WebRTC Security Architecture", IETF draft (work in progress), März 2015, abrufbar unter https://tools.ietf.org/html/draft-ietf-rtcweb-security-arch-11

Technischer Hintergrund

Von der Konzeption her sind VoIP-Lösungen ziemlich einfach: Ein Nutzer gibt die Telefonnummer oder ein anderes Identifizierungsmerkmal (von denen viele wie eine E-Mail-Adresse aussehen) ein, um andere Nutzer „anzurufen“. Mithilfe einer unterstützenden Infrastruktur, manchmal Proxies genannt, initiiert der VoIP-Klient dann die Kommunikationssignalisierung, um das Gerät des Angerufenen aufzufinden. Die Nachrichten, die im Rahmen dieser Prozedur ausgetauscht werden, werden als Signalisierungsnachrichten bezeichnet.

Für VoIP-Lösungen, die das Zusammenwirken mit anderen Anbietern nicht unterstützen, müssen alle Nutzer ihre Geräte bei demselben VoIP-Anbieter registriert haben. In offeneren Systemen kann dieser Erkennungsschritt kompliziert sein, weil Nutzer bei verschiedenen VoIP registriert sein können und die Erkennungsprozedur auf weitere Anbieter ausgedehnt werden kann. Es ist darauf hinzuweisen, dass das Zusammenwirken mit anderen VoIP-Systemen oder sogar mit dem öffentlichen Telekommunikationsnetz zu einem Verlust an Funktionalität und schwächeren Privatsphäre- und Sicherheitseigenschaften führen kann.

Wenn das Gerät des anderen Kommunikationspartners gefunden worden ist, können Sprachpakete zwischen den beiden Parteien ausgetauscht werden. Während Signalisierungsnachrichten häufig indirekt über die unterstützende Infrastruktur zwischen den beiden Parteien geroutet werden, wird Multimedia-Verkehr (wie Sprach- und Videotelefonie) idealerweise direkt übertragen. Diese direkte Kommunikation führt zu geringerer Latenz. Sprachpakete können als Inhalt in dem „Secure Real-Time Transport Protocol“ (SRTP)[6] eingekapselt sein. Es existieren verschiedene Protokolle, um dem überall vorhandenen Überwachungsrisiko zu begegnen.[7]

In praktischen Szenarien bieten Signalisierungsnachrichten mehr Funktionalität als das pure Auffinden von Kommunikationsgeräten, einschließlich der Aushandlung von Protokollparametern und Funktionen. Für anspruchsvollere Nutzungsszenarien, wie Konferenzschaltungen oder Rufweiterleitungen, kann die Prozedur zur Verbindungsherstellung komplexer sein. Für das Angebot von Kanalsicherheit mit SRTP ist außerdem die Einrichtung von kryptografischen Schlüsseln und Algorithmen erforderlich. Daher sind verschiedene unterschiedliche Schlüsselmanagement-

[6] M. Baugher, et al., „The Secure Real-Time Transport Protocol (SRTP)”, März 2004, RFC 3711, abrufbar unter https://tools.ietf.org/html/rfc3711

[7] IAB Statement on Internet Confidentiality, November 2014, abrufbar unter https://www.iab.org/2014/11/14/iab-statement-on-internet-confidentiality/

Protokolle für die Einrichtung der zur Sicherung des medialen Verkehrs benötigten Schlüssel entwickelt worden, die alle geringfügig verschiedene Eigenschaften haben.[8]

Empfehlungen[9]

Im Lichte des oben Gesagten gibt die Arbeitsgruppe den verschiedenen Parteien folgende Empfehlungen:

Gesetzgeber und Regulierungsbehörden

Gesetzgeber und Regulierungsbehörden auf nationaler, regionaler und sogar globaler Ebene werden daran erinnert, dass im gesetzlichen Schutz der Vertraulichkeit der Kommunikation auf den verschiedenen Regulierungsebenen im Hinblick auf VoIP-Dienste Lücken existieren. Sie werden aufgerufen, die gesetzliche Situation gründlich zu untersuchen und die notwendigen Änderungen vorzunehmen, um sicherzustellen, dass die Bestimmungen zum Fernmeldegeheimnis, die in vielen nationalen Verfassungen und regionalen und globalen Regulierungsinstrumenten vorhanden sind, auch VoIP und andere Multimedia-Kommunikationsdienste vollständig abdecken.

VoIP-Anbieter, Software-Entwickler und Hardware-Hersteller

Transparenz

VoIP-Diensteanbieter sollten ihre Kunden über die Datenschutz- und Datensicherheits-Charakteristiken der von ihnen angebotenen VoIP-Dienste informieren.

Datenschutzfolgeabschätzung und Evaluierung durch Dritte

Hersteller von Hard- und Software sollten Datenschutzfolgeabschätzungen durchführen. Die Arbeitsgruppe befürwortet auch die Analyse und Überprüfung durch unabhängige, vertrauenswürdige Dritte. Ein Beispiel einer solchen Untersuchung ist die „Secure Messaging Scorecard“ der

[8] Für eine Analyse von Schlüsselaustausch-Technologien und ihren Eigenschaften siehe RFC 5479 (https://tools.ietf.org/html/rfc5479) und RFC 7201 (https://tools.ietf.org/html/rfc7201)

[9] Die Empfehlungen zu VoIP sind zusammen mit denen aus dem ersten Arbeitspapier der Gruppe von 2006 zu lesen; vgl. http://www.datenschutz-berlin.de/attachments/102/WP_VoIP_de.pdf

Electronic Frontier Foundation (EFF).[10] Automatische Werkzeuge werden zum Beispiel von der XMPP Foundation[11] und der GSM Map[12] angeboten.

Design-Überlegungen

Software-Entwickler und Hardware-Hersteller sollten angemessene technische Maßnahmen ergreifen, um den Signalisierungs-Verkehr wie auch den Sprach- und Videotelefonie-Verkehr gegen die weit verbreitete unautorisierte Überwachung zu schützen. Dazu ist es als grundlegende Design-Überlegung unerlässlich, dass Software-Entwickler Implementierungen auf Basis von Ende-zu-Ende-Verschlüsselung sowohl für die Signalisierung als auch für den Inhalt anstreben.

Der VoIP-Signalisierungsverkehr muss authentisiert und Integrität und Vertraulichkeit müssen zwischen den teilnehmenden VoIP-Signalisierungsknoten geschützt werden. Die Bereitstellung von Ende-zu-Ende-Integrität für den gesamten VoIP-Signalisierungsverkehr ist bedauerlicherweise in den meisten VoIP-Architekturen nicht möglich, weil die Signalisierungs-Nutzdaten bei der Übertragung verändert werden.[13] Die Übertragung von Signalisierungs-Nachrichten über Verbindungen, die nicht kryptografisch geschützt sind, sollte vermieden werden. Es ist darauf hinzuweisen, dass es angesichts des Ausmaßes allgegenwärtiger Überwachung im heutigen Internet keine angemessene, dem Stand der Technik entsprechende Sicherheitstechnik ist, sich allein auf die physische Sicherheit zu verlassen.[14]

Verkehrsdaten über die Kommunikation, wie die Identifikatoren der kommunizierenden Parteien, Kommunikations-Präferenzen (wie Codecs und Sprache), Länge der (verschlüsselten) Datenpakete und Online-Status verraten oft eine überraschende Menge an Informationen. Die Arbeits-

[10] Electronic Frontier Foundation (EFF), „Secure massaging Scorecard“, Oktober 2015, abrufbar unter https://www.eff.org/secure-messaging-scorecard
[11] XMPP(Extensible Messaging and Presence Protocol) Foundation, „XMPP Security Tests“, Oktober 2015, abrufbar unter http://xmpp.net
[12] GSM – *Global System for Mobile Communications* (vorher „Groupe Spécial Mobile“). Vgl. Karsten Nohl, „GSM Map“, Oktober 2015, abrufbar unter https://gsmmap.org
[13] Da die Modifizierung der Nutzdaten von Signalisierungsnachrichten Signaturalgorithmen bricht, wie auf S. 16 des RFC 7340 beschrieben (https://tools.ietf.org/html/rfc7340) und die meisten VoIP-Architekturen Signalisierungs-Nutzdaten bei der Übertragung modifizieren, muss die Anzahl der teilnehmenden Knoten so klein wie möglich gehalten werden, um die Integrität des gesamten VoIP-Signalisierungsverkehrs sicherzustellen. RFC 7044 bietet eine Lösung zur stufenweisen Anwendung von Nachrichtenschutz („message protection“), während die Nachrichten durch das SIP-Kommunikations-Netzwerk geroutet werden. Dies bietet der kommunizierenden Partei Informationen über den Verlauf (https://tools.ietf.org/html/rfc7044).
[14] Während die für „klassische“ Telekommunikationsdienste genutzte Leitungs-Infrastruktur als „sicher per Definition“ angesehen wurde, kann diese Annahme nicht mehr weiter gelten: Heutzutage werden Leitungen in großem Umfang von Geheimdiensten abgehört.

gruppe empfiehlt daher, den Umfang der Daten zu begrenzen, der Intermediären, wie z. B. Signalisierungs-Gateways, zugänglich gemacht wird, und die Verwendung persistenter Identifikatoren soweit wie möglich zu vermeiden.

Die Arbeitsgruppe ermutigt VoIP-Anbieter nachdrücklich, Schlüsselmanagement-Mechanismen zu verwenden, die es Intermediären nicht erlauben, an Schlüsselmaterial zu gelangen (weil es im Klartext eingebettet in die Signalisierungs-Nachrichten übertragen wird), und ein Schlüsselmanagement-Protokoll zu verwenden, das „Perfect Forward Secrecy" (PFS)[15] benutzt. PFS ist ein Sicherheitsmerkmal, das die Entschlüsselung zurückliegender Konversationen durch Kompromittierung der geheime Schlüssel innerhalb längerer Zeiträume durch einen Angreifer verhindert. Trotz der Beschränkungen einiger VoIP-Architekturen sollte die Priorität auf die Implementierung von Ende-zu-Ende-Sicherheit für Sprach- und Videokommunikation gelegt werden.

Es sollten Maßnahmen entwickelt werden, mit denen Nutzer durch Verifizierung der Schlüssel nachprüfen können, ob ein „Man-in-the-middle"-Angriff stattgefunden hat, soweit Zertifikate zum Aufbau der Ende-zu-Ende-Kommunikation erforderlich sind. Zertifikate[16] könnten durch vertrauenswürdige Dritte ausgegeben und könnten– als Option – mit Pseudonymen (Telefonnummer, Nutzername, oder Namen von Organisationen) verbunden werden, die den kommunizierenden Parteien angezeigt werden.

VoIP-Diensteanbieter müssen standardmäßig den Umfang der personenbezogenen Daten, die sie speichern und verarbeiten, auf das für die Erbringung und Abrechnung (falls zutreffend) des Dienstes Notwendige beschränken, soweit eine zusätzliche Speicherung und Verarbeitung von Daten nicht ausdrücklich durch Gesetz vorgeschrieben ist. Der Schutz gespeicherter Daten gegen unautorisierten Zugriff muss sichergestellt werden.

VoIP-Diensteanbieter müssen grundlegende datenschutzrelevante Leistungsmerkmale, wie Rufnummernunterdrückung, wenigstens in derselben Art und Weise anbieten, wie dies in Fest- und Mobilfunknetzen üblich ist. Da die Unterdrückung der Rufnummer und das „Caller ID Spoofing" bestimmte Arten von Angriffen ermöglicht, sollten kürzlich entwickelte Schutzmechanismen be-

[15] Die PFS-Eigenschaften sind genauer erklärt in https://en.wikipedia.org/wiki/Forward_secrecy. Vgl. auch A. Menezes, P van Oorschot, und S. Vanstone. *Handbook of Applied Cryptography*. CRC Press, Boca Raton, FL, USA 1996 (S. 496).

[16] J.Peterson, et al., „Secure Telephone Identity Credentials: Certificates", IETF draft (work in progress), März 2016, abrufbar unter https://tools.ietf.org/html/draft-ietf-stir-certificates-03

rücksichtigt werden.[17] Die Unterdrückung der Rufnummerninformation macht Zugriffskontrolllisten, manchmal auch Freundeslisten genannt, weniger effektiv. Aufgrund der direkten Verbindung zwischen den Kommunikationspartnern werden ihnen die jeweiligen IP-Adressen bekannt. Um dies zu verhindern, sollte die optionale Nutzung von Proxies oder Anonymisierungsdiensten (z. B. Tor[18], TURN[19]) nicht verboten werden.

Vorhandene, offene Standards, die Gegenstand von umfassender Überprüfung und Verifikation durch eine große Zahl unabhängiger Experten gewesen sind, sollten wiederverwendet werden. Für den Schutz von Sprachkommunikation sind mehrere standardisierte Lösungen verfügbar.[20],[21] Es ist darauf hinzuweisen, dass der Standardisierungsprozess in verschiedenen Organisationen die Veröffentlichung technischer Spezifikationen ohne eine signifikante Überprüfung durch Experten erlaubt oder, im schlimmsten Fall, sogar ohne jegliche Überprüfung. Daher sollte eine Entscheidung darüber, welche technische Spezifikation genutzt werden soll, den Grad der Überprüfung in Betracht ziehen. Standardisierungsorganisationen werden ermutigt, für mehr Transparenz über den Prozess zu sorgen, durch den eine Spezifikation entwickelt worden ist.

Nutzerbeteiligung

VoIP-Anbieter sollten ihren Nutzern ermöglichen, ihren eigenen Identitäts-Anbieter zu wählen, wo solch eine Trennung zwischen Identitäts-Anbieter und VoIP-Diensteanbieter technisch möglich ist.

VoIP-Anbieter sollten (wo dies angemessen ist) Datenportabilität anbieten, um ihren Kunden einen bequemen Zugriff auf relevante Daten, wie Freundeslisten und Konfigurationsdaten zu ermöglichen.

---

[17] IETF, „Secure Telephone Identity Revisited (STIR) Working Group“, Oktober 2015, abrufbar unter https://datatracker.ietf.org/wg/stir/charter/

[18] Weitere Informationen über die Onion-Routing-Technologie Tor sind verfügbar unter https://en.wikipedia.org/wiki/Tor_(anonymity_network)

[19] R. Mahy, et al., „Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)“, RFC 5766, April 2010, abrufbar unter https://tools.ietf.org/html/rfc5766

[20] M. Westerlund und C. Perkins, „Options for Securing RTP Sessions“, RFC 7201, April 2014, abrufbar unter https://tools.ietf.org/html/rfc7201

[21] D. Wing, et al., "Requirements and Analysis of Media Security Management Protocols", RFC 5479, April 2009, abrufbar unter https://tools.ietf.org/html/rfc5479

Operationale Überlegungen

Alle Akteure in der Lieferkette müssen schnell auf Datensicherheits- und Datenschutz-Schwachstellen in den Protokollen und der genutzten Hard- oder Software reagieren. Für Schwachstellen in verteilter Software, wie Smartphone-Apps oder herunterladbarer Software, erfordert dies einen Software-Update-Mechanismus.

VoIP-Dienstanbieter müssen sicherstellen, dass Datenschutz- und Datensicherheitsmerkmale ihrer Produkte standardmäßig aktiviert sind. Datenschutz- und Datensicherheitsmechanismen sollten dem Kunden ohne prohibitive Kosten angeboten werden.

VoIP-Dienstanbieter sollten einen föderierten Zugang (federated access) zu ihren VoIP-Diensten anbieten. Dies ermöglicht es Nutzern, sich mit Nutzern anderer VoIP-Anbietern zu verbinden, ohne verschiedene VoIP-Klienten herunterzuladen und installieren zu müssen. Als Minimum müssen Nutzer über Veränderungen von Sicherheits- und Datenschutzeigenschaften ihrer Kommunikation beim „Interworking“ mit anderen VoIP-Systemen (oder sogar dem öffentlichen Telefonnetz) informiert werden und über jeden Verlust von Funktionalität, Sicherheit oder Schutz der Privatsphäre, der aus solchen Veränderungen entstehen kann.

Zweckbindung

Anbieter, Software-Entwickler und Hardware-Hersteller, die Verkehrsdaten verarbeiten, müssen das Prinzip der Zweckbindung respektieren.

Nutzer

Nutzer von VoIP-Diensten sollten die möglichen Risiken für die Sicherheit und die Privatsphäre ihrer Kommunikation berücksichtigen. Sie sollten sich über Sicherheits- und Datenschutzeigenschaften der verschiedenen Dienste informieren, und die von ihnen genutzten Dienste und Dienstanbieter danach auswählen. Schließlich sollten Sie sicherstellen, dass existierende Sicherheits- und Datenschutzmechanismen eines Dienstes vor dessen Nutzung aktiviert werden.

Über die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation („Berlin Group“)

Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation (englisch: International Working Group on Data Protection in Telecommunications - IWGDPT, auch bekannt als “Berlin Group”) besteht aus Vertretern von Datenschutzbehörden und Organisationen aus aller Welt, die sich mit dem Schutz der Privatsphäre beschäftigen. Die Arbeitsgruppe wurde 1983 im Rahmen der Internationalen Datenschutzkonferenz auf Initiative der Berliner Landesdatenschutzbehörde gegründet, die seither den Vorsitz führt. Seit ihrer Gründung hat die Arbeitsgruppe eine Vielzahl von Empfehlungen („Gemeinsame Standpunkte“ und „Arbeitspapiere“) zur Verbesserung des Schutzes der Privatsphäre in der Telekommunikation verabschiedet. Seit Anfang der neunziger Jahre beschäftigt sich die Gruppe insbesondere mit dem Schutz der Privatsphäre im Internet.

Weitere Informationen über die Arbeitsgruppe sowie die von der Gruppe verabschiedeten Dokumente sind auf der Webseite der Arbeitsgruppe abrufbar: http://www.berlin-privacy-group.org .