Studie zeigt: Deutsche Apps setzen verstärkt auf Werbe- und Tracking-Dienste

SMARTPHONE-APPS KONTAKTIEREN IM SCHNITT 25 SERVER UND DURCHQUEREN SECHS NETZWERKE

Bild: ff(s)

Jede Berührung des Smartphone-Displays setzt weltweit Dutzende Server in Bewegung. Eine aktuelle Untersuchung der 65 beliebtesten Apps in Deutschland offenbart die komplexen digitalen Infrastrukturen hinter alltäglichen Anwendungen. Während US-Konzerne auf eigene Netzwerke setzen, nutzen deutsche Anbieter deutlich mehr externe Dienste – mit Folgen für Datenschutz und digitale Souveränität.

In Deutschland besitzen etwa 69 Millionen Menschen ein Smartphone.[1] Das Institut für Internet-Sicherheit – if(is) hat nun analysiert, welche digitalen Infrastrukturen die beliebtesten Apps tatsächlich nutzen. Das Ergebnis: Hinter dem vermeintlich einfachen „läuft in der Cloud" verbirgt sich ein komplexes globales Netzwerk.

Für die Untersuchung wählten die Forscher 65 Apps aus den Top-50-Rankings des Google Play Stores und des iOS App Stores in Deutschland aus. Diese wurden in drei Gruppen eingeteilt: „Alle Apps" (65 Apps), „Top 20 Apps" (die meistgenutzten Anwendungen) und „Deutsche Apps" (14 Anwendungen mit Firmensitz in Deutschland). Um vergleichbare Ergebnisse zu gewährleisten, wurden alle 65 Apps vorab in funktionale Gruppen wie E-Mail, Messenger, Social Media oder Shopping eingeteilt. Innerhalb jeder Gruppe erfolgte die Nutzung nach definierten Ablaufszenarien, zum Beispiel Liken von Beiträgen in Social-Media-Apps oder das Senden und Empfangen von E-Mails in der gleichen Anzahl. Jede App wurde dabei fünf Minuten lang genutzt. Wenn möglich, wurde für jede App ein neues Nutzerkonto angelegt.

AUFZEICHNUNG UND ANALYSE DES TRAFFICS

Um den Smartphone-Traffic mitzuschneiden und zu analysieren, wurde ein neues Motorola Moto G24 mit Android 14 verwendet. Um sowohl App-spezifischen als auch den gesamten Netzwerkverkehr zu erfassen, kamen zwei Verfahren zum Einsatz:

- **On-Device-Erfassung mit PCAPdroid:** Die Android-App „PCAPdroid" zeichnet den Netzwerkverkehr einzelner Anwendungen gezielt auf. So lassen sich App-Sessions isoliert betrachten, ohne dass System- oder Hintergrundprozesse den Mitschnitt verfälschen. PCAPdroid speichert die Traffic-Daten im PCAP-Format, das später in Analyse-Tools wie Wireshark importiert werden kann.
- **Port-Mirroring im WLAN:** Zusätzlich wurde der gesamte Smartphone-Traffic, inklusive dem Android Hintergrund-Traffic, mittels Port-Mirroring an einem PC mitgeschnitten. Das Setup bestand aus **Smartphone – Access Point – Switch – Router – PC.** Der Access Point übernahm allein die WLAN-Funktion, während der Switch den Verkehr zum PC spiegelte. Auf dem PC lief Wireshark mit Filterregeln, um anhand der statisch eingestellten MAC-Adresse des Smartphones dessen Datenpakete zu ermitteln. Andere Geräte, die Traffic im Netzwerk erzeugen, wurden so zuverlässig ausgeklammert.

Um eine belastbare Datengrundlage zu gewährleisten, verzichteten die Forscher bewusst auf virtuelle Emulatoren oder Root-Berechtigungen. Zahlreiche Apps erkennen solche Umgebungen und passen ihr Netzwerkverhalten entsprechend an [3]. Zur Einordnung der erfassten IP-Adressen sowie zur Bestimmung von Hosting-Anbietern, Peering-Beziehungen und der geografischen Verteilung nutzten sie außerdem öffentlich zugängliche Datenquellen, darunter ipinfo.io, PeeringDB, GeoIP-Datenbanken sowie die weitverbreitete Hosts-Liste von Steven Black auf GitHub.

APPS VERBINDEN SICH WELTWEIT

Die Analyse des Smartphone-Datenverkehrs verdeutlicht das Ausmaß der digitalen Infrastruktur, die hinter den meistgenutzten Apps steckt. Bei den 65 untersuchten Anwendungen stellten die Forschenden fest, dass insgesamt über 1.600 Server mit unterschiedlichen IP-Adressen kontaktiert wurden. Im Durchschnitt nimmt jede App Verbindung zu rund 25 einzelnen Servern auf, und die IP-Pakete durchlaufen dabei etwa 6,35 eigenständige Netzwerke (Autonome Systeme, ASNs). Mehr als drei Viertel dieser Netzwerke und Server befinden sich in US-amerikanischer Hand.

Besonders stark vertreten sind die Rechenzentren von drei Unternehmen: Amazon, Google und Akamai. Bei diesen Anbietern wurden die meisten eindeutigen IP-Adressen registriert. In rund 90 Prozent aller Top-Apps sind sie präsent. Fast jede der 65 Anwendungen greift somit auf mindestens einen dieser drei globalen Infrastruktur-Riesen zurück.

Auch die DNS-Aktivität ist ein wichtiger Faktor. Im Durchschnitt fragt jede App 65 Domains ab, wobei etwa 13 Aufrufe pro Anwendung auf Werbe- oder Tracking-Server entfallen. Diese machen insgesamt 23 Prozent aller DNS-Anfragen aus und verdeutlichen, wie häufig Drittanbieter-Komponenten in den Datenstrom eingreifen.

Das dabei übertragene Datenvolumen ist beachtlich. Die gesamten Uploads aller Apps summieren sich auf circa 115,6 MB, während die Downloads mit rund 2,84 GB deutlich darüber liegen. Pro App entspricht das etwa 1,78 MB Upload und 43,7 MB Download. Jede Interaktion zieht somit eine nennenswerte Datenmenge nach sich.

Obwohl moderne Plattformen längst IPv6 anbieten, bleibt IPv4 mit einem Anteil von 96 Prozent das technisch dominierende Protokoll. Gleichzeitig wird rund 93 Prozent des Traffics verschlüsselt.

Die Ergebnisse der Analyse machen deutlich, dass bereits wenige Minuten Smartphone-Nutzung ein komplexes, weltumspannendes Netz aus Diensten und Verbindungen durch den Datenaustausch in Bewegung setzen.

US-DOMINANZ IN DER DIGITALEN INFRASTRUKTUR

Diese globalen Datenströme spiegeln sich auch in der Netzwerkanalyse wider: Welche Akteure die digitale Infrastruktur dominieren, verdeutlichen

die Abbildungen 1a und 1b. Sie veranschaulichen die zehn führenden autonomen Systeme, die von den 65 meistgenutzten Smartphone-Apps in Deutschland kontaktiert werden, gemessen an der Anzahl der Konversationen. Eine Konversation bedeutet dabei einen zusammenhängenden Datenaustausch zwischen Smartphone und entferntem Server, wie ihn Wireshark anhand von IP-Flows und Port-Kombinationen aufzeichnet.

Von allen aufgezeichneten Sessions entfallen 60 Prozent auf drei US-Tech-Giganten: Google mit 30 Prozent, Amazon mit 16 Prozent und Facebook mit 14 Prozent. Weitere große Content-Delivery-Netzwerke und Cloud-Provider wie Akamai, Fastly und Cloudflare erreichen jeweils Werte bis zu 14 Prozent. Insgesamt liegen mindestens 75 Prozent aller Top-ASNs in US-amerikanischer Hand, was die starke Konzentration des App-Traffics bei wenigen Anbietern unterstreicht.

Die Konzentration auf wenige Provider führt zu einer starken Abhängigkeit. Unternehmen haben oft nur begrenzten Einfluss darauf, über welche Netzknoten ihre Daten geleitet werden. Damit sind sie unmittelbar von Preisänderungen oder technischen Umstellungen der großen Anbieter betroffen.

DEUTSCHE APPS STEUERN GRÖSSERE INFRASTRUKTUREN AN

Neben der dominanten Rolle weniger US-Anbieter fällt auf, dass deutsche Apps oft deutlich komplexere Netzwerkstrukturen nutzen. Abbildung 2 zeigt, wie viele autonome Systeme die unterschiedlichen App-Gruppen durchschnittlich einbinden:

- **Alle Apps:** 6,35 autonome Systeme (Netzwerke)
- **Top 20 Apps:** 5,6 autonome Systeme (Netzwerke)
- **Deutsche Apps:** 11,35 autonome Systeme (Netzwerke)

Deutsche Anwendungen steuern fast doppelt so viele Netzwerke an wie die international dominierenden Top-20-Apps und liegen damit auch deutlich über dem Gesamtdurchschnitt.

Internationale Großanbieter betreiben häufig eigene, hochintegrierte Netzwerke und Content-Delivery-Strukturen. Durch den Betrieb eigener Rechenzentren und optimierter Peering-Vereinbarungen können sie ihren Datenverkehr gebündelt über vergleichsweise wenige autonome Systeme abwickeln. Das erklärt, warum Apps wie WhatsApp oder YouTube mit etwa fünf bis sechs autonomen Systemen pro App auskommen.

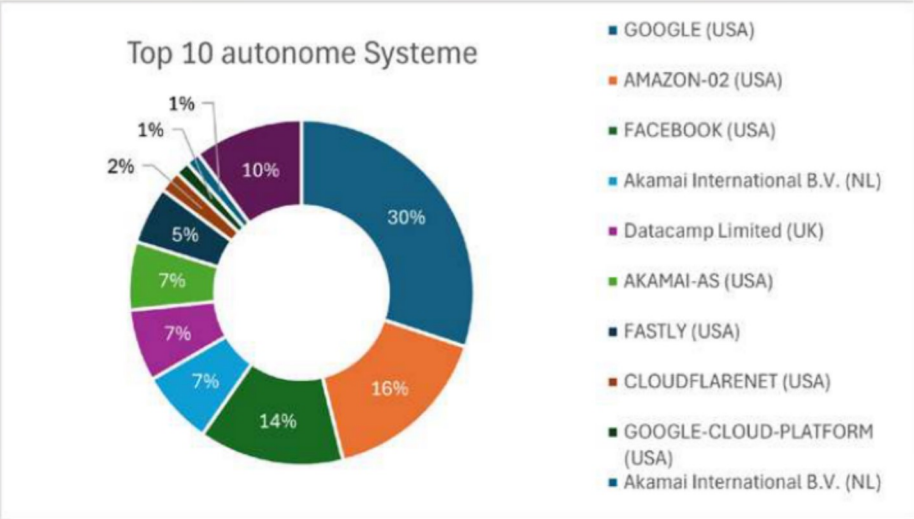


Abbildung 1a: Verteilung der autonomen Systeme bei der Unterstützung aller Apps (Bild: if(is))

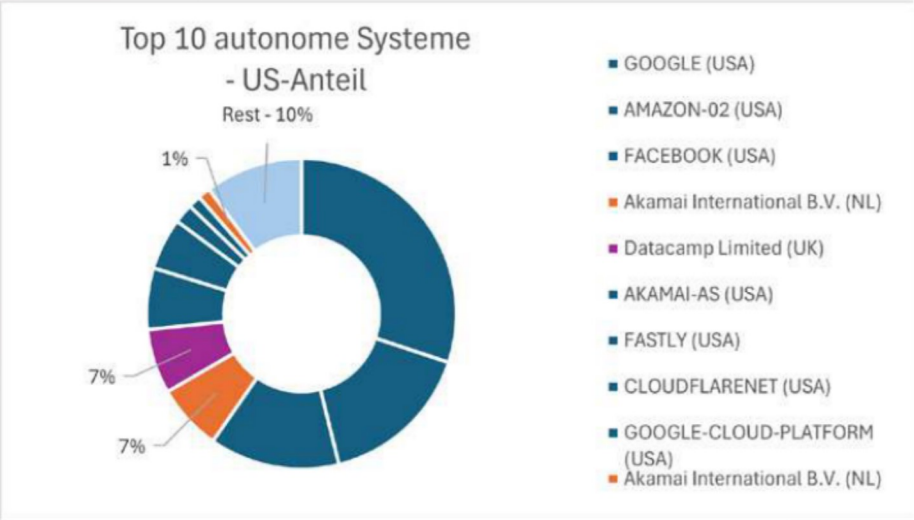


Abbildung 1b: US-Anteil aus Abbildung 1a in dunkelblau (Bild: if(is))

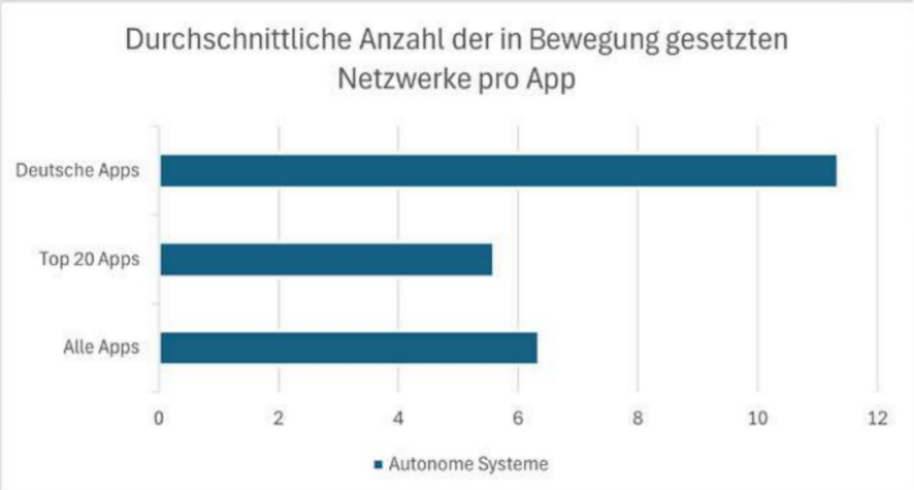


Abbildung 2: Durchschnittliche Anzahl eindeutiger Netzwerke (ASNs) mit denen eine App kommuniziert (Bild: if(is))

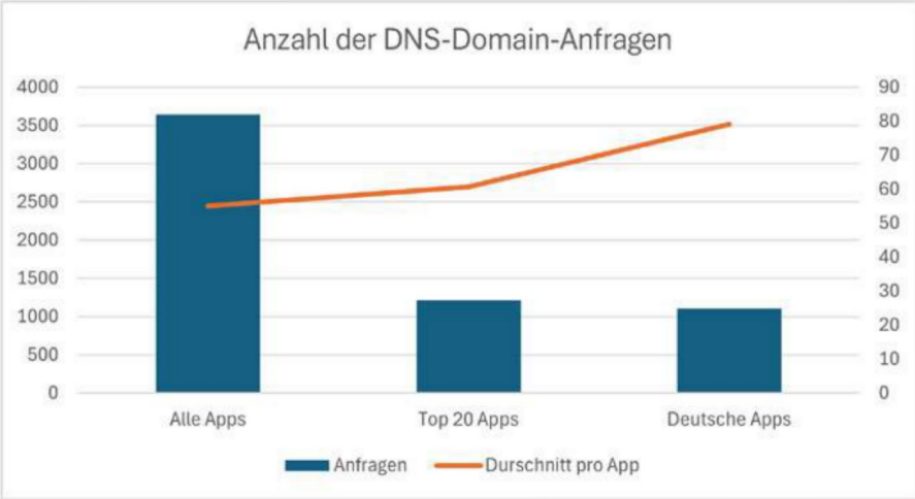


Abbildung 3: Gesamt- und durchschnittliche Anzahl an DNS-Domain-Anfragen (Bild: if(is))

Deutsche Apps hingegen nutzen seltener eine monolithische Infrastruktur. Stattdessen greifen sie auf eine Vielzahl spezialisierter externer Dienste zurück, etwa regionale Dienstleister, Analytics-Plattformen sowie Content-Delivery-Networks. Jede zusätzliche Integration spiegelt sich als weiteres autonomes System in unserer Messung wider.

Eine hohe Zahl an autonomen Systemen pro App steht einerseits für Vielfalt und Skalierbarkeit, bedeutet jedoch auch wachsende Komplexität und weniger transparente Abhängigkeiten in der Infrastruktur. Der Einsatz europäischer oder eigener Infrastrukturen könnte dabei helfen, die Abhängigkeit von US-Hyperscalern zu reduzieren und die digitale Souveränität zu stärken.

MEHR DNS-ANFRAGEN PRO APP-KATEGORIE

Neben der Vielzahl autonomer Systeme fällt bei deutschen Apps auch die DNS-Aktivität ins Auge. Hier zeigt sich ebenfalls ein deutlich komplexeres Muster. Abbildung 3 vergleicht die Gesamtzahl der DNS-Domain-Anfragen (Balken, linke Achse) und den Durchschnitt pro App (Linie, rechte Achse) für drei App-Gruppen:

- **Alle Apps:** etwa 3.600 Anfragen insgesamt, ca. 55 Anfragen pro App (65 Apps)
- **Top-20-Apps:** etwa 1.200 Anfragen insgesamt, ca. 60 Anfragen pro App (20 Apps)
- **Deutsche Apps:** etwa 1.100 Anfragen insgesamt, ca. 80 Anfragen pro App (14 Apps)

Im Durchschnitt generieren deutsche Anwendungen rund 80 DNS-Anfragen, was etwa ein Drittel mehr ist als bei den US-dominierten Top-20-Apps (60) und deutlich mehr als der Durchschnitt aller Apps (55). Dieser erhöhte DNS-Traffic deutet erneut auf eine fragmentierte Infrastruktur hin. Anstatt zentrale, eigene Nameserver zu nutzen, greifen deutsche Apps offenbar häufiger auf eine Vielzahl externer Domains und Dienste zu.

TRACKING BEI DEUTSCHEN APPS

Ein weiterer auffälliger Unterschied zeigt sich bei der Nutzung von Werbe- und Tracking-Diensten. Hier klafft die größte Lücke zwischen deutschen Apps und internationalen Anbietern. Abbildung 4 zeigt den Anteil an Werbung und Tracking der aufgerufenen Domains (Balken, linke Achse) sowie die durchschnittliche Anzahl an unterschiedlich aufgerufenen Werbe- und Tracking-Domains pro App (Linie, rechte Achse):

- **Alle Apps:** etwa 23 Prozent Werbung und Tracking, durchschnittlich circa 13 unterschiedliche Domains pro App
- **Top-20-Apps:** etwa 15 Prozent Werbung und Tracking, durchschnittlich circa neun unterschiedliche Domains pro App
- **Deutsche Apps:** etwa 41 Prozent Werbung und Tracking, durchschnittlich circa 33 unterschiedliche Domains pro App

In diesem Kontext sind mit „Werbe- und Tracking-Domains " jene Hostnamen gemeint, die typischerweise für nicht unmittelbar funktionsrelevante Dienste wie Werbung und Tracking genutzt werden. Die Quelle dieser Domains ist die weitverbreitete Open-Source-Liste „Hosts" von Steven Black.

Deutsche Anwendungen rufen deutlich mehr Werbe- und Tracking-Domains auf als US-dominierte Top-Apps und der Gesamtdurchschnitt. Das heißt jedoch nicht zwangsläufig, dass die internationalen Anbieter weniger Nutzerdaten erheben. Vielmehr setzen sie unter anderem häufiger auf serverseitiges Tracking, bei dem die Requests im Backend stattfinden und nicht über öffentlich sichtbare DNS-Abfragen laufen. Dank optimierter Infrastrukturen und moderner Integrationsmethoden können die großen Anbieter Analysen und Profiling betreiben, ohne jeden einzelnen Endpunkt im Client direkt sichtbar zu machen.

Die höhere Dichte an Werbung und Tracking bei deutschen Apps resultiert vor allem aus der Integration zahlreicher externer Drittanbieter-

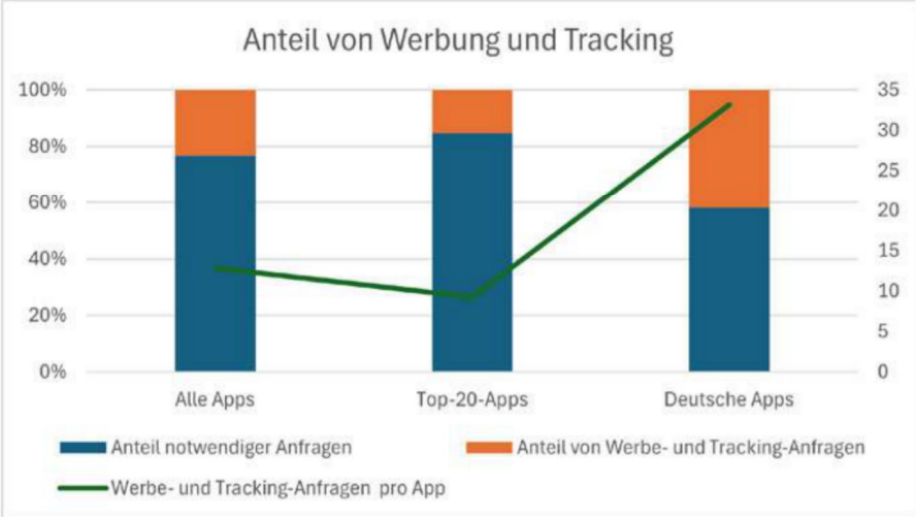


Abbildung 4: Verhältnis von Werbung und Tracking zu notwendigen DNS-Anfragen (Bild: if(is))

DIGITALE INFRASTRUKTUREN UND DIGITALE SOUVERÄNITÄT

Digitale Infrastrukturen bilden das Rückgrat unserer vernetzten Welt. Sie reichen von Glasfaserkabeln und Rechenzentren bis hin zu Content-Delivery-Netzwerken und Cloud-Plattformen großer Anbieter wie Microsoft, Google oder Amazon. Zentral ist dabei das Zusammenspiel aus Client-Server-Architektur und DNS-basierten Diensten. Smartphones lösen Hostnamen auf, initiieren API-Aufrufe an Server-Endpunkte und nutzen verteilte Dienste.

Digitale Souveränität

Digitale Souveränität bezeichnet die Fähigkeit, diese Infrastruktur sowie die übertragenen und gespeicherten Daten selbstbestimmt zu kontrollieren. Dabei sind vor allem folgende Aspekte entscheidend:

- *Geografische Verteilung: Die physische Lage von Rechenzentren hat Einfluss auf Latenz, Ausfallsicherheit und Compliance. Eine ausgewogene Mischung aus nationalen, europäischen und internationalen Standorten verringert das Risiko lokaler Störungen oder die Auswirkungen geopolitischer Spannungen.*
- *Anbieterdiversität: Die Abhängigkeiten von wenigen Hyperscalern reduziert die Handlungsspielräume und kann mit Preiserhöhungen und Leistungsänderungen einhergehen. Die Nutzung mehrerer regional verteilter Provider stärkt die Unabhängigkeit und steigert die betriebliche Resilienz.*

Entscheidend ist nicht nur die Leistungsfähigkeit einzelner Komponenten, sondern vor allem ihre Zusammensetzung und Steuerbarkeit als Gesamtsystem. Eine souveräne digitale Landschaft erfordert Vielfalt, regionale Präsenz und transparente Datenflüsse als Grundvoraussetzungen für stabile IT-Dienste.

Smartphones als Endpunkt

Smartphones fungieren heute als Endpunkte in komplexen digitalen Infrastrukturen. Nach aktuellen Zahlen der Bitkom nutzen bereits 83 Prozent aller Deutschen ein Smartphone.[1] Mit einem gemeinsamen globalen Marktanteil von rund 99 Prozent sind die dominierenden Betriebssysteme Android mit circa 72 Prozent und iOS mit 27 Prozent [2].

Smartphones und digitale Infrastrukturen wie moderne Cloud-Rechenzentren bilden eine untrennbare Symbiose. Die Portabilität und ständige Vernetzung der Smartphones ermöglichen dynamisch skalierbare Dienste, schnelle Updates und Innovationen. Dadurch rücken digitale Anwendungen direkt in unseren Alltag. Gleichzeitig vergrößert diese enge Kopplung jedoch auch Abhängigkeiten und technische Ausfallrisiken.

Zudem wirft permanentes Tracking Fragen zu Datenschutz und ökologischer Nachhaltigkeit auf.

Autonome Systeme

Das Internet besteht aus miteinander verbundenen Netzwerken, den sogenannten autonomen Systemen (AS oder ASN). Jedes autonome System ist einem Unternehmen als Betreiber zugeordnet, und alle autonomen Systeme bilden gemeinsam das Internet. Alle IP-Adressen sind den autonomen Systemen zugeordnet. Die Zuordnung eines ASN zu einem Land bezieht sich auf den Betreiber und dessen Policies, nicht zwangsläufig auf den physischen Standort der Server oder Rechenzentren. So kann ein ASN den USA zugeordnet sein, aber dennoch deutsche IP-Adressen besitzen, was verdeutlicht, wie komplex nationale Zuordnungen im globalen Datenverkehr sind.[4]

Dienste, die jeweils eigene Aufrufe erzeugen. Dadurch wird die Infrastruktur fragmentierter und die Infrastrukturen der Drittanbieter sind leichter identifizierbar. Es zeigt sich, dass die technische Umsetzung (clientseitig vs. serverseitig) die Messbarkeit deutlich beeinflusst, jedoch nicht zwangsläufig das tatsächliche Ausmaß der Datenerfassung.

DIE 15 GRÖSSTEN NETZWERKE NACH ANZAHL IHRER IP-ADRESSEN

Neben DNS-Abfragen und autonomen Systemen lohnt auch ein Blick auf die IP-Adressen selbst. Sie zeigen, welche Anbieter hinter der Infrastruktur der Apps stehen und wie viele eindeutige IP-Adressen von den 65 untersuchten Smartphone-Apps jeweils pro Netzwerk (ASN) kontaktiert werden. Mit 338 einzelnen IPs führt Amazon.com das Feld an, gefolgt von Google LLC (237 IPs) und Akamai Technologies (142 IPs). Microsoft belegt mit 74 IP-Adressen den vierten Platz, dicht gefolgt von Cloudflare (62) und Google Cloud (61). Unter den Top 15 finden sich außerdem klassische Hyperscaler wie Amazon AES (48 IPs), welches Amazons IP-Raum erweitert sowie spezialisierte CDN- und Hosting-Anbieter, wie Fastly (27) und CDN77 (24). Mit OVHcloud (30), IONOS SE (20 IPs) und Hetzner Online (17 IPs) sind auch deutsche beziehungsweise europäische Provider vertreten.

Die Anzahl unterschiedlicher IP-Adressen pro Netzwerk spiegelt das Ausmaß und die Breite der Netzwerkinfrastruktur wider, über die App-Daten geroutet werden. Große Cloud- und CDN-Anbieter unterhalten global verteilte Serverfarmen mit Hunderten von IP-Adressen, um geringe Latenzen, hohe Ausfallsicherheit und Lastverteilung sicherzustellen.

Gleichzeitig lässt sich aus der Verteilung ablesen, welche Anbieter für die beliebtesten Apps in Deutschland unverzichtbar sind. Hyperscaler dominieren nicht nur die Konversationsstatistik, sondern stellen auch die umfangreichsten Adressräume bereit. Die Präsenz europäischer Provider unter den Top 15 zeigt, dass regionale Provider zwar vorhanden sind, jedoch in IP-Kapazität und geografischer Abdeckung hinter den Big-Tech zurückbleiben. Die Daten machen deutlich, dass Smartphone-Apps eng mit wenigen globalen Infrastrukturgebern verbunden sind. Deshalb ist es wichtig, diese Verbindungen bei Architektur- und Betriebsentscheidungen zu berücksichtigen.

WELCHE APPS VERBRAUCHEN AM MEISTEN DATEN?

Doch nicht nur, wohin Daten fließen, ist entscheidend – sondern auch, wie viele Daten einzelne Apps verursachen. Dabei zeigen sich deutliche Unterschiede zwischen den einzelnen App-Kategorien:

- **Grocery-Apps** senden im Schnitt 1,0 MB und empfangen etwa 14,2 MB, ein Verhältnis von rund 1 zu 14. Dies spiegelt den hohen Download-Anteil wider, da Produktbilder, Preise und Angebote kontinuierlich nachgeladen werden.
- **Mail-Apps** zeigen ein differenziertes Bild. Im Gesamtdurchschnitt werden 2,5 MB gesendet und 40,3 MB empfangen (1 zu 16). Entfernt man allerdings GMX und Web.de, sinkt

das Verhältnis auf rund 1,8 MB gesendet zu 3,7 MB empfangen (1 zu 2). Outlook und Gmail folgen diesem schlankeren Profil. GMX und Web.de binden über ihre Kernfunktionen hinaus Cloud-Speicher, News-Feeds und weitere Zusatzdienste ein, was das Datenvolumen deutlich erhöht. Outlook und Gmail beschränken sich hingegen weitgehend auf den reinen E-Mail-Verkehr, weshalb ihr Traffic-Profil deutlich schlanker ausfällt.

- **Messenger-Apps** senden im Schnitt 5,0 MB und empfangen 23,6 MB (1 zu 4,8). Hier dominieren Medien- und Dateitransfers innerhalb Chats.
- **Shopping-Apps** weisen mit 2,9 MB zu 34,5 MB (1 zu 12) ein ähnliches Muster wie Grocery auf, allerdings auf einem höheren Datenvolumen insgesamt, da detaillierte Produktansichten und personalisierte Empfehlungen übertragen werden.
- **Social-Apps** schließlich liegen mit 1,0 MB an gesendeten und 31,8 MB an empfangenen Daten (1 zu 32) an der Spitze des Down-/Up-Verhältnisses, bedingt durch kontinuierliches Laden von Feeds, Bildern und Videos.

In allen Kategorien überwiegt deutlich der Download-Anteil. Die Mail-Apps ohne GMX und Web.de bilden eine Ausnahme, die zeigt, dass das Datenprofil stark von integrierten Zusatzdiensten abhängt. Insgesamt verdeutlichen diese Werte, welche App-Typen besonders viele Daten verbrauchen und wo die Hauptlast im mobilen Datenverkehr liegt.

IPV4- VERSUS IPV6-ANTEIL IM APP-TRAFFIC

Abbildung 5 veranschaulicht den prozentualen Anteil von IPv4- und IPv6-Verbindungen aller untersuchten Smartphone-Apps. Von sämtlichen aufgezeichneten Verbindungen entfallen rund 96 Prozent auf IPv4-Adressen, während nur etwa 4 Prozent der Verbindungen über IPv6 laufen.

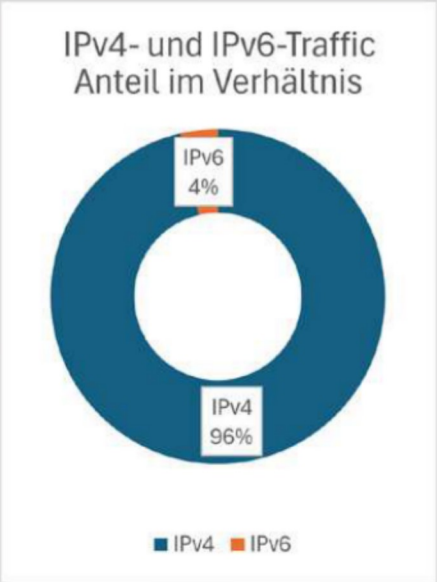


Abbildung 5: Vergleich des Anteils von IPv4- und IPv6-Traffic (Bild: if(is))

Interessanterweise bleibt IPv6 damit selbst bei den beliebtesten Apps weiterhin eine Randerscheinung. Obwohl zahlreiche Provider und Apps IPv6 unterstützen, dominieren in der Praxis nach wie vor IPv4-Adressen. Dies lässt sich vor allem auf drei Faktoren zurückführen. Zum einen sind viele etablierte Anwendungen und Backend-Dienste nach wie vor auf IPv4 ausgelegt, um maximale Kompatibilität und einen reibungslosen Betrieb zu gewährleisten. Einige Netzbetreiber und Content-Delivery-Network-(CDN)-Anbieter schrecken vor einer kompletten Abschaltung ihrer IPv4-Umgebungen zurück, da sie unerwartete Störungen befürchten. Um die flächendeckende Nutzung auszubauen, ist man außerdem auf die Umstellung von Diensten von Drittanbietern auf IPv6 angewiesen.

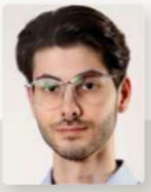
Die Messwerte basieren auf der kombinierten Auswertung des gesamten Smartphone-Traffics, inklusive Android-Hintergrundaktivitäten, die nicht in allen Endgeräte-Logging-Tools sichtbar sind. Dadurch ergibt sich ein vollständigeres Bild des tatsächlichen Protokolleinsatzes im mobilen Alltag.

Bei der Verschlüsselung der Datenübertragung zeigt sich ein erfreulich hohes Niveau. Etwa 93 Prozent des gesamten Datenverkehrs der analysierten Apps werden über gesicherte Protokolle übertragen, nur etwa 7 Prozent bleiben unverschlüsselt.

Dieses Ergebnis zeigt, dass App-Anbieter und Plattformbetreiber dem Schutz von Nutzerdaten heute eine hohe Priorität einräumen.

FAZIT

Smartphones sind Endpunkte einer globalen digitalen Infrastruktur. Die Untersuchung zeigt, dass deutsche Apps im Durchschnitt mehr Server und Domains ansteuern als ihre internationalen Konkurrenten – ein Hinweis auf komplexe und fragmentierte Backend-Strukturen. Um die Symbiose von Smartphone und digitalen Infrastrukturen effizienter, unabhängiger und ressourcenschonender zu gestalten, ist Transparenz über diese Datenflüsse unerlässlich. ■



FERHAN KESICI
studiert den Master Internet-Sicherheit an der Westfälischen Hochschule Gelsenkirchen und beschäftigt sich im Rahmen des Studiums auch mit dem Thema „Analyse der Nutzung der digitalen Infrastruktur durch Smartphone-Apps".

NORBERT POHLMANN
ist Professor für Cybersicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT und im Vorstand des Internetverbandes – eco.

Literatur

[1] *Statista. „Smartphone-Nutzung in Deutschland." Online verfügbar unter: https://de.statista.com/themen/6137/smartphone-nutzung-in-deutschland (Zugriff am 8. Juli 2025).*

[2] *StatCounter. „Mobile Operating System Market Share Worldwide." Online verfügbar unter: https://gs.statcounter.com/os-market-share/mobile/worldwide/ (Zugriff am 8. Juli 2025).*

[3] *OWASP. „MAS Testing Guide – Tampering and Reverse Engineering: Why You Need It." Online verfügbar unter: https://mas.owasp.org/MASTG/0x04c-Tampering-and-Reverse-Engineering/#why-you-need-it (Zugriff am 8. Juli 2025).*

[4] *Cloudflare. „What is an Autonomous System?" Online verfügbar unter: https://www.cloudflare.com/de-de/learning/network-layer/what-is-an-autonomous-system/ (Zugriff am 8. Juli 2025).*