Transparenzbericht CyberGhost VPN 2015

CyberGhost ist niemandes Honigtopf!

Gegründet 2011 in Bukarest, Rumänien, ist Cyberghost Schöpfer eine der weltweit zuverlässigsten Datenschutz- und Sicherheitslösungen. Das Unternehmen verwahrt und anonymisiert die Online-Präsenz von über 7,5 Millionen Anwendern rund um den Globus, verteidigt die Privatsphäre als grundlegendes Menschenrecht und entwickelt, fördert und unterstützt neue, benutzerorientierte Verschlüsselungstechnologien. Als erstes Unternehmen der Branche veröffentlichte CyberGhost 2013 einen Transparenzbericht.

Der Transparenzbericht vermittelt Einsicht in die Beweggründe von Strafverfolgungsbehörden, Polizeidienststellen, Website-Betreibern, Privatpersonen und Rechtsanwaltskanzleien, die Identität eines Cyberghost-Benutzers abzufragen. Hierbei lassen sich drei Hauptkategorien unterscheiden, mit denen die Herausgabe der Nutzerdaten gerechtfertigt werden: DMCA-Beschwerden, polizeiliche Anfragen und Beschwerden über Malware-Aktivitäten.

Für Cyberghost ist Privatsphäre ein Menschenrecht und gehört zum Fundament demokratischer Gesellschaften, weshalb das Unternehmen keine Protokolle über Nutzer und deren Aktivitäten anlegt und alle Anfragen entsprechend negativ zurückweisen muss. Die Tatsache der Anfragen an sich bekräftigt aber die Annahme, dass die Speicherung von Online-Aktivitäten mittlerweile als selbstverständlich gilt. Ebenso wie sie die Notwendigkeit deutlich macht, dass Unternehmen wie kritische Bürger aktiv die Verantwortung für ihre privaten Daten in die Hand nehmen müssen. Cyberghost empfiehlt daher auch anderen IT-Unternehmen und Branchenführern nachdrücklich, das Privatsphärenschutzproblem moderner Gesellschaften auf regelmäßiger Basis anzugehen, Benutzerdaten und Kommunikation prinzipiell zu verschlüsseln und nur die für den jeweiligen Dienst absolut notwendige Daten zu speichern.

Art der Anfragen

Alle Anfragen sind in drei Hauptkategorien zusammengefasst:

DMCA-Beschwerden, also Anfragen auf Grundlage des US-amerikanischen Digital Millennium Copyright Acts, werden in der Regel von verschiedenen Anwaltskanzleien im Auftrag von Unternehmen wie Paramount, Sony Pictures oder andere eingereicht und werfen einzelnen Nutzern vor, urheberrechtlich geschütztes Material illegal über eine Cyberghost-IP verteilt zu haben. Die Beschwerden beinhalten Informationen über die Torrents, die jeweilige Zeit, die verwendeten IP-Adressen und die genutzten Ports.

Beschwerden über Malware-Aktivitäten werden von verschiedenen Seiten an uns herangetragen, darunter private Nutzer wie Organisationen, die beispielsweise Spam erhalten haben oder über CyberGhost-IPs aus dem Netz angegriffen worden sind. Zur Anzeige gebrachte Cybercrime-Fälle beinhalten weiter unter anderem DDoS-Attacken auf Website-Betreiber und Entwickler, den Betrieb von Botnets, verschiedene Fälle von Betrug, unrechtmäßige Einloggversuche und automatisierte E-Mailversand/Spam-Kampagnen durch Websites, die ohne VPN über ihre IP-Adresse als

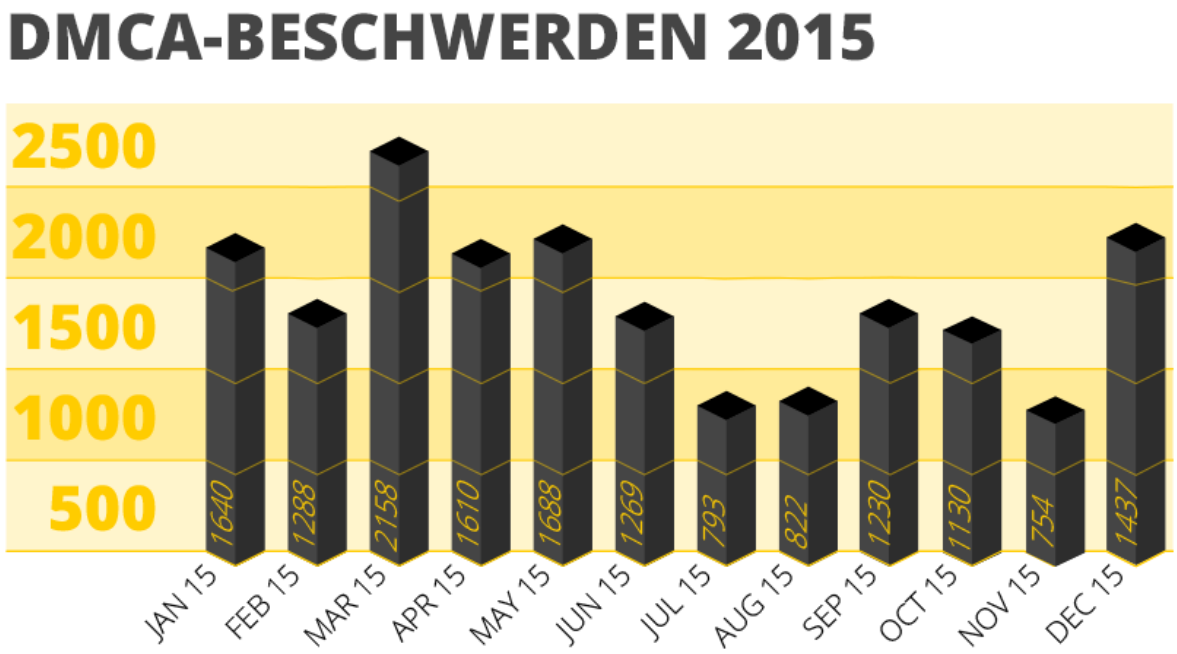
Spamversender erkennbar wären. In dieser Kategorie subsummiert sind auch weitergeleitete Beschwerden von Datenzentren, mit denen das Unternehmen zusammenarbeitet.

Polizeiliche Anfragen erreichen uns von verschiedenen Strafverfolgungsbehörden und Polizeidienststellen und fordern Zugriff auf Protokolle für eine bestimmte, im Zusammenhang mit der jeweiligen Untersuchung stehende IP-Adresse. Diese Anfragen werden in der Regel von den Rechenzentren empfangen und an Cyberghost weitergeleitet.

Übersicht weltweit

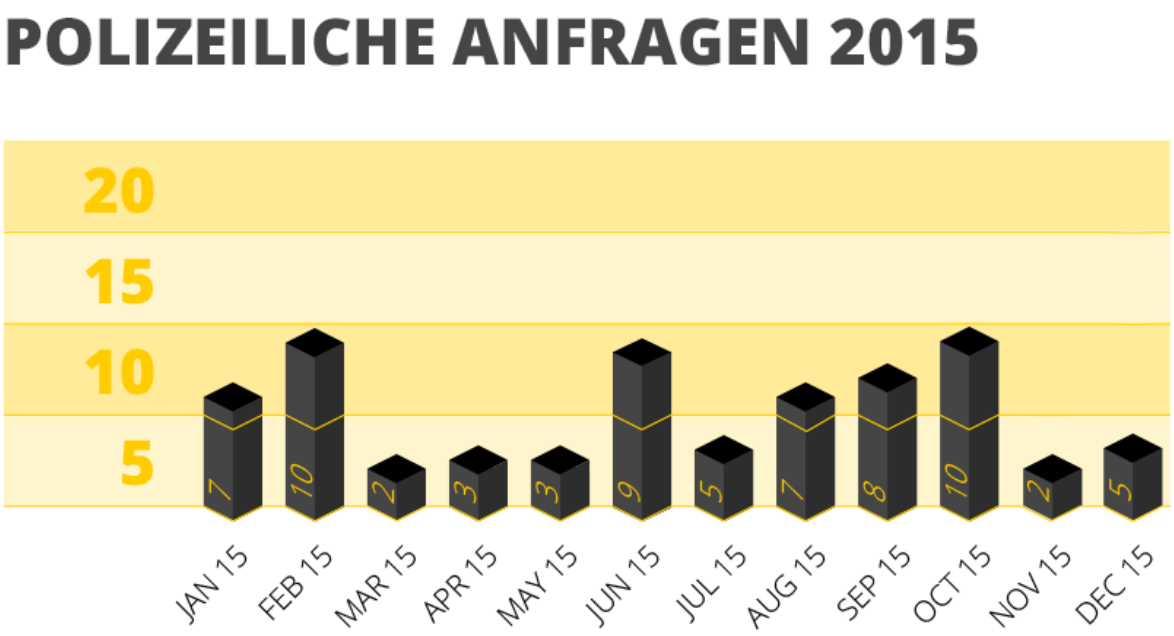
DMCA-Beschwerden

Im Vergleich zum Vorjahr hat sich die Zahl der Anfragen um durchschnittlich 21 % (bezogen auf die letzten 12 Monaten) verringert – gleichwohl die Zahl der Nutzer im selben Zeitraum um 60 % gestiegen ist. Die Zahl der DMCA-Beschwerden ist ferner mit der erhöhten Aktivität der zahlreichen Produktions- und Vertriebsunternehmen sowie Urheberrechtsinhaber zu verknüpfen. In Zahlen ausgedrückt, erhielt Cyberghost im Schnitt 1.318 Beschwerden pro Monat.



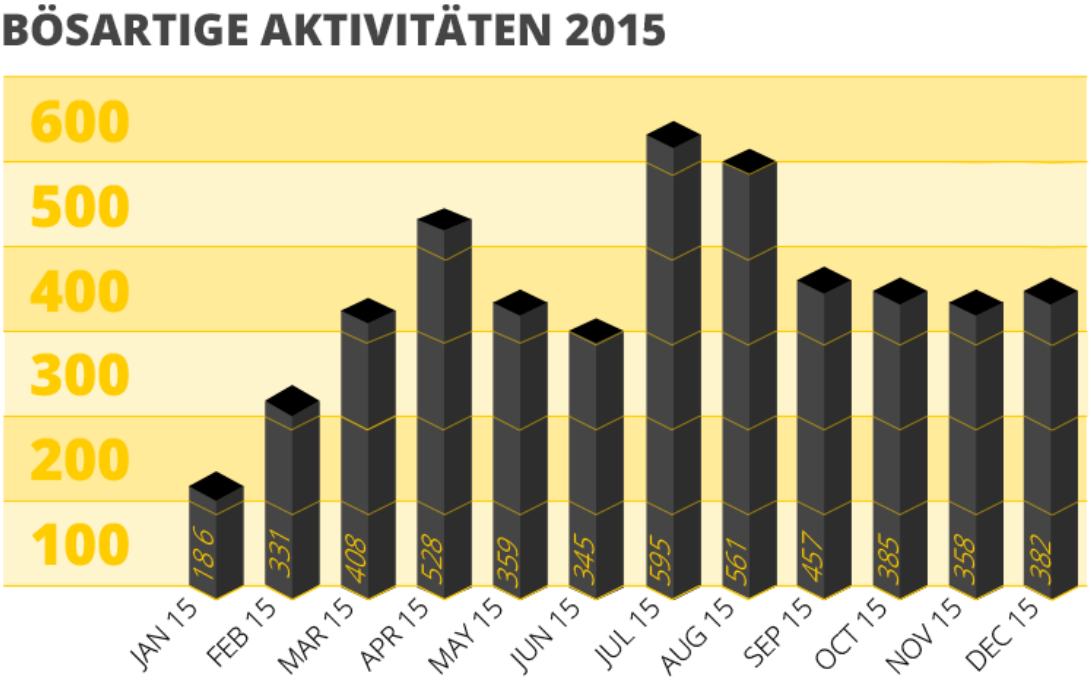
Polizeiliche Anfragen

Der Anstieg der Nutzerzahlen von 3,5 Millionen auf 7,5 Millionen (60 %) schlug sich ebenfalls nicht in der Anzahl der polizeilichen Anfragen nieder. Ganz im Gegenteil wurden zwischen Januar 2015 und Dezember des gleichen Jahres trotz Anwender-Wachstum 24 % weniger Anfragen als 2014 auf Herausgabe von Nutzerdaten gezählt, insgesamt 71 und durchschnittlich sechs pro Monat.



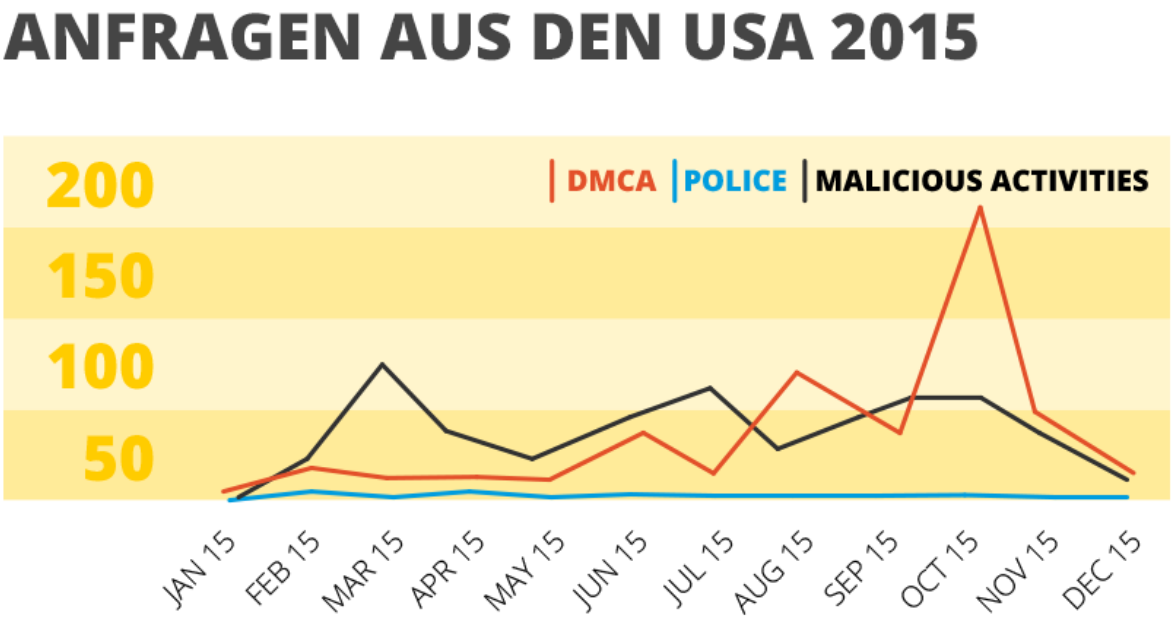
Beschwerden über Malware-Aktivitäten

Ein komplett anderes Bild als die Anfragen hinsichtlich Urheberrechtsverletzungen und Strafverfolgung liefern die Beschwerden über bösartige Aktivitäten, die unter Missbrauch des CyberGhost-VPN-Dienstes ausgeführt wurden. Global betrachtet stieg die Zahl gemeldeter Malware-Aktivitäten um 310 % von durchschnittlich 99 Beschwerden pro Monat in 2014 auf bis zu 407 Meldungen pro Monat im Jahr 2015. Im gleichen Zeitraum wurden auch von Sicherheitsfirmen wie Kaspersky Lab, Trend Micro, Cisco and Symantec deutliche Steigerungen bösartiger Aktivitäten gemeldet.



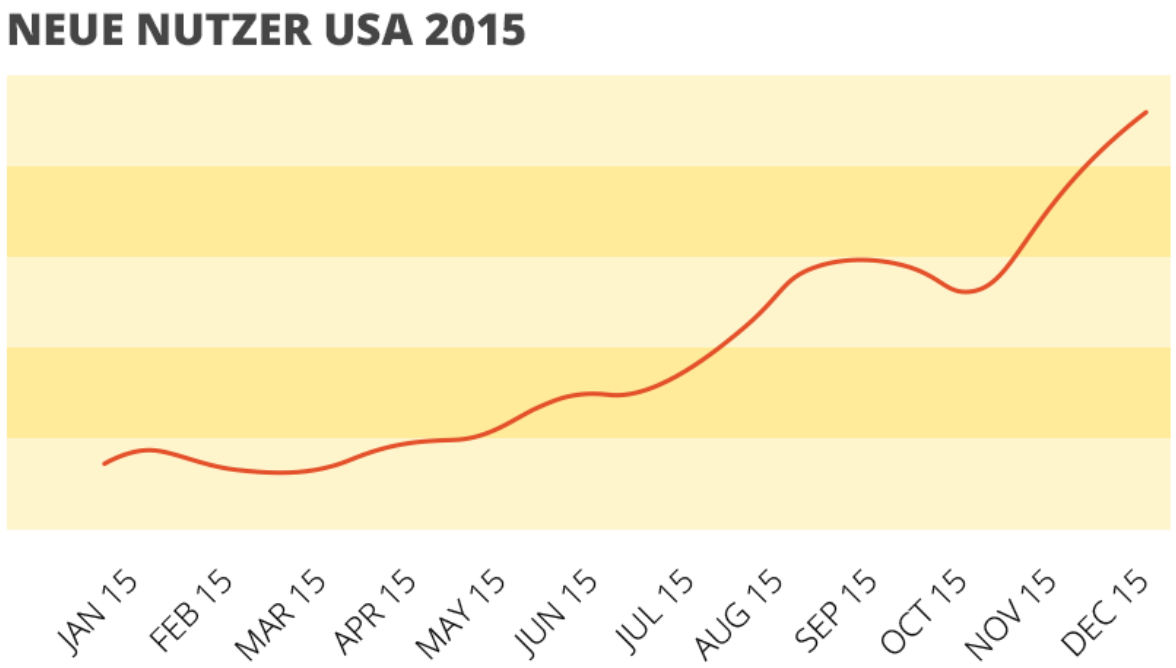
Übersicht USA

Neue US-Vorschriften im Hinblick auf Zensur und Massenüberwachung resultierten 2015 in einer erhöhten CyberGhost-Benutzerzahl. Gleichzeitig ließ sich ein Rückgang der DMCA-Beschwerden beobachten (59 % weniger Anfragen), ebenso wie 17 % weniger polizeiliche Anforderungen. Parallel zum globalen Anstieg der Malware-Aktivitäten ist aber auch in den USA eine deutliche Erhöhung von 243 % in Bezug auf bösartige Angriffe festzustellen.



So brachte der Ablauf von drei Bestimmungen hinsichtlich Überwachung und Ausspähung (Section 215, ‚The Lone Wolf'-Bestimmung und die ‚Roving Wiretap'-Bestimmung) den kontrovers diskutierten 'Patriot Act' im Juni 2015 zurück ins öffentliche Bewusstsein. Ersetzt durch den 'USA Freedom Act', der eine Reform der Massenüberwachung in den USA beinhaltete, beendete eine Mehrheit von 67 Senatoren zumindest die Sammlungen von Telefonanrufen innerhalb der USA.[1]

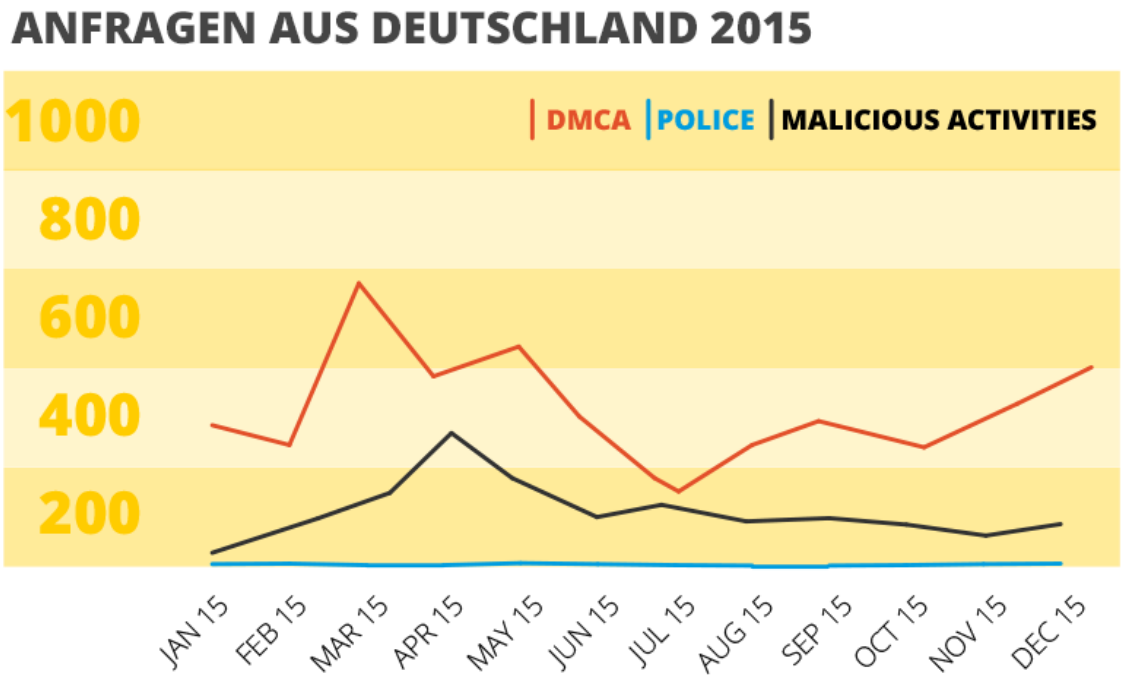
Nationale und internationale Medien lenkten in der Folge die Aufmerksamkeit ihrer Leser auf die Implikationen dieser Bestimmungen, berichteten verstärkt über ältere und aktuelle NSA-Aktivitäten und hoben die Bedeutung der Privatsphäre hervor. Für CyberGhost bedeutete die innerstaatliche Renaissance in Sachen Privatsphäre ein Wachstum bis zu 150 % zwischen Juni und Dezember 2015, wie in der Grafik unten ersichtlich.



Neue Anwender in den USA 01.2015-12.2015

[1] Http://www.usnews.com/news/articles/2015/06/02/senate-passes-freedom-act-ending-patriot-act-provision-lapse

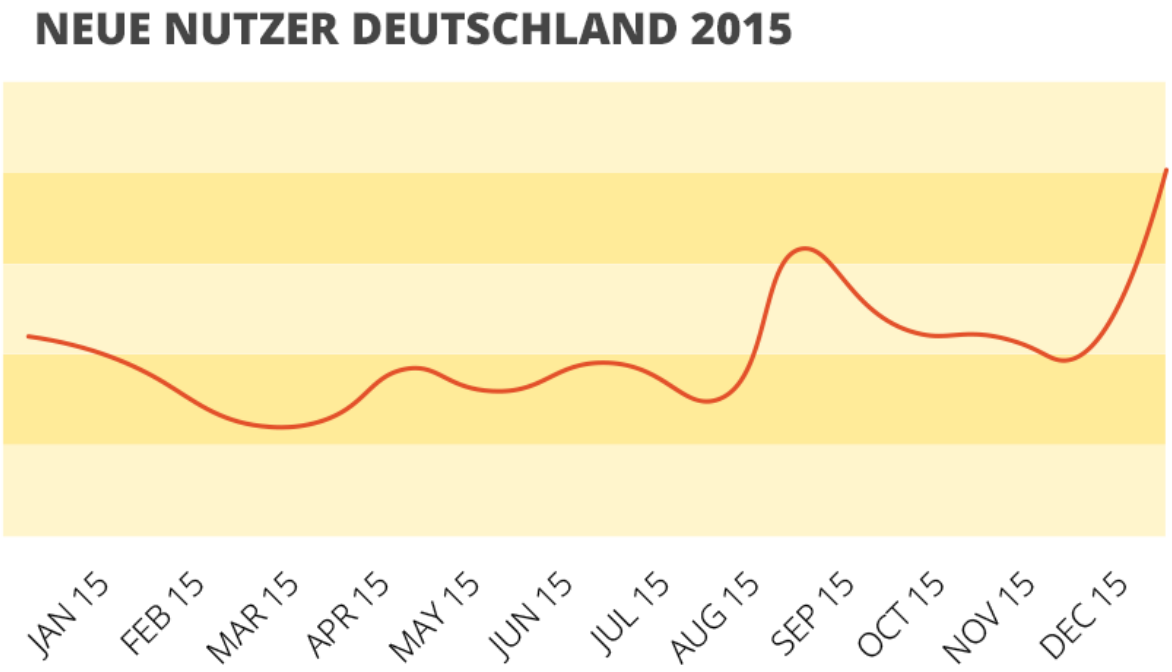
Übersicht Deutschland



Die Zahlen für Anfragen aus Deutschland gleichen sich dem globalen Trend an. Beschwerden wegen böswilliger Aktivitäten erhöhten sich um 115 %, während DMCA-Anforderungen um 27 % und polizeiliche Anfragen um 4 % zurückgingen.

Auch hier trug die innenpolitische Entwicklung zu einem Anstieg der Anwenderzahlen bei. Im Mai 2015 veröffentlichte WikiLeaks Transskripte der Arbeit des Parlamentarischen Untersuchungsausschusses zur NSA-Affäre über zehn Monate[2] und löste damit in interessierten Kreisen Betroffenheit und Bestürzung über die geheim gehaltenen Aktivitäten aus. Kurze Zeit später verklagte die Organisation ‚Reporter ohne Grenzen' auf Grundlage der Enthüllungen den Bundesnachrichtendienst (BND). Gleichzeitig stellte man klar, dass Quellenschutz und Whistleblower als kritische Komponenten freier journalistischer Untersuchungen, Recherchen und Berichterstattung empfunden werden.

[2] https://wikileaks.org/bnd-nsa/press/?english

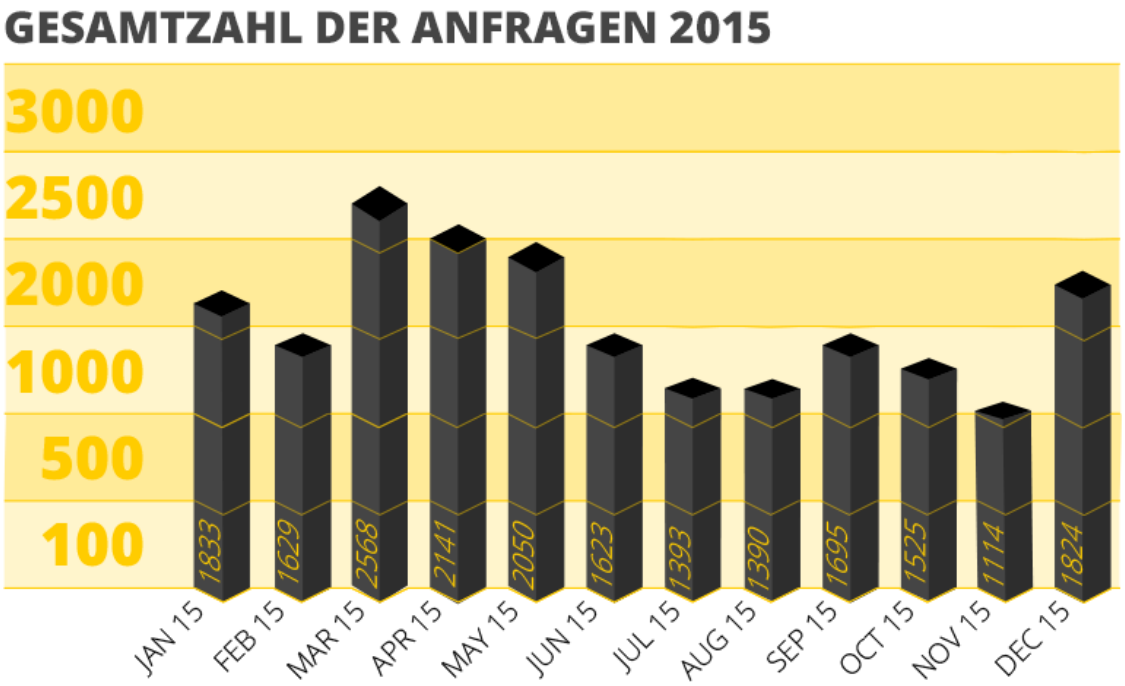


Entwicklung der Anwenderzahlen in Deutschland 01.2015-12.2015

Auch die internationale Berichterstattung im Sommer 2015 leistete einen Beitrag zum erhöhten Bewusstsein der Notwendigkeit des Schutzes vertraulicher Daten und der individuellen Privatsphäre. Beides zusammen lässt sich mit dem 60-%-igen Anstieg deutscher Nutzer in 2015 in Verbindung bringen.

Jenseits der Anfragen – Einblicke in die Herausforderungen zur Gewährleistung von Verschlüsselung und Anonymität

Um die Missbrauchsfälle zu reduzieren, ergreift Cyberghost verschiedene Maßnahmen, darunter die Sperrung von Ports in Ländern, in denen entsprechende Gesetze sowie daraus resultierender Druck auf Partner-Datenzentren die Verwendung von Peer-to-Peer-Protokollen wie Torrent einschränken oder unterbinden, so in den Vereinigten Staaten, Australien, Hongkong, Tokio, Singapur und Mexiko. Auch auf den freien Servern sind keine Peer-to-Peer-Verbindungen möglich.



Gegenläufige Entwicklung bei Urheberrechtsverstößen und Malware-Aktivitäten zwischen 09.2014 und 08. 2015

Weitere Maßnahmen wurden ergriffen, um Malware-Aktivitäten zu stoppen. Da die meisten Beschwerden die IP-Angabe der Quelle sowie des Opfers beinhalten, blockiert Cyberghost den Zugang zur Angreifer-IP, um zukünftige Attacken zu verhindern.

Ohne Partner kein VPN-Netzwerk

Die Zusammenarbeit mit Rechenzentren weltweit beinhaltet ständige Auseinandersetzungen mit den Betreibern, um die Interessen von VPN-Anwendern durchsetzen zu können. Auf der einen Seite stehen die meisten Rechenzentren unter dem Druck staatlicher Institutionen und lokaler Regierungsstellen, auf der anderen verfolgt Cyberghost eine strikte ‚Keine Protokolle'-Geschäftspolitik und kann daher Anfragen zu Nutzerdaten in steter Regelmäßigkeit nicht nachkommen. Dies führte in der Vergangenheit immer wieder zu unlösbaren Konflikten und Spannungen und sorgt dafür, dass es CyberGhost in verschiedenen Ländern sehr schwer hat, Server anzumieten, in erster Linie in den USA, Russland und der Tschechei. Verständlicherweise, denn die Zusammenarbeit mit CyberGhost zu unseren Bedingungen setzt die Rechenzentren der Gefahr aus, verklagt und durchsucht zu werden. Im Extremfall drohen die Beschlagnahmungen von Servern und sogar Geschäftsschließungen.

Zensur, staatliche Webfilter und Massenüberwachung

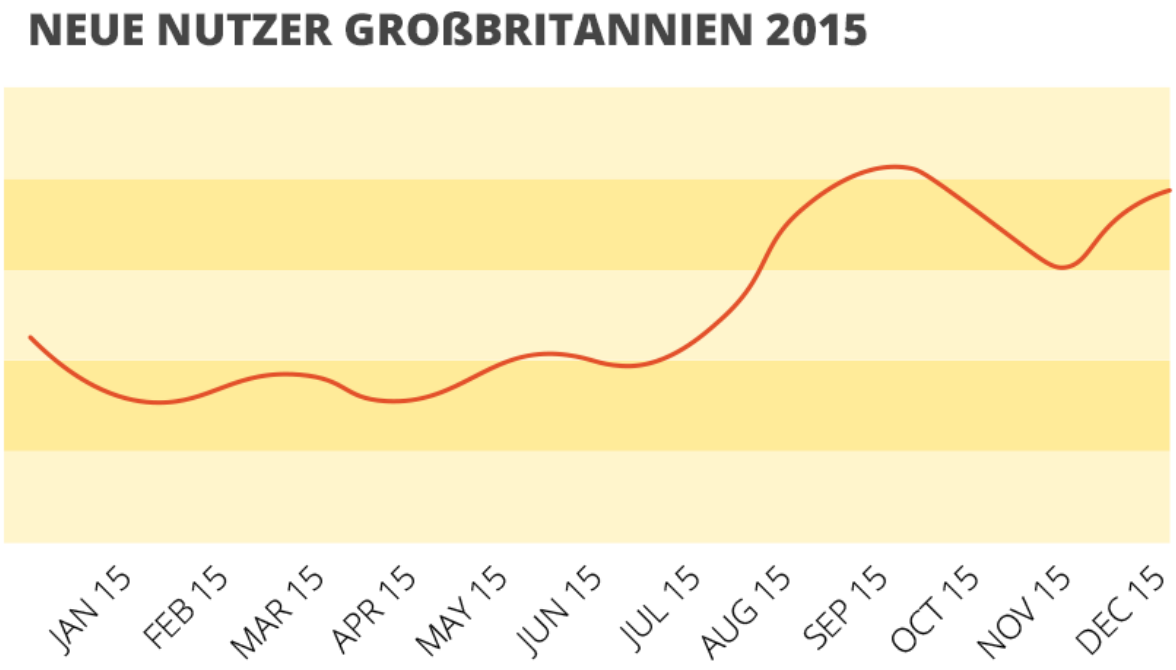
Die oben verschiedentlich vorgebrachten Gründe können als Antrieb gesehen werden, warum ein Internetanwender zu CyberGhost VPN greift, gleichzeitig wissen wir aber kaum etwas über die Motive, die dazu führen, dass Menschen ihre Online-Privatsphäre mit einem VPN schützen. Einige der erwähnten Gesetzesänderungen können direkt dazu geführt haben, andere erst durch ihre

Hervorhebung in den internationalen Medien und wieder andere erst durch ihre kumulative Wirkung.

Auch ließen die Anstrengungen von Regierungen, das Internet unter Kontrolle zu bringen, das Bewusstsein über Zensur, staatliche Webfilter und Massenüberwachung in den letzten zwölf Monaten generell ansteigen und trug ebenfalls zur Zunahme der Nutzerzahlen bei. Unabhängig davon, ob ein Staat zu den demokratischen oder nicht-demokratischen gezählt werden muss, verändern stetige gesetzliche ‚Anpassungen' die Online-Erfahrung der Bürger, beeinflussen die Wahrnehmung von Privatsphäre und fördern die Bereitschaft, Maßnahmen zur Verschlüsselung von Kommunikation und zur Herstellung von Online-Anonymität zu ergreifen. Im vergangenen Jahr erfuhren politisch so unterschiedlich aufgestellte Länder wie Pakistan, Iran, Großbritannien, Türkei, Russland und viele weitere entsprechende tiefgreifende Änderungen im gesellschaftlichen Zusammenleben, on- wie offline.

Großbritannien: Gerichtlich angeordnete Sperren

Obwohl nicht als Gesetz erlassen, das als direktes Zensurgesetz interpretiert werden könnte, ermöglicht der sogenannte ‚Abschnitt 97' trotzdem schwerwiegende Eingriffe in die Grundlagen einer freien Gesellschaft und ermöglicht Rechteinhabern, Internet Service Provider zu zwingen, Seiten zu sperren, die gegen Urheberrechte verstoßen. Solche Sperren basieren zwar offiziell auf Gerichtsbeschlüsse, allerdings werden diese unter Ausschluss der Öffentlichkeit angefertigt und können wegen ihres nicht überprüfbaren Charakters dazu führen, dass auch ‚saubere' Websites gesperrt werden.



Neue Anwender in Großbritannien 01.2015-12.2015

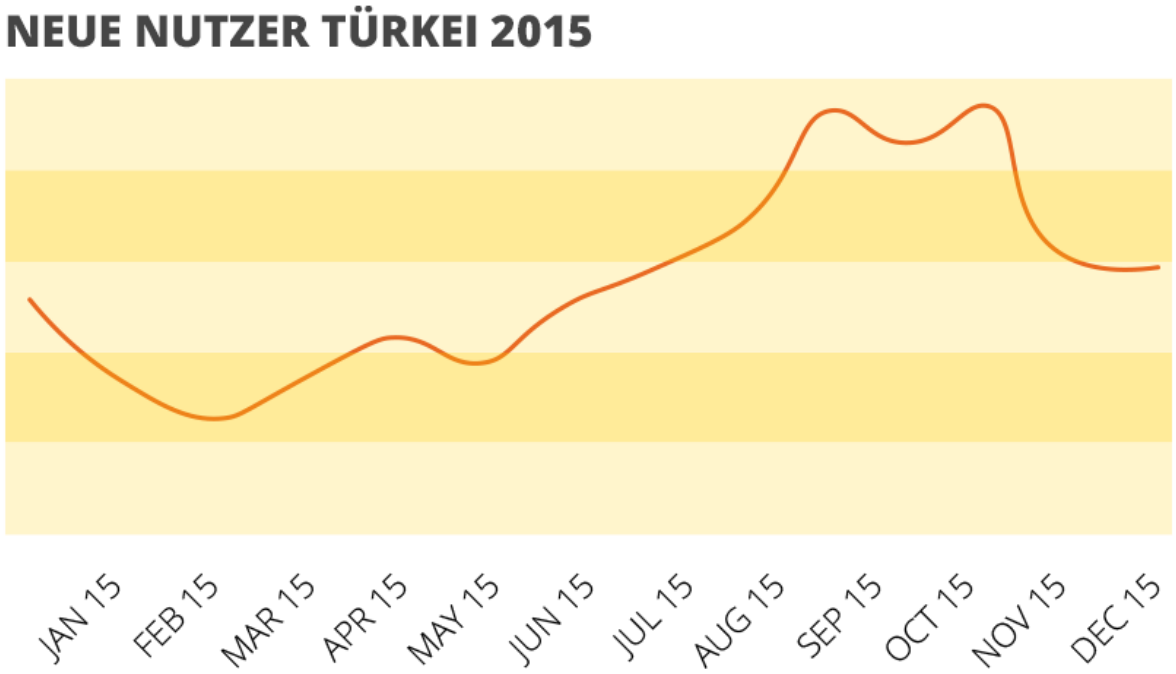
Türkei

In den letzten 12 Monaten behandelten internationale Medien gleich mehrere Gesetzesänderungen innerhalb der Türkei, die sich auch im Anstieg von CyberGhost-Nutzern reflektieren. So erlaubt ein vom türkischen Parlament am 5. Februar 2014 verabschiedetes Gesetz der Fernmeldebehörde (TIB) die Sperrung jeder beliebigen Website innerhalb von 4 Stunden ohne Gerichtsbeschluss. Ferner verpflichtet es Internet-Provider, alle Daten über die Webaktivitäten ihrer Kunden für zwei Jahre zu speichern und den Behörden auf Anfrage zur Verfügung zu stellen.

2015 erließ die Regierung mehrere Twitter-Verbote, wie das vom 22. Juli 2015, das erst per Gerichtsbeschluss aufgehoben wurde, als Twitter einwilligte, Bilder von einem im Südosten des Landes verübten Selbstmordanschlag zu entfernen. Diese vorübergehenden Verbote sozialer Medien ereignen sich in der Türkei mittlerweile regelmäßig.

Im April 2015 umfasste die Liste blockierter Websites durch das überwachende Unternehmen Engelli Web mehr als 78.000 Domainnamen.[3]

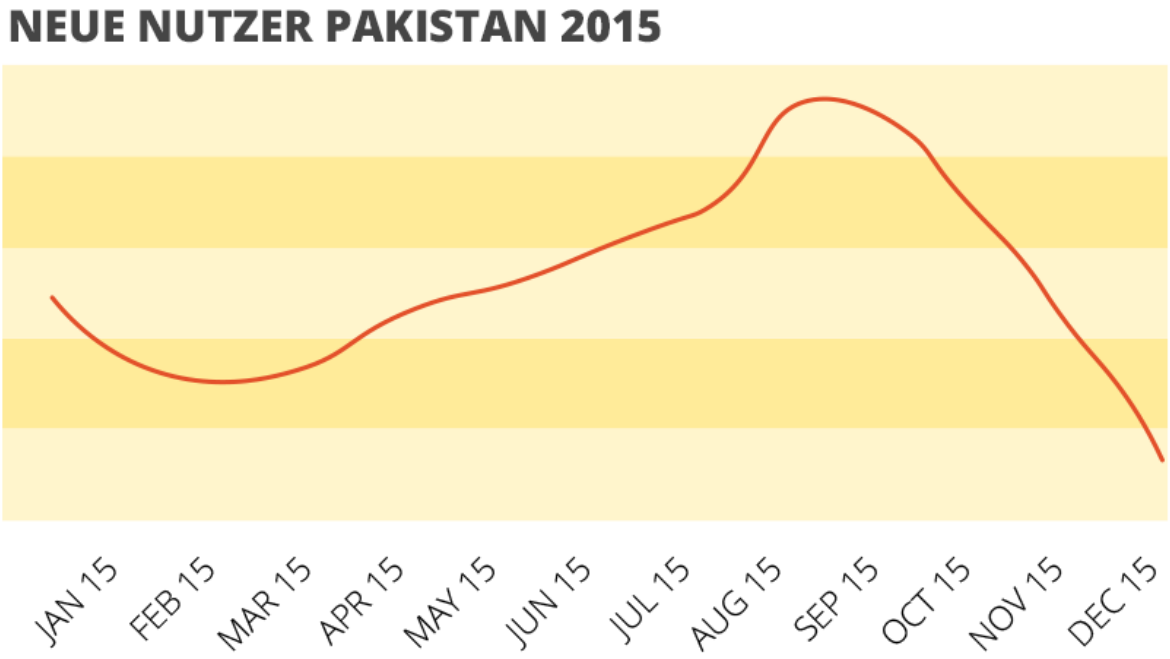
Im Licht dieser Ereignisse wird verständlich, dass der Zuwachs an türkischen CyberGhost-Nutzern mit 68 % im Jahr 2015 zu den höchsten Wachstumsraten innerhalb eines Landes gehört.



Neue Anwender in der Türkei 01.2015-12.2015

Pakistan konnte mit 73 % in nur 6 Monaten (03.2015 – 08.2015) die höchste CyberGhost-Wachstumsrate für sich verbuchen. Ein Grund für diesen enormen Anstieg kann im Verbot der Wordpress-Blogging-Plattform gesehen werden, die im März 2015 von der Pakistan Telecommunication Authority (PTA) als Bedrohung der nationalen Sicherheit eingestuft wurde[4].

[3] http://engelliweb.com/
[4] http://techcrunch.com/2015/03/22/wordpress-blocked-in-pakistan/



Neue Anwender in Pakistan 01.2015-12.2015

Auch **Russland** sah sich im vergangenen Jahr einem Anstieg strenger Zensurmaßnahmen ausgesetzt, darunter der Vorfall vom Juni 2015, als mehrere ISPs die 485 Milliarden Web-Seiten des Internet Archivs blockierten. Die Maßnahme folgte einer Anordnung, eine einzelne Seite wegen angeblicher Bewerbung ‚extremistischem Materials' zu zensieren. Die russische Regierung ging im August 2015 sogar noch einen Schritt weiter und sperrte kurzzeitig die Online-Bibliothek Wikipedia, nachdem sich die Betreiber weigerten, eine Webseite mit Informationen über die Vorbereitung und der Verwendung von Charas zu löschen, einer Form von Cannabis. Wikipedia war ein paar Stunden später wieder zugänglich, als die beanstandete Seite mit dem ‚Online-Inhalt über Drogenkonsum' entfernt worden war.

Auch das Cyber-Zahlungsmittel Bitcoin geriet ins Visier der staatlichen Zensur, weil es ‚zur Schattenwirtschaft beträgt'.[5] Dies führte zur Sperre von bitcoin.org und anderen Websites im Zusammenhang mit Bitcoin.

Die Sache mit dem Einkommen

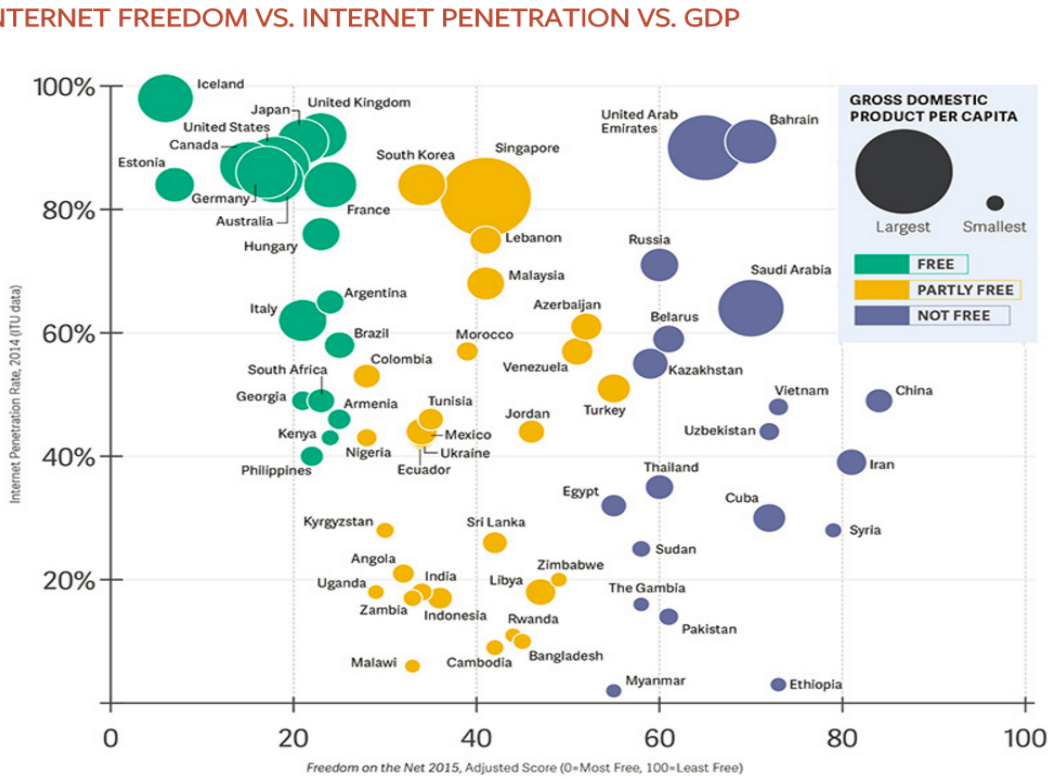
Die Top-8-Länder, in denen Cyberghost verwendet wird, lassen sich auch in finanzieller Hinsicht unterteilen: die zahlenden Kunden kommen aus den Top-4-Ländern Deutschland (mittleres Nettoeinkommen 2.315 €), USA (2360 €), Großbritannien (2810 €) und Frankreich (2223 €). Demgegenüber setzen sich die restlichen Plätze 5 bis 8 aus Ländern zusammen, in denen das durchschnittliche Nettoeinkommen 350 €[6] nicht übersteigt und in denen in erster Linie der kostenlose Service genutzt wird: Russland, Nigeria, Iran und Pakistan[7].

Die Daten zeigen ein Gleichgewicht zwischen beiden Nutzergruppen: Jenen, die einen sehr schnellen Service und Zugang zu mehr als 650 Servern auf der ganzen Welt genießen (und gleichzeitig den

[5] http://www.newsbtc.com/2015/01/13/russia-blocks-bitcoin-sites/

freien Zugriff unterstützen) und jenen, die nicht über die wirtschaftlichen Mittel verfügen, sich ein Premium-Abonnement leisten zu können – sehr oft Länder, in denen auch die Einhaltung von Menschenrechten zu bemängeln ist. Der CyberGhost-Free-Service basiert somit in erster Linie auf dem Beitrag, den die am meisten entwickelten Länder leisten.

Die aktuelle Studie ‚Freiheit im Netz 2015' von Freedom House.org, veröffentlicht im Oktober 2015, zeigt anschaulich die Korrelationen zwischen Internetfreiheit, Internetverbreitung und Bruttoinlandsprodukt.



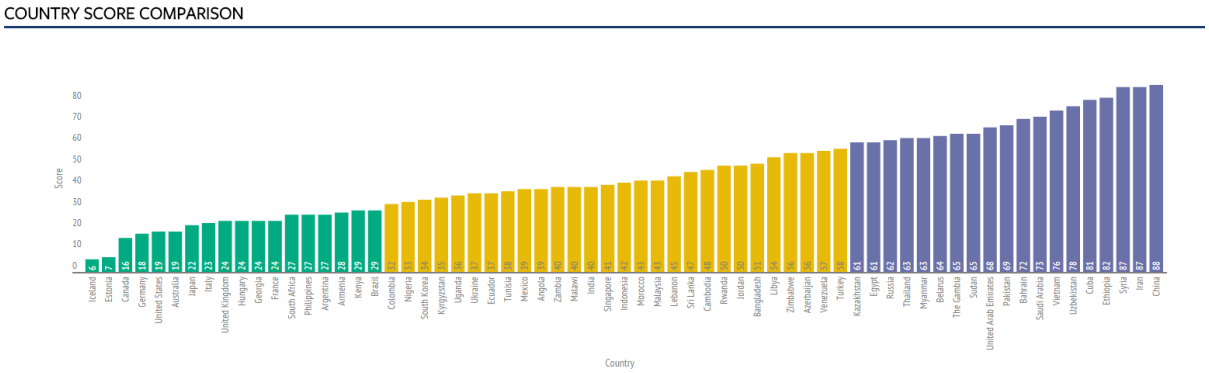
Ist Privatsphäre eine persönliche Angelegenheit?

Maßnahmen zur Aufklärung der Öffentlichkeit in Bezug auf Online-Sicherheit und Privatsphäre sollten auch die Nutzung von VPNs beinhalten. Mehrere Organisationen haben dem bereits Rechnung getragen und unterschiedliche Programme ins Leben gerufen, darunter die ‚BC AWARE-Kampagne für Privacy & Security Awareness[12]', der ‚Data Privacy Day' von www.staysafeonline.org, dessen Programm ‚Privatsphäre respektieren, Daten schützen und Vertrauen aufbauen[13]' (2013) neben Cyberghost auch die Homeland Security[14] unterstützte, sowie die 'Privacy Awareness Week', eine Initiative des Asia Pacific Privacy Authorities Forums (APPA) in Zusammenarbeit mit dem Büro des kanadischen Datenschutzbeauftragten[14] und viele weitere Kampagnen. Sie alle haben das Ziel, die Öffentlichkeit über die Bedeutung der Privatsphäre zu informieren. Einige dieser Kampagnen werden von staatlichen Institutionen rund um den Globus unterstützt …

Kann Privatsphäre gemessen werden?

Obwohl das Konstrukt ‘Privatsphäre’ naturgemäß individuell und kulturell unterschiedlich bewertet wird, existieren für die verschiedenen Ebenen möglicher Privatsphäre in verschiedenen Ländern durchaus Klassifizierungen in Form von Punkten (Scores), beispielsweise:

- BackgroundChecks.org schuf die sogenannte ‚Privatsphären-Anzeigetafel’ (Privacy Scoreboard), auf der verschiedene Merkmale eines Landes bewertet werden, darunter ob ein Land Privatsphären-Gesetze in Kraft gesetzt hat, Spionagesoftware einsetzt und die freie Rede unterstützt. Basierend auf diesen Kriterien liegen die besten Orte für Privatsphäre unter anderem in Spanien (+50), Tschechien (+50), Island (+50), Norwegen (+50) und Slowenien (+40). Am anderen Ende der Liste finden sich Bahrain (-25), Iran (-25), Nigeria (-20), Syrien (-20) und Malaysia (-20).
- DLA Piper misst die Regulierungsanstrengungen in jedem Land und platziert Kanada, Deutschland, Frankreich, Schweden, Norwegen und andere europäischen Staaten zu jenen mit hoher Internetregulierung und starker Durchsetzung entsprechender Gesetze, während die USA, Australien und Argentinien als stark regulierend und Russland, Ukraine, Süd-Afrika und Mexico überraschenderweise als moderat regulierend bezeichnet werden.
- Auf die Frage, wie privat sie verschiedene Arten persönlicher Daten einschätzten, verliehen die Teilnehmer der ‘Global Consumer Sentiment’-Umfrage (durchgeführt von der Boston Consulting Group im Jahr 2013[6]) ihren Kreditkartendaten den höchsten Wert, gefolgt von anderen finanziellen Daten, Information über Kinder und genetischen gesundheitlichen Prädispositionen.
- Freedom House veröffentlichte kürzlich den ‘Freedom on the Net 2015’-Report, der die aktuelle Lage der Freiheit im Internet beleuchtet und im fünften Jahr in Folge deren Niedergang diagnostiziert, „[…] weil mehr Regierungen Informationen von öffentlichem Interesse zensieren, während die Überwachung ausgeweitet und der Privatsphärenschutz kompromittiert werden.”[7]



Aus den Daten oben geht hervor, dass sich die Bürger der erwähnten Länder der Privatsphärenproblematik bewusst sind und verschiedene Maßnahmen zu deren Schutz ergreifen. Auf der anderen Seite benötigen und suchen Anwender in nichtdemokratischen Ländern Onlineschutz für ihre digitalen Identitäten. Die in der letzten Dekade geschaffenen Regulierungen und Privatsphären-relevanten Gesetze stehen in enger Verbindung mit diesem Verhalten.

Verschlüsselung: Die digitale Waffe, die alle verwenden sollten

---

6 https://www.bcgperspectives.com/content/slideshow/information_technology_strategy_digital_economy_data_privacy_by_the_numbers/#ad-image-0

7 https://freedomhouse.org/report/freedom-net/freedom-net-2015

Der von Cyberghost veröffentlichte Transparenzbericht zielt darauf ab, über die Art der Anfragen und Beschwerden an den Dienst zu informieren und das Bewusstsein für die eigentliche Tatsache zu schaffen, dass Online-Bürgerinnen und -Bürger beobachtet, überwacht und sogar verfolgt werden. Jeder, der im Internet unterwegs ist, sollte Verschlüsselung als ultimative Waffe betrachten, um die eigene Identität zu schützen.

Die Revolution der digitalen und technisierten Welt beginnt mit uns und den Maßnahmen, die wir ergreifen, unsere Identität zu schützen. Unsere Waffe in diesen digitalen Zeiten ist die Verschlüsselung. Julian Assange: „Kryptographie ist die ultimative Form der gewaltfreien direkten Aktion."

Die Verschlüsselung von Kommunikation auf allen Ebenen ist der Schlüssel zur Absicherung von Internetanwendern. Egal ob wir über vertrauliche Finanzinformationen reden, persönliche medizinische Daten, Identitätsdiebstahl, journalistische Recherche zu sensiblen Themen oder Informations- und Redefreiheit in nicht demokratischen Ländern: Daten müssen verschlüsselt werden. Verschlüsselung ist die einzige Möglichkeit, mit der sich digitale Bürger schützen können.

Wir betonen ausdrücklich den Kern aller unsere Aktivitäten: Cyberghost protokolliert keine Online-Aktivitäten. Datenschutz ist unser Kerngeschäft und unsere Leidenschaft. Cyberghost steht für ein freies Internet weltweit, für Meinungsfreiheit, freiem Informationsfluss und restriktionsloser Forschung in einem unzensierten Internet!

Aufruf an die IT-Industrie

Wir empfehlen der technischen Industrie, sich auf einen Standard-Transparenzbericht zu einigen, der relevante Daten für die Nutzer hervorhebt, nicht für Unternehmen. Wir alle müssen in die Lage versetzt werden, das Signal von den Geräuschen zu unterscheiden!

Da ein Teil der veröffentlichten Transparenzberichte für einige Tech-Unternehmen wenig mehr als PR-Kampagnen bedeuten, laden wir die EFF und anderen Organisationen ein, zwischen kooperativen Unternehmen zu vermitteln und eine Standardberichtsform zu entwickeln, die den Vergleich ähnlicher Daten erlaubt. Wir freuen uns auf zukünftige Kooperationen mit anderen Unternehmen, um diesen Standard für Transparenzberichte Realität werden zu lassen und einen wirklichen Unterschied zu machen, basierend auf Wahrheit.

Verweise:

Http://www.usnews.com/news/articles/2015/06/02/senate-passes-freedom-act-ending-patriot-act-provision-lapse
https://wikileaks.org/bnd-nsa/press/?english
http://www.revk.uk/2013/11/section-97a-orders.html
http://www.ispreview.co.uk/index.php/2013/08/open-rights-group-uk-pushes-for-isp-website-blocking-orders-to-be-public.html
https://freedomhouse.org/report/freedom-net/2013/turkey
http://engelliweb.com/
http://techcrunch.com/2015/03/22/wordpress-blocked-in-pakistan/
https://antizapret.info/site.php?id=5244
http://techcrunch.com/2014/12/03/github-russia/
http://www.newsbtc.com/2015/01/13/russia-blocks-bitcoin-sites/
https://en.wikipedia.org/wiki/list_of_countries_by_average_wage
http://www.tradingeconomics.com/russia/wages
https://freedomhouse.org/report/freedom-net/freedom-net-2015
http://www.bcaware.ca/about-us/why-this-campaign/
https://www.staysafeonline.org/
http://www.dhs.gov/national-cyber-security-awareness-month
https://www.priv.gc.ca/information/paw/index_e.asp
https://www.bcgperspectives.com/content/slideshow/information_technology_strategy_digital_economy_data_privacy_by_the_numbers/#ad-image-0
https://freedomhouse.org/report/freedom-net/freedom-net-2015