Glasfaserkabel und Spionage-U-Boote: Wie die NSA die Nervenzentren der Internet-Kommunikation anzapft

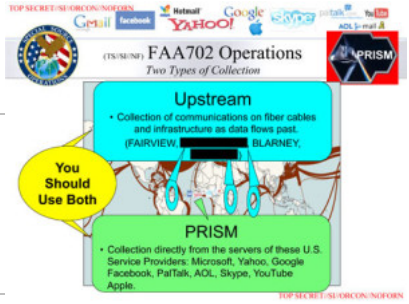
Von Andre Meister | Veröffentlicht: 20.06.2013 um 19:05h | 22 Antworten

Geheimdienste wie die amerikanische NSA nutzen viele verschiedene Technologien, um Kommunikationsverkehre abzuhören und zu speichern. Neben Kooperation mit Betreibern und dem Hacken von Systemen können sie auch die weltweiten Glasfaserleitungen direkt anzapfen. Das macht die NSA schon seit Mitte der Neunziger – ein Spionage-U-Boot nach 9-11 machte das zur Routine.

Große Teile der Daten im Internet laufen über Glasfaserkabel, viele internationale und interkontinentale Verbindungen laufen über Seekabel. In der sehenswerten Doku 20.000 Kabel unter dem Meer gibt es dazu weitere Informationen, auf cablemap.info eine interaktive Karte.

Der amerikanische Geheimdienst NSA zapft genau diese Kabel an. Das wurde durch eine Folie der PRISM-Präsentation öffentlich bestätigt, in der es heißt:

> *Collection of communications on fiber optic cables and infrastructure as data flows past.*
> *(FAIRVIEW, [redacted], BLARNEY, [redacted])*



Das geht natürlich am einfachsten, wenn der Eigentümer bzw. Betreiber des Kabels kooperiert und einfach eine Kopie der versendeten Daten liefert. Der Telekommunikationskonzern AT&T hat der NSA in San Francisco einfach einen eigenen Raum gegeben, in den es die Daten lieferte.

Doch auch ohne Mitwirkung der Firmen ist ein Anzapfen möglich und genau das tut die NSA. Die verschiedenen Techniken dahinter sind öffentlich bekannt:

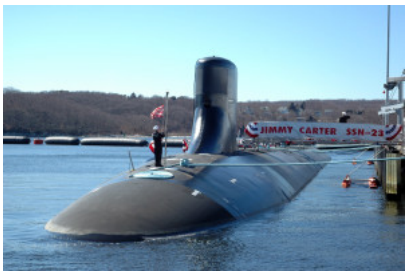
> *Die einfachste Attacke auf die Lichtsignale nutzt eine Auftrennung der Glasfaserstrecke (Splicing): Dabei schleifen Unbefugte ein zusätzliches Gerät zwischen Sender und Empfänger ein.*
>
> *Bei der Splitter-Coupler-Methode beispielsweise biegen Angreifer die Glasfasern, um mittels spezieller "Biegekoppler" heimlich auf den Informationsfluss zuzugreifen. Beim eigentlichen Empfänger ändert sich das Nutzsignal dabei nur kaum spürbar und auch der Netzwerkbetrieb leidet nicht darunter.*
>
> *Überhaupt nicht nachweisbar sind Einbrüche, die den direkten Kontakt mit der Datenleitung völlig vermeiden (non-touching methods). Solche Angriffsmethoden machen sich zunutze, dass aus jedem Kabel minimale Lichtmengen strahlen: Hochempfindliche Fotodetektoren fangen diese so genannte Rayleigh-Streuung auf und verstärken sie.*

Im Mai 2001 beschrieb Neil Jr. für das Wall Street Journal und ZDNet, dass amerikanische Behörden schon damals unbemerkt Unterseekabel angezapft haben. Noch vor 9-11.

Jahrzehntelang hat die NSA ihre Signals Intelligence-Überwachung durch das Abhören von Funksignalen gemacht. Weil die meiste Kommunikation ohnehin über Satelliten oder Richtfunk lief, war das ein leichtes Spiel für Systeme wie das weltweite Spionagenetz Echelon und Spionagesatelliten. Auch das Anzapfen der wenigen Kupferleitungen in den Ozeanen war vergleichsweise einfach.

Seit dem ersten Seekabel aus Glasfaser 1988 verschob sich die weltweite Kommunikation immer mehr auf die Übertragung von Licht. Die NSA hat das natürlich erkannt und schon Anfang 1989 Forscher-Teams in seiner Zentrale und Forschungszentren zusammengestellt, deren explizite Aufgabe die Entwicklung von Methoden zum Eindringen in Glasfaser-Kabel und Abschöpfen der Daten war. Und sie waren erfolgreich.

Die USA können nicht nur Überland-Glasfasern anzapfen, was auch Kriminelle tun, sondern auch die zentralen Untersee-Kabel, durch die ein Großteil der weltweiten Internet-Kommunikation fließt. Schon Mitte der Neunziger Jahre hat die NSA mit einem speziellen Spionage-U-Boot ein Unterseekabel in hunderten Metern Tiefe gespliced, also ein Gerät eingebaut, dass die Daten einfach an eine dritte Stelle leitet.



1997 haben NSA und Navy vorgeschlagen, das Atom-U-Boot USS Jimmy Carter für "Spezialoperationen" zu modifizieren und zum besten amerikanischen Spionage-U-Boot aufzubauen. 1998 stimmte der Kongress zu, das Boot mit "fortschrittlicher Technologie für spezielle Marinekriegsführung und taktische Überwachung" (Zitat Navy) auszurüsten. Eins der vielen Features ist: state-of-the-art Technologie zum Anzapfen von Untersee-Glasfaserkabeln.

Was schon in den Neunzigern durchgeführt wurde, ist für das 2,8 Milliarden Dollar teure U-Boot seit dem Stapellauf 2004 Routine. Zum Anzapfen kann die NSA nicht nur das "Biegen", sondern auch das "Splicen", laut Aussage von Beteiligten auch ohne entdeckt zu werden.

Was der NSA Ende des letzten Jahrtausends noch Probleme bereitet hat, waren die schier gigantischen Datenmengen, die sie mit dieser Methode abgehört haben. Damals sagte der NSA-Direktor Michael Hayden, dass die Technologie noch Feind der NSA sei. Aber die steigende Rechenleistung von Supercomputern und Mega-Rechenzentren ermöglichen es, "dass ein einzelner Analyst Informationen aus riesigen Mengen von Rohdaten extrahieren kann."

Genau was Edward Snowden sagt.

Wir wollen netzpolitik.org weiter ausbauen. Dafür brauchen wir finanzielle Unterstützung. Investiere in digitale Bürgerrechte.

« Zulassung großer Drohnen in den zivilen Luftraum wird zur Angelegenheit militärischer Luftfahrtbehörden

Jung & Naiv – Folge 64: Soldateneinsatz im eigenen Land »

22 Kommentare

1. tfhfg
   Am 20. Juni 2013 um 19:27 Uhr veröffentlicht | Permalink
   wieso die schwarzen Balken?

   Antworten

   Andre Meister
   Am 20. Juni 2013 um 20:27 Uhr veröffentlicht | Permalink
   Das hätten wir auch gerne gewusst. Die sind nicht von uns, sondern von der Washington Post. Wir würden auch gerne die Original-Folien veröffentlichen, haben sie aber leider nicht.

   Antworten

   an_o_nym
   Am 21. Juni 2013 um 05:15 Uhr veröffentlicht | Permalink
   Weil es für die US Regierung peinlich sein könnte und US-Amerikaner eine heilige patriotische Pflicht haben..... ?
   Journalisten haben sich besonders daran zu halten und wegen irgendwelchen Fake-Anklagen im Gefängnis zu sitzen ist auch nicht schön.

   Antworten

   superguppi
   Am 21. Juni 2013 um 20:21 Uhr veröffentlicht | Permalink
   Orte oder Kabel-Namen.
   Südamerika: Panama oder Columbien oder Honduras
   Afrika: Kenia oder Tansania
   Kabel Südafrika- Singapur

   Antworten

2. D. Lux
   Am 20. Juni 2013 um 20:13 Uhr veröffentlicht | Permalink
   Das finde ich viel spektakulärer als Echelon und PRISM

   Antworten

European Digital Rights
Free Software Foundation Europe
Logbuch:Netzpolitik
net-politics.eu
newthinking.de
re:publica

3. Erik
Am 20. Juni 2013 um 20:27 Uhr veröffentlicht | Permalink

Ich glaube mich zu erinnern, dass die NSA auch vor 9-11 (wahrscheinlich eher im Kalten Krieg) Unterseekabel per U-Boot "angegriffen" hat, um abzuhören. Stand im NSA-Buch von James Bamford. Hab es leider nicht zur Hand…

Antworten

4. Krabbler
Am 20. Juni 2013 um 20:38 Uhr veröffentlicht | Permalink

Die schauen zu viele Agentenfilme, die Amis. *kopfschüttel*
Danke für die Recherche!

Antworten

5. yves
Am 20. Juni 2013 um 21:27 Uhr veröffentlicht | Permalink

Ich frage mich eher, warum die Telekommunikationsfirmen, die die Seekabel betreiben den Datenstrom nicht einfach verschlüsseln. Unabhängig von der NSA muss man doch fast von sowas ausgehen…

Antworten

> Jakob
> Am 20. Juni 2013 um 22:43 Uhr veröffentlicht | Permalink
>
> Warum sollten sie? Sind ja nicht deren Daten, sondern "nur" die Daten der Nutzer…
>
> Antworten
>
> > Pirat
> > Am 21. Juni 2013 um 00:26 Uhr veröffentlicht | Permalink
> >
> > Die "Nutzer" könnten aber auch Russische oder Chinesische Firmen sein, denke nicht das es im Volkswirtschaftlichen Interesse wäre wenn diese abgehört und so Industriespionage betrieben würde. D.h dürften die entsprechenden Regierungen ja wohl ein Interesse daran haben das das verschlüsselt wird.

6. krokodoc
Am 20. Juni 2013 um 22:50 Uhr veröffentlicht | Permalink

War z.B. 2008 ein Thema als innerhalb kürzester Zeit mehrere Kabel im Mittelmeer "von Ankern zerstört" wurden.

http://edition.cnn.com/2008/TECH/02/08/internet.outage/
"Fundamentally, if somebody wants to cut a cable, they can do so — all you need to do is go trawling with an anchor," said Stephan Beckert an analyst with TeleGeography, a research company that consults on global Internet issues. He scoffed at conspiracy theories posted online by what he calls "the tin-foil hat crowd."

Oder hier mit dem Unterpunkt "Conspiracy Theories"
https://en.wikipedia.org/wiki/2008_submarine_cable_disruption#Cause_of_cable_brea

Antworten

> Pirat
> Am 21. Juni 2013 um 00:27 Uhr veröffentlicht | Permalink
>
> Wäre ja mal was für Terroristen, die Internetkabel zwischen EU und USA kaputt machen, dann wäre das Internet futsch und es würde zur Weltwirtschaftskrise kommen.
>
> Antworten

7. Tat-1
Am 21. Juni 2013 um 03:09 Uhr veröffentlicht | Permalink

Surftip – interaktive(!) Karte der Unterseekabel.
Nicht vom Retrodesign abschrecken lassen.

http://submarine-cable-map-2013.telegeography.com/

Antworten

8. chatter
Am 21. Juni 2013 um 08:03 Uhr veröffentlicht | Permalink

hallo

gibt es eigentlich noch etwas was nicht angezapft wird? heute kann man doch wirklich kein einzigen schritt mehr ohne überwachung und abhörungen machen. mir scheint wir haben uns daran schon zu sehr gewöhnt und es stört niemanden mehr. selbst die zeiten des sorglosen chattens ist längst vorbei

Antworten

9. Tobias
Am 21. Juni 2013 um 10:03 Uhr veröffentlicht | Permalink

Das scheint mir ein sehr kostspieliges Unterfangen zu sein, wenn man den tatsächlichen Nutzen abwägt. Auch wenn man weniger zweckrational an die Angelegenheit herangeht und das ganze wertrational bewertet, frage ich mich wieso Kosten für jedes Sozialprojekt (Bildung, Gesundheitsvorsorge, Arbeitslosenversicherung, Armutsbekämpfung) oder Infrastrurkturprojekte (Netzausbau, Instalthaltung) einer immensen öffentlichen Kontroverse unterzogen werden und als erstes von Austeritätsbestrebungen in den Blick genommen werden, während die Kosten für solche Geheimoperationen nicht nur verschwiegen werden, sondern gar nicht erst Teil der öffentlichen Diskurse sind. Jede Debatte darüber wird lapidar mit Phrase abgewürgt (»Neuland«. »Sicherheit«, »War on Terror«).

Die Frage ist allerdings ob die so dargestellten Bedrohungsszenarien wirklich so dramatisch sind, dass es den Aufbau einer Überwachungsgesellschaft rechtfertigt, die zuerst alle Ressourcen für Solidarität und Infrastruktur reduziert, bevor Maßnahmen debattiert werden, die weder mit dem demokratischen Selbstverständnis ohne weiteres vereinbar sind und dabei auf ein offenbar in Teilen eher fiktives Bedrohungspotential zurück greift. Metaphern, wie die einer Wall oder Stadtmauer greifen nur bedingt, da die Konstruktion einer Stadtmauer nur bedingt gegen die eigenen Bürger eingesetzt werden kann. Vielleicht geht es am Ende eher um die Entwicklung von Maßnahmen, um bestehende Ordnung um jeden Preis erhalten und stablisieren zu können, ohne zu berücksichtigen, welche fatale Folgen die Beraubung politischer Dynamik für Gesellschaften haben kann, insbesondere solche in denen ein demokratisch-konstitutives und rechtsstaatliches Selbstverständnis weit verbreitet scheint.

Antworten

> Kurt
> Am 21. Juni 2013 um 10:32 Uhr veröffentlicht | Permalink
>
> Was mir bei solchen Enthüllungen immer wieder auffällt: “Normale” Bürger wie Du und ich können einfach die Gedankengänge krimineller Psychopathen nicht nachvollziehen. Das ist dann die Ursache für den inflationären Gebrauch des Wortes “Verschwörungstheoretiker”.
>
> Antworten

10. Wolfgang
Am 21. Juni 2013 um 14:52 Uhr veröffentlicht | Permalink

Bleibt mal auf dem Teppich. Habt ihr einen Plan, welche Datenvolumen über diese optischen Kabel gehen? Diese Datenvolumen kann man weder ad-hoc in einem U-Boot verarbeiten, noch irgendwo wegspeichern auf dem U-Boot und dann nachträglich scannen. Und das müsste man dann ja für ALLE Transatlantikkabel machen.
Es ist schon eher wahrscheinlich, dass da nicht auf dem Grund des Ozeans, sondern direkt beim Einspeisepunkt auf dem Festland gescannt wird.
Aber ja, in Zeiten des kalten Kriegs haben die Amis glaub ich mal eine diplomatische (elektrische) Telefonleitung der Russen im Meer angezapft. Aber verglichen zum Anzapfen einer optischen Glasfaser und dem Demultiplexen dieser Hochgeschwindigkeits-Datenströme war das aus heutiger Sicht ein Kinderspiel.

Antworten

> Phiber Optic
> Am 21. Juni 2013 um 15:12 Uhr veröffentlicht | Permalink
>
> Warum gescannt? Das kann alles in Datenzentren wie Utah gedumpt werden.
>
> Am angezapften Kabel bleibt das U-Boot natürlich nicht hängen, sondern installiert einen Splitter und legt eine eigene Faserleitung von dort zum eigenen RZ.
> Ja, beim Einspeisepunkt ist das einfacher, das geht aber nur mit Kooperation des Betreibers. Und das geht, wenn überhaupt, nur im eigenen Land.
>
> Kabel anzapfen geht überall.
>
> Antworten
>
> > Wolfgang
> > Am 21. Juni 2013 um 17:00 Uhr veröffentlicht | Permalink
> >
> > Aus technischer Sicht stimme ich dir zu, das könnte man so machen. Die Kosten dafür mal außer Acht gelassen …

11. Sascha
Am 24. Juni 2013 um 20:55 Uhr veröffentlicht | Permalink

Warum kann ich mit Safari/Mac hier keine Comments posten?

Was mir fehlt in der Diskussion ist der Moment “Was wird angefangen mit den

Daten”. Also so in etwa: Du bist einer von vielen gutbezahlten Mathematiker, Soziologen oder Statistiker bei einer der Geheimdienste. Bekommst nen Haufen stets aktualisierter Daten und einen direkten Echtzeitzugriff. Keine direkten Inhalte nur Verbindungsdaten von Mobiles, Mobile-Net, Kabelnetz, Telefon – Telnummern, IPs, Dauer, Datum und Uhrzeit. Wer mit wem, wann und wo. Zur Korrelation der Daten hast du gleichzeitig Zugriff auf eine Datenbank mit aktuellen Ereignissen.

Was fällt dir ein, was kann man den Daten machen? Was geht da?

Antworten

Edward Snowden

Am 25. Juni 2013 um 11:35 Uhr veröffentlicht | Permalink

Alles speichern, so lange es geht. Dafür gibt es Datencenter wie Utah. Mindestens alles Verschlüsselte speichern, bis man es entschlüsseln kann. Aus allen Verbindungsdaten einen sozialen Netzwerk-Graphen der kompletten Weltbevölkerung machen. Permanente Rasterfahndung nach festzulegenden Kriterien. “Interessante” Kommunikation auf ewig speichern.

Antworten

Hans Speck

Am 25. Juni 2013 um 15:50 Uhr veröffentlicht | Permalink

Wie KURT oben schon sagte: ““Normale” Bürger wie Du und ich können einfach die Gedankengänge krimineller Psychopathen nicht nachvollziehen.” Denen fällt in ihren Allmachtsphantasien schon noch einiges ein, wie sie uns allseits beherrschen wollen oder nach welchen Kriterein sie uns dann sortieren werden – in “überlebenswert” oder “nicht”…

Und außerdem: glaubst Du wirklich, daß die Inhalte nicht auch ausgewertet werden?
Ich meine, bis jetzt ist es schon immer so gewesen, daß das was technisch MÖGLICH war, auch GEMACHT wurde – egal ob es ungesetzlich war oder ethisch bedenklich oder unmoralisch – siehe Klonen etc.
Also…

Antworten

Einen Kommentar hinterlassen

Ihre E-Mail wird *niemals* veröffentlicht oder weitergegeben. Erforderliche Felder sind mit * markiert

Name *
NAME_FULL
E-Mail *
EMAIL_ADDRESS
Website
UNKNOWN_TYPE
Kommentar

Sie können diese HTML-Tags und -Attribute verwenden `<a href="" title=""> <abbr title=""> <acronym title=""> <b> <blockquote cite=""> <cite> <code> <del datetime=""> <em> <i> <q cite=""> <strike> <strong>`

Absenden