

1 Langfassung:

2
3 Das Open Root Server Network (ORSN) startet den Betrieb

4
5 **Das Open Root Server Network (ORSN)**, eine private Initiative zur
6 Bereitstellung von Root-Nameservern, **startet am 13. August 2013 seine**
7 neu initiierte **Arbeit**. Das Open Root Server Network (ORSN), welches
8 bis 2008 bereits existierte und nun neu gestartet wurde, soll
9 möglichen staatlichen Zensurversuchen bei dem Betrieb des weltweiten
10 Internets vorbeugen. Es werden DNS-Root-Server in Europa bereit-
1 gestellt, die als Nachschlagewerk für sämtliche Internetadressen
2 dienen sollen. Hauptvorteil des Open Root Server Network (ORSN) ist
3 die dezentrale und zensur-unabhängige Struktur, die neben den Root-
4 Servern der ICANN betrieben werden soll. Die ICANN allerdings, und
5 somit auch die Namensauflösung im Internet, untersteht dem US-
6 Amerikanischen Handelsministerium.

7
8 „Gerade in Zeiten der Abhörprogramme PRISM und TEMPORA ist eine
9 staats-unabhängige Alternative zu den bestehenden Servern für das
10 freie Internet lebensnotwendig. Davon profitieren die Menschen und die
1 Wirtschaft in allen Ländern.“ so Markus Grundmann, der Gründer der
2 Initiative.

3
4 Durch die Domain Name Server (DNS) wird das Internet in der heutigen
5 Form erst nutzbar. So wird bei der Eingabe in Webbrowsern, wie z.B.
6 InternetExplorer, Safari oder Firefox, die Web-Adresse in eine
7 mehrstellige Zahlenkolonne umgewandelt, der sog. IP-Adresse. Mit
8 dieser erst kann eine Webseite oder andere Dienste aufgerufen werden.
9 So wird z.B. aus der Webseite „bund.de“ durch nachfragen bei dem
10 Domain Name Server (DNS) die IP-Adresse 77.87.229.48. Von dieser IP-
1 Adresse kann dann der Inhalt der Webseite abgerufen werden. Wenn also
2 dieses „Adressbuch“ gelöscht, blockiert oder manipuliert werden kann,
3 dann hätte das ernsthafte Auswirkungen auf die private Kommunikation
4 aber auch auf sämtliche Wirtschaftsbereiche in Deutschland, Europa und
5 der Welt.

6
7 Das Open Root Server Network (ORSN) will dieser Unsicherheit
8 entgegenwirken, indem zahlreiche Root-Server, verteilt auf viele
9 europäische Länder, wie z.B. Frankreich, Portugal, Deutschland,
10 Niederlande, Italien, Griechenland, Österreich, Schweiz, Luxemburg,

1234567890123456789012345678901234567890123456789012345678901234567890



c/o Markus Grundmann
Schlossstrasse 25
38179 Schwuelpen
Germany

contact@orsn.org

<http://www.orsn.eu>

1 die Adressbuch-Funktion übernehmen, auch wenn die amerikanische
2 Zentrale gestört oder manipuliert werden sollte.

3 Die Mitarbeiter des Open Root Server Network (ORSN) legen Wert darauf,
4 dieses parallele Netzwerk aus Sicherheitsgründen betreiben zu wollen.
5 Zum einen soll dem Ungleichgewicht der Einflussmöglichkeiten zwischen
6 den USA und Europa entgegengewirkt werden, und zum anderen ist es
7 technisch durchaus sinnvoll, bei einem Cyberangriff eine Alternative
8 bereit zu halten.

9
10 Neben dem Initiator Markus Grundmann besteht das Open Root Server
1 Network (ORSN) aus ehrenamtlichen Privatpersonen aus Deutschland und
2 Europa, die einen Teil Ihrer Freizeit und Ihrer Computer-Hardware für
3 die „Adressbuch-Funktion“ im Internet bereitstellen.

4 Das Open Root Server Network (ORSN) stützt sich bei seiner Arbeit auf
5 eine breite Community und deren freiwillige Kontrolle und Transparenz.
6 ORSN ist ein 100%-kompatibles Root-Server Netzwerk zu den Systemen der
7 amerikanischen ICANN. Keine TLD (Top-Level-Domain) mehr oder weniger
8 wird in der ORSN-Datenbank Einzug halten.

9 Die Kontrolle liegt bei der Community und damit bei den Menschen, die
20 das Internet so interessant machen, und den Bürgern in den jeweiligen
1 Ländern, die im Internet gezielt Daten und Informationen
2 bereitstellen.

3
4 Das Open Root Server Network (ORSN) setzt auf Transparenz und auf
5 Datensicherheit. Geeignete Schutzmechanismen der Community werden auch
6 in Zukunft dafür sorgen, dass keine Nation auf dieser Welt einfach vom
7 Internet abgeschnitten wird.

8
9 Weitere Informationen gibt es unter www.ORSN.org.

30
1 (494 Worte / 3669 Zeichen)

2
3
4 **Kurzfassung:**

5
6 **Open Root Server Network gestartet**

7
8 **Das Open Root Server Network (ORSN) startet am 13. August 2013 seine**
9 **Arbeit.** Das Open Root Server Network (ORSN) soll möglichen staatlichen
40 Zensurversuchen bei dem Betrieb des weltweiten Internets vorbeugen. Es

Pressekontakt:
press@orsn.org

1 werden DNS-Root-Server in Europa bereitgestellt, die als
2 Nachschlagewerk für sämtliche Internetadressen dienen sollen.
3 Hauptvorteil des Open Root Server Network (ORSN) ist die dezentrale
4 und zensurunabhängige Struktur, die neben den Root-Servern der US-
5 amerikanischen ICANN betrieben werden soll.

6
7 „Gerade in Zeiten der Abhörprogramme PRISM und TEMPORA ist eine
8 staats-unabhängige Alternative zu den bestehenden Servern für das
9 freie Internet lebensnotwendig. Davon profitieren die Menschen und die
10 Wirtschaft in allen Ländern.“ so der Gründer Markus Grundmann.

1
2 Durch die Domain Name Server (DNS) wird das Internet in der heutigen
3 Form erst nutzbar. So wird bei der Eingabe in Webbrowsern die Web-
4 Adresse in eine sog. IP-Adresse umgewandelt. Mit dieser kann eine
5 Webseite erst aufgerufen werden. Wenn also dieses „Adressbuch“
6 gelöscht, blockiert oder manipuliert werden kann, dann hätte das
7 ernsthafte Auswirkungen auf die private Kommunikation aber auch auf
8 sämtliche Wirtschaftsbereiche in Deutschland, Europa und der Welt.

9
10 Das Open Root Server Network (ORSN) will dieser Unsicherheit
1 entgegenwirken, indem zahlreiche Root-Server die Adressbuch-Funktion
2 übernehmen, auch wenn die amerikanische Zentrale gestört oder
3 manipuliert werden sollte.

4 Die Mitarbeiter des ORSN legen Wert darauf, dieses parallele Netzwerk
5 aus Sicherheitsgründen betreiben zu wollen. Es soll aber auch dem
6 Ungleichgewicht der Einflussmöglichkeiten zwischen den USA und Europa
7 entgegenwirken.

8
9 Neben dem Initiator Markus Grundmann besteht das Open Root Server
10 Network (ORSN) aus ehrenamtlichen Privatpersonen.

1 Das Open Root Server Network (ORSN) stützt sich bei seiner Arbeit auf
2 eine breite Community und deren freiwillige Kontrolle und Transparenz.
3 ORSN ist ein 100%-kompatibles Root-Server Netzwerk zu den Systemen der
4 amerikanischen ICANN.

5
6 Das Open Root Server Network (ORSN) setzt auf Transparenz und auf
7 Datensicherheit. Geeignete Schutzmechanismen der Community werden auch
8 in Zukunft dafür sorgen, dass keine Nation auf dieser Welt einfach vom
9 Internet abgeschnitten wird.

1 Weitere Informationen gibt es unter www.ORSN.org.

2
3 (317 Worte / 2347 Zeichen)
4
5
6

7 Hintergrundinformationen:
8

9 **Wie funktioniert das Browsen im Internet?**

10 Wenn eine Benutzer (wir nennen ihn mal Michel D.) im Internet surft,
1 oder seine Bankgeschäfte erledigt, dann gibt er meist eine eindeutige
2 Web-Adresse in Form von www.meineBank.de in seinen Web-Browser ein.

3 Der Browser allerdings weiß damit ersteinmal nichts anzufangen und
4 schaut ganz selbstständig in einem Internet-Adressbuch beim Provider
5 vom Michel D. nach, der Provider tut das selbse auch, und dessen
6 Provider auch. Alle fragen also bei den sog. Domain Name Servern nach
7 „wie heißt die richtige Adresse wenn Michel D. www.meineBank.de
8 aufrufen will“. Als Ergebnis erhält der Computer von Michel D. die
9 Antwort „Die richtige Adresse von www.meineBank.de lautet:

20 <http://123.45.67.89>“. Also ruft der Browser von Michel D. Diese
1 Adresse auf und zeigt die dann erhaltenen Daten auf dem Bildschirm an.
2 Michel D. kriegt von all dem nichts mit, weil sein Computer und „das
3 Internet“ diese Kommunikation rasend schnell im Hintergrund erledigen.
4 Michel D. ist dann zufrieden, dass er die gewohnte Webseite seine Bank
5 sieht, ohne zu wissen, ob die IP-Nummer, die sein Computer im
6 Hintergrund erhalten hat tatsächlich von seiner Bank stammt.
7

8 **Sind Daten im Internet sicher?**

9 Daten können im Internet sicher sein, allerdings nur wenn die Systeme
30 transparent und überprüfbar sind.

1 Zur Zeit allerdings ist weltweit nur eine zentrale Stelle für die
2 Namen und die Zuordnung der IP-Adressen zuständig. Dies ist die ICANN,
3 die zudem auch noch dem amerikanischen Handelsministerium unterstellt
4 ist. Mit einer dazu parallelen Struktur, wie es die Initiative Open
5 Root Server Network (ORSN) bereitstellen will, wird es zu dieser einen
6 zentralen Stelle eine Alternative geben. Der Benutzer könnte sich
7 entweder auf die „Amerikaner“ oder die „Europäer“ verlassen. Michel D.
8 oder seine Internet-Provider könnten aber auch bei beiden Name-Server-
9 Netzwerken die endgültigen Adressen erfragen und diese vergleichen mit
40 dem möglichen Ergebnis „wenn beide gleich sind, dann wird es wohl

1 stimmen".

2
3 **Mir kann doch nichts passieren, oder?**

4 Jedem Internet-Nutzer kann es entweder aus böser Absicht oder aufgrund
5 eines Computerfehlers passieren, dass er oder sie eine falsche oder
6 gefälschte IP-Adresse zurückerhält. Der Benutzer Michel D. wird das
7 sicherlich nicht merken und der angezeigten Webseite vertrauen.

8 Drei extreme Szenarien könnten aber durchaus eintreten:

9 Bei einem technischen Fehler des zentralen Name-Server-Systems könnte
10 eine falsche IP-Adresse verschickt werden, dann erhält Michel D. nicht
1 die Seite seiner Bank, sondern eine andere Webseite, die vielleicht
2 einen Computervirus auf Michel D.s Computer einschleust. Das will
3 Michel D. sicher nicht.

4 Es könnte aber auch sein, dass eine kriminelle Bande die IP-Adressen
5 manipuliert. Für solche Manipulationen sind einzelne zentrale Systeme
6 besonders gut geeignet. Dann würde Michel D. vielleicht eine Seite
7 sehen, die genauso aussieht, wie die Webseite seiner Bank. Der würde
8 er wohl vertrauen und seine Bankdaten und PIN eingeben. Damit wären
9 seine Bankdaten abgefischt, vielleicht inzwischen sein Bankkonto
20 bereits leer geplündert. Das will Michel D. sicher auch nicht.

1 Oder es könnte sein, dass europäische und amerikanische Gerichte oder
2 Behörden einfach unterschiedlicher Meinung sind. Dann könnte z.B. eine
3 europäische Bank in Amerika auf der Liste der Unterstützer der
4 Schurkenstaaten stehen. Das US-Handelsministerium würde dann
5 vielleicht die IP-Adressen dieser Bank sperren oder auf eine
6 Hinweisseite umleiten. Damit könnte Michel D. und viele Firmen in
7 Europa ihre Bankgeschäfte nicht mehr erledigen. Michel D. würde
8 vielleicht eine Pfändung wegen nicht bezahlter Rechnungen erhalten.
9 Das will Michel D. auf gar keinen Fall.

30
1 **Warum soll in Europa eine Alternative zu dem amerikanischen ICANN**
2 **etabliert werden?**

3 Das Internet mit seinen vielen über die ganze Welt verteilten
4 Computern und Netzen ist heute aus dem privaten und wirtschaftlichen
5 Leben nicht mehr wegzudenken. Viele Strukturen sind aber immer noch
6 historisch „gewachsen“, so auch die eine, zentrale Vergabestelle ICANN
7 in den vereinigten Staaten. So eine einzige Stelle ist immer
8 angreifbar und damit unsicher, selbst wenn technisch alle
9 Sicherheitsvorkehrungen getroffen wurden.

40 Das Open Root Server Network (ORSN) will also keine Konkurrenz

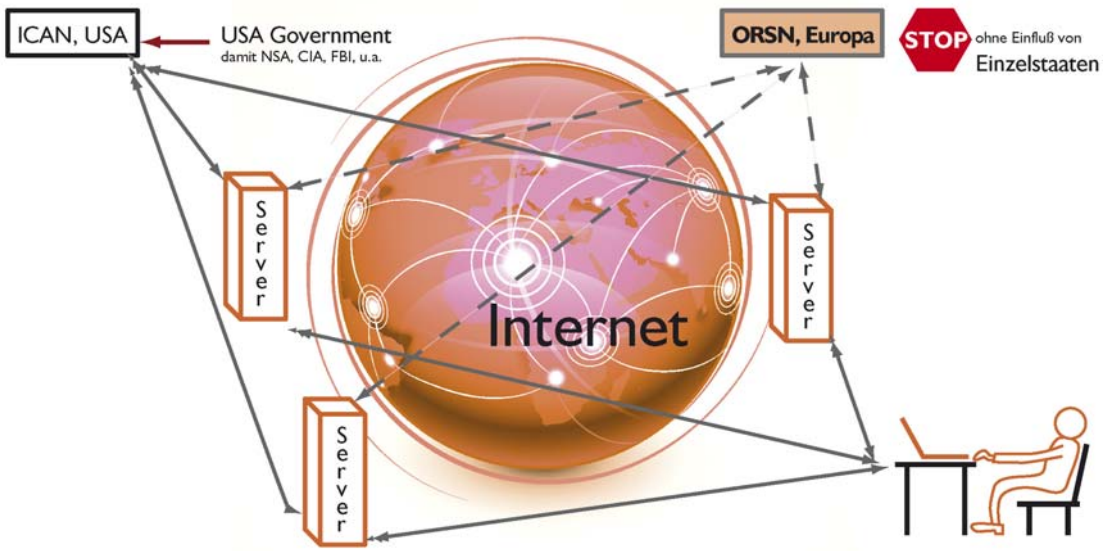
1 aufbauen, sondern eine technische Alternative bereitstellen,

- 2 • die Außerhalb der USA existiert,
- 3 • von staatlichen Stellen unabhängig ist,
- 4 • transparent ist und
- 5 • der Kontrolle der Internet-Community untersteht, aber auch
- 6 • 100% kompartibel zu den ICANN-Name-Servern ist.

7 Inhaltliche Problematiken, wie z.B. mit der Namensvergabe, die in den
 8 entsprechenden ICANN-Gremien diskutiert werden, können und sollen mit
 9 dem alternativen Open Root Server Network (ORSN) nicht gelöst werden.

10 Durch das ORSN soll lediglich eine alternative technische Möglichkeit
 1 eröffnet werden, um das Internet insgesamt unabhängiger und Community-
 2 orientierter zu machen.

Nameserver-Abhängigkeiten mit und ohne ORSN



Illustrationsbeispiel: © Open Root Server Network (ORSN), Gr. Schwuelper, Kostenfreie
 9 Nutzung gestattet.

Willkommen auf der Projektseite des Open Root Server Network.

Das **ORSN** wurde im Januar 2002 gegründet und bis Mitte 2008 betrieben. In dieser Zeit waren die damaligen ICANN koordinierten DNS-Root-Server verstärkt auf dem amerikanischen Kontinent vertreten. Nur wenige Systeme waren auf der restlichen "Hälfte" unserer Erde installiert. Unser Netzwerk sollte dieses Ungleichgewicht reduzieren und die europäische Community etwas unabhängiger gestalten. In den vergangenen Jahren zwischen 2002 und 2008 wurde unser DNS-Netzwerk ständig erweitert. Wir betrieben in den Spitzenzeiten bis zu 13 Root-Server, verteilt auf viele europäische Länder, wie z.B. Frankreich, Portugal, Deutschland, Niederlande, Italien, Griechenland, Österreich, Schweiz, Luxemburg und ein System sogar in den USA, das durch den ISC-Gründer und BIND-Entwickler Paul Vixie betrieben wurde.

Wir begründeten die Existenzberechtigung von ORSN immer dadurch, dass ein geographisches Ungleichgewicht dieser wichtigen DNS-Server bestand. Ein weiterer Punkt ist die Tatsache, dass nur eine einzige Nation (USA) die tatsächliche Verwaltungsmacht besitzt. Die ICANN-Root-Server unterstehen immer noch dem US-Handelsministerium. Eine solche wichtige Infrastruktur sollte eigentlich unter der Führung einer weltweiten Organisation stehen. Das hat sich bis zum heutigen Tag nicht geändert.

Im Jahr 2008 wurde ORSN mit langer Vorlaufzeit abgeschaltet. ICANN und seine Root-Server-Betreiber führten flächendeckend so genannte AnyCast-Instanzen auf der ganzen Welt ein. Bei diesem Verfahren werden die ursprünglichen 13 Root-Server dupliziert und mit Hilfe des BGP-Protokolls in das Internet propagiert. Das war einer der stärksten Gründe ORSN abzuschalten. Technisch gesehen hatten wir damals nichts dagegensetzen. Der zweite Grund ORSN zu etablieren, war immer noch die Einflussnahme auf den Datenbestand der Root-Server. Und auch zum heutigen Zeitpunkt sind alle Internetnutzer davon abhängig, was in diesen Servern eingetragen ist und in Zukunft eingetragen bleibt.

Und das ist genau der Grund, warum im Juni 2013 das ORSN-Projekt wieder "reaktiviert" wurde. Nach den Enthüllungen von Edward Snowden und Berichten in den Medien ist erst jetzt das Ausmaß der totalen Überwachung von Geheimdiensten in den USA (NSA mit Prism) und dem britischen EU-Partner (GCHQ mit Tempora) überhaupt ersichtlich. Inwieweit der Bundesnachrichtendienst (BND) in Deutschland weitere Anstrengungen unternimmt bzw. für die vorherigen "Programme" den Weg bereitet hat, ist bis jetzt noch nicht an die Öffentlichkeit gelangt bzw. ersichtlich. An dieser Stelle könnte man berechtigt die Frage stellen, warum das ORSN auf Grund der Überwachungsmaßnahmen wiederbelebt wurde. Was hat beides miteinander zu tun? Was kann das ORSN dagegen tun?

Auf diese Fragen kann man eine pauschale Antwort geben: Nichts.

ORSN wird keine technische Möglichkeiten besitzen, Überwachungsmaßnahmen zu deaktivieren oder sogar dagegen vorzugehen. Aber wir als Internetnutzer (kurz Community) können uns von diesen Systemen distanzieren (die, die unsere tägliche Kommunikation aufzeichnen/verarbeiten) und ein eigenes DNS-Server-Netzwerk aufbauen das von der Community kontrolliert wird. In ganz Europa und anderen Teilen dieser Erde. ORSN wird wieder über dieselben DNS-Informationen verfügen, über die es bereits in den Jahren 2002-2008 verfügte. ORSN ist ein zu den ICANN-Systemen 100%ig kompatibles Root-Server-Netzwerk. Keine TLD mehr oder weniger wird in unserer Datenbank den Einzug halten.

Ein Unterschied zu ICANN wird es aber geben. Die Kontrolle liegt bei der Community und damit bei den Menschen, die das Internet so interessant machen. Den Bürgern in den jeweiligen Ländern, die im Internet Daten gezielt bereitstellen. Daten, die die Freigabe zur Veröffentlichung haben und nicht Daten, die abgeschöpft werden. Wir hoffen, dass ORSN weiten Zuspruch erhält, um das Netz der Netze wieder etwas -vertraulicher- zu gestalten.

Diese Plattform wird die gesamte Arbeit des ORSN-Teams dokumentieren. Sie werden die Betriebszustände unserer Infrastruktur in Echtzeit einsehen können. Wir werden unsere Datenbasis veröffentlichen.

ORSN setzt auf Transparenz und auf Datensicherheit. Geeignete Schutzmechanismen werden auch in Zukunft dafür sorgen, dass keine Nation auf dieser Welt einfach aus dem DNS fällt.

Hannover | 01. Juli 2013

- ▶ **Projektinformationen**
- ▶ ORSN Dokumentation
- ▶ Projektmitglieder
- ▶ Join ORSN
- ▶ Support
- ▶ FAQ
- ▶ Techn. Informationen
- ▶ WHOIS Datenbank
- ▶ Sponsoren-Übersicht
- ▶ Pressemitteilungen
- ▶ Dokumente & Logos
- ▶ Kontakt zum Team
- ▶ Impressum
- ▶ ORSN Root CA (SSL)



© Copyright 2002, 2013 by ORSN
 Open Root Server Network
 All rights reserved.

The following SLDs are provided by ORSN:
 orsn.org | orsn.net | orsn.eu
 orsn.de and orsn-servers.eu

All other domains (e.g. orsn-servers.net | .com) are not provided by this project.

Language
 DE | EN

SVR 12

Homepage, Quelle: www.orsn.org, © Open Root Server Network (ORSN), Gr. Schwuelper, Kostenfreie Nutzung gestattet.

Pressekontakt:

ORSN, Open Root Server Network

Sven Weingaertner

press@orsn.org

www.orsn.org

Germany



c/o Markus Grundmann
Schlossstrasse 25
38179 Schwuelper
Germany

contact@orsn.org

<http://www.orsn.eu>

1 © 2013, Sven Weingaertner, München, Germany

2 © 2013, Open Root Server Network (ORSN), Gr. Schwuelper, Germany

3
4 Kostenfreie Nutzung dieser Informationen und Grafiken ist gestattet
5 auf begrenzte Zeit bis einschließlich 2014, unbegrenzte regionale
6 Verbreitung, unbeschränkte Medien, allerdings nur im Rahmen einer
7 redaktionellen Berichterstattung. Darüber hinaus ist eine
8 redaktionelle und grafische Be-/Überarbeitung des Materials gestattet.

9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40