Löwenstark Digital Group GmbH
Petzvalstr. 38
38104 Braunschweig
Tel.: 0531 21360 5500
Fax: 0531 21360 5795
kontakt@loewenstark.com

Localhost

Stand: 04.07.2022

Was bedeutet Localhost?

Der Begriff Localhost – auch Loopback-Adresse – steht für einen virtuellen Server, der auf dem eigenen Computer läuft. Üblicherweise unterteilt er sich in die Loopback-Adresse „127.0.0.1“ (IPv4) und „::1“ (IPv6). Er wird zumeist für Netzwerke verwendet und bietet Usern die Möglichkeit, mit lokalen Computern zu kommunizieren – etwa über einen Anruf oder eine IP-Verbindung oder den IP-Stack zu kontrollieren. Rufen Sie die IP-Adresse Ihres Localhosts auf, kommuniziert der PC mit sich selbst.

Das hat den entscheidenden Vorteil, dass berechtigte Nutzer einen Zugang zu lokal installierten Websites haben und diese über einen Browser aufrufen können. Die IP-Adresse wird also dazu verwendet, um den Localhost über die Loopback-Schnittstelle zu erreichen. Diese wird allerdings nicht von jedem Betriebssystem unterstützt.

Wie werden IP-Adressen zugewiesen?

Grundsätzlich besitzen alle User eines Netzwerks eine individuelle und unverwechselbare IP-Adresse. Nur so lässt sich sicherstellen, dass Daten durch das Übertragungsprotokoll TCP/IP auch außerhalb des Internets – also in lokalen Netzwerken – gesendet und empfangen werden können. Dabei sorgt das Internetprotokoll dabei dafür, dass sowohl die Adresse als auch das dahinter liegende Subnetz während der Übertragung erreicht werden können.

Öffentliche IP-Adressen werden – genau wie Domainnamen im *Domain Name System (DNS*) – von der internationalen Organisation *Internet Corporation für Assigned Names and Numbers (ICANN)* zugewiesen. Dazu werden diese in verschiedene Klassen unterteilt:

- Klasse A: 0.0.0.0 – 127.255.255.255
- Klasse B: 128.0.0.0 – 191.255.255.255
- Klasse C: 192.0.0.0 – 223.255.255.255
- Klasse D: 224.0.0.0 – 239.255.255.255
- Klasse E: 240.0.0.0 – 255.255.255.255

Ähnlich vielen anderen Nummerierungssystemen behält sich die Institution allerdings vor, Adressbereiche für bestimmte Zwecke zu reservieren. Das betrifft beispielsweise den Bereich zwischen „127.0.0.0“ und „127.255.255.255“. Warum sie genau diesen Bereich zurückhält, ist bis heute unbekannt – allerdings fällt auf, dass die 127 den letzten Block des Klasse-A-Netzwerks darstellt.

Wie läuft das Loopback der IP-Adresse 127.0.0.1 ab?

Innerhalb des reservierten Adressbereichs des 127er-Blocks ist es möglich, ein lokales Netzwerk einzurichten. Im Gegensatz zu den anderen Umfeldern hat ICANN dafür gesorgt, dass IP-Adressen hier jedoch nicht eindeutig zugewiesen werden.

Löwenstark Digital Group GmbH
Petzvalstr. 38
38104 Braunschweig
Tel.: 0531 21360 5500
Fax: 0531 21360 5795
kontakt@loewenstark.com

Stattdessen leitet der Router die Zugriffsanfrage über das Internet an einen Server weiter, der diese bearbeitet und – je nach den Benutzerrechten – den Zugang zur IP-Adresse oder der Domain freigibt.

Gibt der User hingegen 127.0.0.1 in die Adresszeile ein, leitet der Router die Anfrage nicht an das Internet weiter, sondern löst das Loopback aus. Das liegt daran, dass das Übertragungsprotokoll TCP/IP an der Zahlenkombination 127 erkennt, dass der Nutzer sich selbst und nicht das Internet öffnen möchte. Das Loopback-Gerät ist dabei so eingestellt, dass die Rückverbindung zum eigenen Computer möglich ist: Das Betriebssystem erstellt eine virtuelle Schnittstelle (lo oder lo0), die Windows- oder Unix-Systeme über den Befehl ifconfig anzeigen können.

Viele Funktionen des Localhost können Sie nur nutzen, wenn dieser die angefragte Datei im Internet finden kann. Schließlich macht es einen Unterschied, ob ein Nutzer ein HTML-Dokument auf dem lokalen PC oder über einen Server öffnen möchte.

Der Localhost als vielseitiges Tool

Die Funktion des Localhosts bringt viele Vorteile mit sich. So ermöglicht er Entwicklern, Webanwendungen oder Programme zu testen, bevor diese online gehen. Gleichzeitig können Administratoren damit regelmäßig die Netzwerkverbindungen prüfen. Eine weitere wichtige Eigenschaft ist die Host-Datei: Denn alle Netzwerkuser können diese verwenden, um schädliche Webseiten zu blockieren.

Anwendungen und Programme über den Localhost testen

Bei der Entwicklung neuer Softwares oder Apps ist es unerlässlich, diese vor der Veröffentlichung immer wieder zu testen. Auch wenn eine Anwendung lokal problemlos funktioniert, kann es zu Störungen kommen, sobald diese online geht. Daher ist der Localhost eine gute Möglichkeit, die Funktionsweisen mit Zugriff auf das Internet zu testen. Denn da die Verbindung ausschließlich in Ihrem geschlossenen System existiert, stellen Sie eine Internetverbindung her, ohne Netzwerkfehler zu verursachen.

Darüber hinaus können die Entwickler das Loopback sogar nutzen, um spezielle Anforderungen an eine API zu schicken oder mobilen Apps den Zugriff auf Serverkomponenten vom zu erlauben.

Mit dem Localhost Netzwerkverbindungen prüfen

Am häufigsten verwenden Nutzer die Loopback-Adresse zur Abfrage der Netzwerkleistung (Ping-Anfrage). Über die Windows-Eingabeaufforderung testen die User die Schnelligkeit ihrer Verbindung und erhalten gleichzeitig eine detaillierte Übersicht über mögliche Probleme im Netzwerk.

So erstellen Sie eine Ping-Anfrage an den Localhost mit Windows, macOS und Linux:

1. Zur Überprüfung Ihrer Netzwerkleistung sollten Sie zunächst als Administrator eingeloggt sein.
2. Anschließend öffnen Sie das Fenster *Eingabeaufforderung* beziehungsweise *Terminalfenster* und starten die Run-Funktion (Windows-Taste + R).
3. Danach öffnet sich ein Fenster, in dem Sie *cmd* eingeben und auf a*usführen*
4. Im letzten Schritt geben Sie in dem neuen Fenster: *ping 127.0.0.1* oder *ping localhost*

Löwenstark Digital Group GmbH
Petzvalstr. 38
38104 Braunschweig
Tel.: 0531 21360 5500
Fax: 0531 21360 5795
kontakt@loewenstark.com

5. Nun erhalten Sie eine Übersicht über die Anzahl der gesendeten, empfangenen und verlorenen Daten sowie die ungefähre Umlaufzeit der Übertragung.

Über den Localhost verdächtige oder schädliche Websites blockieren

Möchten Sie den Zugriff anderer Nutzer auf eine potenziell schädliche Website verhindern, können Sie den Localhost auch zum Blockieren dieser benutzen. Dazu sperren Sie die entsprechende Host-Datei – den Vorläufer des DNS –, die die IP-Adressen ihren Domains zuordnen kann. Ein Domainname wird bei Eingabe in eine IP-Adresse übersetzt.

Obwohl im Regelfall mittlerweile das globale DNS genutzt wird, sind die jeweiligen Host-Dateien noch in den meisten Betriebssystemen vorhanden. So ist es weiterhin möglich, die Websites auf diesem Weg zu blockieren. Im Windows-Betriebssystem finden Sie die Host-Datei unter „system32driversetchosts“, bei anderen unter „/etc/hosts“. Dort erhalten Sie zumeist folgende zwei Einträge: „127.0.0.1 localhost“ und „::1 localhost“.

Zum Sperren der Website fügen Sie diese nun der Liste hinzu und weisen sie der IP-Adresse 127.0.0.1 zu.

Gibt ein Nutzer innerhalb Ihres Netzwerks die entsprechende Website-URL ein oder versucht ein bösartiges Skript den Zugriff, überprüft der Browser immer zuerst die Host-Datei – bei entsprechendem Eintrag wird der Zugriff also verhindert. Dazu können Sie auch den Domainnamen 0.0.0.0 benutzen.

Im Anschluss versucht der Browser, die nicht auffindbare Website mit dem Localhost zu öffnen. Da diese jedoch nicht vorhanden ist, ist für den User eine Fehlermeldung zu sehen. Haben die Benutzer allerdings einen eigenen Testserver aufgesetzt, öffnet sich an dieser Stelle gegebenenfalls die Seite home.html – da es sich hierbei aber um eine eigene Datei handelt, entsteht hierbei kein Schaden.

Der Localhost als Schutz vor Fremdzugriffen

Neben der internen Zugriffsverweigerung sperrt das TCP/IP-Protokoll auch externe Anfragen an den Localhost. Dadurch können potenzielle Angreifer sich nicht ohne Weiteres in Ihr System hacken. Zudem können bestimmte Personen von dem Aufrufen der Website gesperrt werden –, etwa wenn sie die Seite nicht benötigen oder es sich um sensible Daten handelt. Hin und wieder wird allerdings von Paketen berichtet, die reservierte IP-Adressen im Internet veröffentlichen –, den sogenannten Mars-Paketen.

Auch wenn der Localhost durchaus eine geeignete Methode zum Blockieren unerwünschter Zugriffe darstellt, ist er nicht die beste Lösung. Das liegt vor allem daran, dass der Administrator jeden Eintrag manuell hinzufügen oder entfernen muss – müssen Nutzer eine gesperrte Seite wieder aufrufen, bedeutet dies häufig einen Mehraufwand. Hinzu kommt, dass nur der Administrator die Rechte zur Änderung besitzt, der die Blockade eingerichtet hat.

Überdies können Kriminelle die Host-Datei mithilfe von Malware manipulieren, was negative Folgen für die Sicherheit beim Surfen haben kann. Um das zu verhindern, sollten keinesfalls Einträge kopiert werden, die sich auf anderen Websites befinden, ohne diese vorher zu kontrollieren.

Löwenstark Digital Group GmbH
Petzvalstr. 38
38104 Braunschweig
Tel.: 0531 21360 5500
Fax: 0531 21360 5795
kontakt@loewenstark.com

Gibt es einen Unterschied zwischen 127.0.0.1 und Localhost?

Mehr als 16 Millionen IP-Adressen können die Loopback-Adresse 127.0.0.1 verwenden – damit ist sie auch die am häufigsten genutzte, um über die Netzwerkverbindung Daten mit sich selbst auszutauschen.

- Die Loopback-Adresse ist daher ein virtuelles Netzwerkgerät, bei dem Anfangs- und Endpunkt identisch sind.
- Der Localhost ist hingegen die Kommunikationsschnittstelle zwischen Computer und Server. Dadurch können Sie ihn zur Nachbildung eines Netzwerks verwenden –, auch dann, wenn kein Netzwerk vorhanden oder zugänglich ist.

- In den allermeisten Fällen sind 127.0.0.1 und Localhost bezüglich ihrer Funktion gleich. Localhost bezeichnet jedoch eine IP-Adresse, wohingegen 127.0.0.1 die Adresse selbst beschreibt. Den Localhost können Sie dadurch an jede IP-Adresse weiterleiten, selbst an eine außerhalb des reservierten Adressblocks.

- Auf einem Unix-/Linux-System meinen außerdem Loopback und Localhost das Gleiche. Administratoren können die Host-Datei daher nutzen, um den Loopback auf 127.0.0.1 umzuleiten.

- Der Localhost ist nur eine Möglichkeit, auf 127.0.0.1 zuzugreifen. Dennoch werden die beiden Begriffe häufig synonym verwendet.