

Virenschutz und Firewall (Ubuntu)

Aufgabe 1

Sie haben zuvor den Virenschutz bei Windows installiert und überprüft. Brauchen Linux-Systeme auch einen Virenschutz? Recherchieren Sie im Internet und beraten Sie sich untereinander.

So schockierend es auch klingt, Linux ist nicht ganz so undurchdringlich, wie Benutzer es oft empfinden. Sein Betriebssystem ist sicherer als das von OS X und Windows. Es gibt jedoch Cyber-Bedrohungen, die die Leistung und die allgemeine Gesundheit des Betriebssystems beeinträchtigen können. Obwohl diese Chancen gering sind, ist Vorsicht besser als Nachsicht.

Es gibt verschiedene Möglichkeiten, wie Linux kompromittiert werden kann. Heutzutage verbinden wir uns mit jedem beliebigen Wi-Fi-Punkt irgendwo, ohne überhaupt an seine Sicherheit zu denken. Solche „Hotspots“ können Malware und Viren enthalten oder ein Jagdrevier für Hacker sein, die nach bestimmten Schwachstellen suchen, sobald Sie dort sind.

Antivirus für Linux ist erforderlich, um es vor spezifischen Bedrohungen zu schützen, die explizit so konstruiert sind, dass sie seine konventionellen Sicherheitsmechanismen umgehen. Diese Bedrohungen können unter anderem in Form von bösartigen URLs, bösartigem Code, E-Mail-Anhängen und Rootkits auftreten. Es gibt noch andere Arten, aber diese sind die häufigsten.

Ohne ein Linux-Virenschutzprogramm kann Ihr PC auch zum Überträger von Windows- oder MacOS-Viren werden, die in einem Skript, einer Datei oder einem Dokument verborgen bleiben können. Vielleicht können sie Ihr Linux nicht infizieren, aber sie können Benutzer mit anderen Betriebssystemen schädigen, wenn Sie diese Dateien freigeben.

Vor diesem Hintergrund benötigen Sie nicht nur einen Virenschutz für Linux, um sich zu schützen, sondern auch, um nicht unbeabsichtigt Malware zu verbreiten. Wie bei der Cybersicherheitssoftware für Windows und MacOS gibt es bezahlte und kostenlose Versionen von Linux-Virenschutzprogrammen. Es gibt zwar nicht so viele Angebote, aber es gibt einige wenige vertrauenswürdige, die Sie in Betracht ziehen sollten, auf deren Höhepunkte wir im Folgenden eingehen werden.

Taken from the website: <https://de.bestantiviruspro.org/best-antivirus-for-linux/>

Aufgabe 2

Wählen Sie einen bekannten Virenschutzsoftware für Linux aus und installieren Sie diese.

Besprechen Sie im Team vor der Installation des Programms warum Sie gerade dieses gewählt haben!

What Is the Best Antivirus for Linux?

1. [Sophos](#) –Leicht und fast unsichtbar (siehe unsere vollständige [Rezension](#))
2. ClamAV Antivirus –E-Mail-Sicherheit, Open Source
3. [ESET](#) –Wirksame Anti-Spyware-Tools, starker Schutz (mehr dazu in unserem [Bericht](#))
4. [Comodo](#) –Sandbox und andere nützliche Funktionen (weitere Informationen finden Sie in unserer [Rezension](#))
5. [Avast](#) –Mail-Server-Schutz und Anti-Malware (vollständige [Rezension](#) lesen)
6. [Bitdefender](#) –Cloud-Schutz & Anti-Ransomware-Funktionen ([Rezension](#))
7. F-Prot Antivirus
8. Hunter

Aufgabe 3

Gibt es noch andere Schutzmechanismen auf Linux-Systemen?

Wie heissen diese und wo finden Sie diese?

- [Linux Firewall aktivieren](#)
- [Systemabbild erstellen \(Zusätzliche Software nötig\)](#)

Aufgabe 4

Auch auf Ubuntu gibt es eine Firewall, welche Sie bei Windows auch bereits kennengelernt haben. Nachfolgend richten Sie diese auf ihrer Laborumgebung ein.

Die Firewall ist mittlerweile zu einem der grundlegenden Sicherheitstools für jeden Computer geworden, egal ob zu Hause oder im Unternehmen. **Die Konfiguration ist oft nicht einfach** und es kann weniger erfahrenen Benutzern Kopfschmerzen bereiten. Um den User zu unterstützen, gibt es Tools wie "**ufw**" (**Uncomplicated Firewall**). Diese vereinfachen die Verwaltung von Firewall-Regeln des Benutzers.

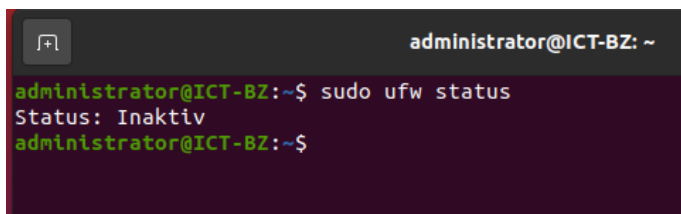
"ufw" ist ein "iptables"-Frontend, das sich besonders gut für Server eignet und in der Tat **das Standardkonfigurationstool unter Ubuntu Linux darstellt**. Die Entwicklung erfolgte mit der Idee, eine einfache und benutzerfreundliche Anwendung zu erstellen. Das Erstellen von Regeln für IPv4- und IPv6-Adressen war noch nie einfacher. In dem Tutorial, das wir Ihnen unten zeigen, lernen Sie die grundlegenden UFW-Anweisungen zu verwenden.

Die grundlegenden Aufgaben, die wir in der Firewall des Systems ausführen können, sind sehr unterschiedlich und reichen vom Blockieren einer bestimmten IP-Adresse oder eines bestimmten Ports bis zum Zulassen des Datenverkehrs nur von einem bestimmten Subnetz (*Teilbereich eines kompletten Netzwerkes*). Wir werden nun die relevantesten Regeln mit den erforderlichen Befehlen überprüfen. Dazu benutzen wir die Kommandozeile in einem Terminalfenster.

Wir zeigen den Status der Firewall und ihre Regeln an:

Prüfen Sie den Status ihrer Firewall:

sudo ufw status



```
administrator@ICT-BZ: ~  
administrator@ICT-BZ:~$ sudo ufw status  
Status: Inaktiv  
administrator@ICT-BZ:~$
```

Sie sehen bei Ubuntu ist die Firewall standardmässig nicht aktiviert.

Firewall ein- und ausschalten

Mit diesem Befehl können Sie die Firewall ein- oder ausschalten

sudo ufw enable (Firewall einschalten)

sudo ufw disable (Firewall ausschalten)

Wie Sie sehen gibt es diverse Befehlserweiterungen zu **ufw** um eine Übersicht zu erhalten können Sie folgenden Befehl eingeben **man ufw** ¹

¹ "**man**" steht für **Manual** (Anleitung). Diese Anleitungen haben unter **Linux/Unix** eine lange Tradition und werden ständig gepflegt.

```
NAME
    ufw - program for managing a netfilter firewall

DESCRIPTION
    This program is for managing a Linux firewall and aims to provide an
    easy to use interface for the user.

USAGE
    ufw [--dry-run] enable|disable|reload

    ufw [--dry-run] default allow|deny|reject [incoming|outgoing|routed]

    ufw [--dry-run] logging on|off|LEVEL

    ufw [--dry-run] reset

    ufw [--dry-run] status [verbose|numbered]

    ufw [--dry-run] show REPORT

    ufw [--dry-run] [delete] [insert NUM] [prepend] allow|deny|reject|limit
    [in|out] [log|log-all] [ PORT[/PROTOCOL] | APPNAME ] [comment COMMENT]

    ufw [--dry-run] [rule] [delete] [insert NUM] [prepend] allow|deny|re-
    ject|limit [in|out [on INTERFACE]] [log|log-all] [proto PROTOCOL] [from
    ADDRESS [port PORT | app APPNAME]] [to ADDRESS [port PORT | app APP-
    NAME]] [comment COMMENT]

    ufw [--dry-run] route [delete] [insert NUM] [prepend] allow|deny|re-
    ject|limit [in|out on INTERFACE] [log|log-all] [proto PROTOCOL] [from
    ADDRESS [port PORT | app APPNAME]] [to ADDRESS [port PORT | app APP-
    NAME]] [comment COMMENT]

    ufw [--dry-run] delete NUM
```

Schalten Sie die Firewall ein mit dem Befehl ***sudo ufw enable***.

Firewall Standardeinstellungen

Standardmässig blockiert man allen eingehenden Datenverkehr und lässt allen ausgehenden Datenverkehr zu.

sudo ufw default deny incoming

und

sudo ufw default allow outgoing

Was passiert, wenn sie die Regel: ***sudo ufw default deny outgoing*** eingeben? Allenfalls müssen Sie das System neustarten, damit die Regel

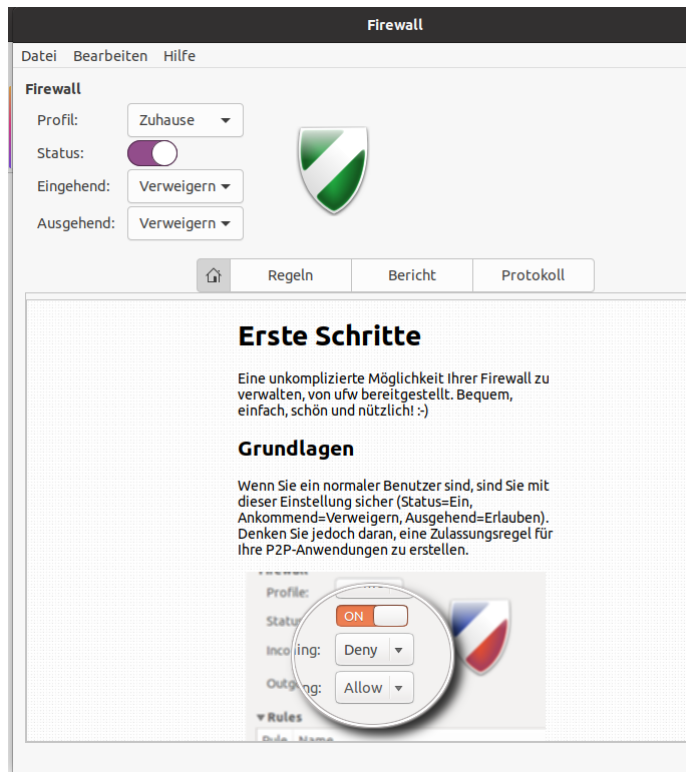
Es liegt nun im Ermessen jedes Administrators wie streng oder locker sein System absichert.

Falls Sie mal die Übersicht verlieren, können sie alle Einstellungen mit dem Befehl ***sudo ufw reset*** zurücksetzen.

Firewall Regeln mit einem GUI?

Eine weitere Vereinfachung einer Firewall-Konfiguration stellt das Programm "**gufw**" dar. Bei GUFW handelt es sich um die Firewall "ufw", allerdings haben einige Entwickler eine grafische Oberfläche dafür entwickelt.

Installieren Sie diese auf ihrem System mit dem Befehl: `sudo apt install gufw`



Natürlich eröffnen sich nun unendliche Möglichkeiten, aber auch Stolpersteine für ein System, leicht kann man sich auch komplett aus einem System aussperren.

Weitere Möglichkeiten finden Sie im Internet, sind aber in diesem Kurs nicht von Bedeutung.

