Thema 1: Die Linux-Community und Karriere im Open-Source-Umfeld

1.4 Lektion 1

Zertifikat:	Linux Essentials
Version:	1.6
Thema:	1 Die Linux-Community und Karriere im Open-Source-Umfeld
Lernziel:	1.4 IKT-Fähigkeiten und Arbeiten mit Linux
Lektion:	1 von 1

Einführung

Es gab eine Zeit, in der die Arbeit **mit Linux auf dem Desktop als schwierig galt**, da dem System viele ausgefeiltere Desktop-Anwendungen und Konfigurationstools fehlten, die andere Betriebssysteme hatten. Das lag unter anderem daran, dass Linux deutlich jünger war als viele andere Betriebssysteme und es einfacher war, zunächst wichtigere Kommandozeilenanwendungen zu entwickeln und die komplexeren grafischen Tools für später zu belassen. Da Linux ursprünglich für fortgeschrittenere Benutzer gedacht war, galt das auch nicht als Problem. Aber diese Zeiten sind längst vorbei**. Linux-Desktop-Umgebungen sind heute sehr ausgereift und lassen in Bezug auf Funktionalität und Benutzerfreundlichkeit keine Wünsche offen.**

Dennoch gilt die **Befehlszeile immer noch als ein mächtiges Werkzeug**, das fortgeschrittene Anwender täglich nutzen. In dieser Lektion werfen wir einen Blick auf einige der grundlegenden Desktop-Fähigkeiten, die Sie benötigen, um das beste Werkzeug für den richtigen Job auszuwählen, einschließlich der Befehlszeile.

Linux-Benutzeroberflächen

Bei der Arbeit mit einem Linux-System interagieren Sie **entweder** über eine **Befehlszeile** oder über eine **grafische Benutzeroberfläche**. Beide Wege ermöglichen den Zugriff auf zahlreiche Anwendungen, die die Ausführung fast aller Aufgaben mit dem Computer unterstützen.

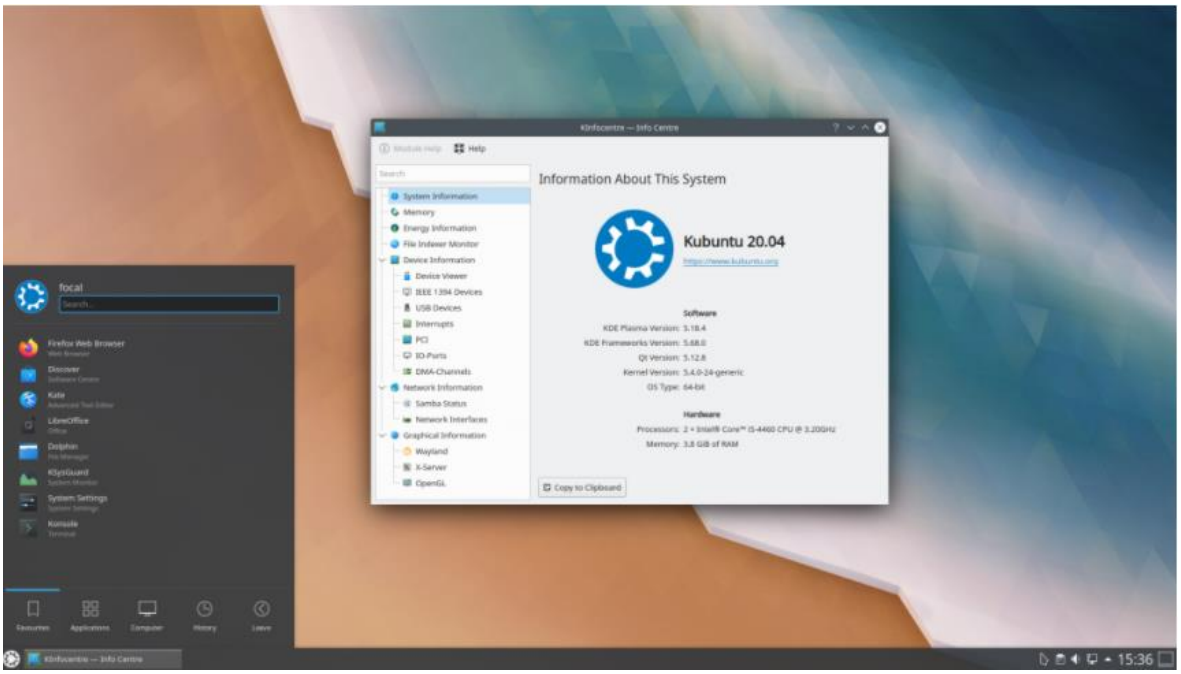
Desktop-Umgebungen

Linux hat einen modularen Ansatz, bei dem verschiedene Teile des Systems von verschiedenen Projekten und Entwicklern entwickelt werden, von denen jeder eine bestimmte Anforderung oder Zielsetzung erfüllt. Darum stehen auch mehrere Desktop-Umgebungen zur Auswahl. Gemeinsam mit Paketmanagern ist die **Standard-Desktop-Umgebung** einer der Hauptunterschiede zwischen den vielen Distributionen.

Im Gegensatz zu proprietären Betriebssystemen wie Windows und macOS, bei denen die Benutzer auf die mit ihrem Betriebssystem mitgelieferte Desktop-Umgebung beschränkt sind, gibt es die **Möglichkeit, mehrere Umgebungen zu installieren** und diejenige auszuwählen, die sich am besten an Sie und Ihre Bedürfnisse anpasst.
Grundsätzlich gibt es zwei große Desktop-Umgebungen in der Linux-Welt: ***Gnome* und *KDE***. Beide sind sehr vollständig, haben jeweils eine große Community hinter sich und verfolgen dasselbe Ziel, wenn auch mit leicht

unterschiedlichen Ansätzen. Kurz gesagt, folgt **Gnome dem KISS (“keep it simple stupid”) Prinzip**, mit sehr schlanken und sauberen Anwendungen. Demgegenüber hat **KDE eine andere Perspektive mit einer größeren Auswahl an Anwendungen** und der Möglichkeit für den Benutzer, jede Konfigurationseinstellung in der Umgebung zu ändern.

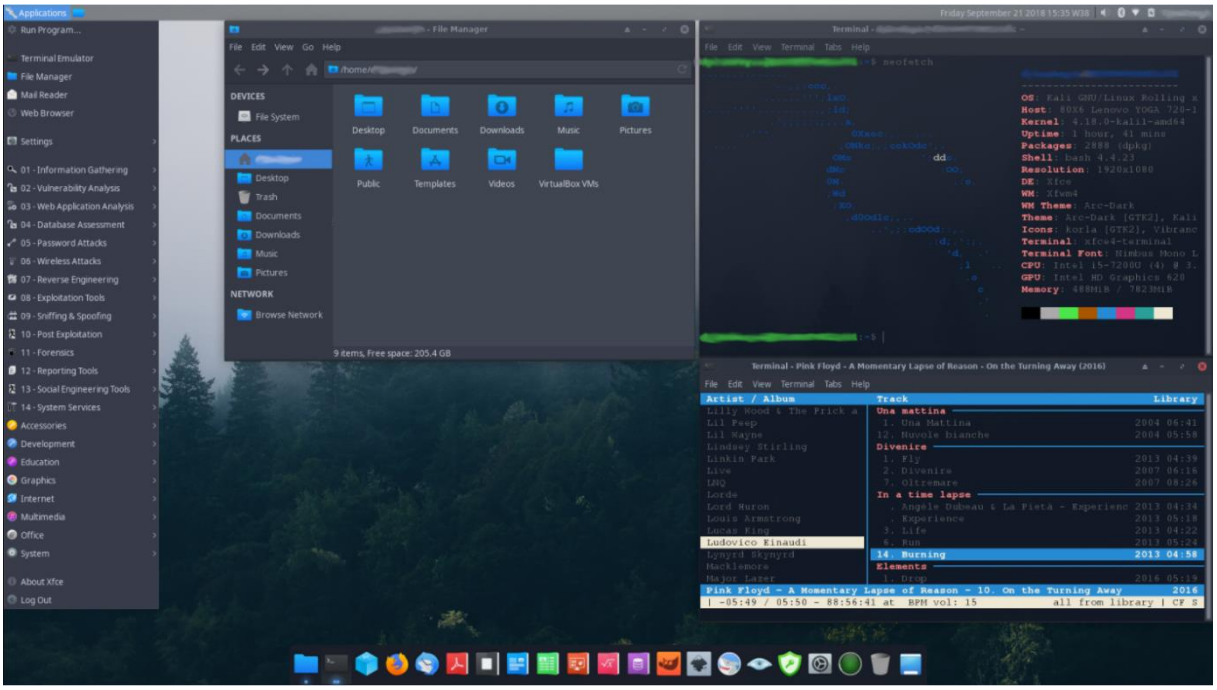
Gnome Desktop



KDE Desktop

Während **Gnome-Anwendungen auf dem GTK-Toolkit (geschrieben in C)** basieren, nutzen **KDE-Anwendungen die Qt-Bibliothek (geschrieben in C++).** Einer der Hauptgründe, Anwendungen mit demselben grafischen Toolkit zu entwickeln, besteht darin, dass die Anwendungen ein ähnliches Look-and-Feel teilen, was wiederum dem Benutzer den Eindruck von Einheitlichkeit vermittelt. Ein weiteres

wichtiges Merkmal ist, dass die Verwendung einer gemeinsamen grafischen Bibliothek für viele häufig verwendete Anwendungen Speicherplatz spart und zugleich die Ladezeit verkürzt, sobald die Bibliothek zum ersten Mal geladen wurde.



XFCE Desktop - Kali Linux - MacOS Mojave Night Theme

Zur Kommandozeile gelangen

Für uns ist eine der wichtigsten Anwendungen der grafische Terminalemulator

In **Gnome** heißt eine solche Anwendung ***Gnome Terminal***, während sie in **KDE als *Konsole*** zu finden ist. Aber es stehen viele weitere zur Wahl, wie z.B. ***Xterm***. Diese Anwendungen sind für uns der Zugang zu einer Kommandozeilenumgebung, um mit einer Shell interagieren zu können.

```
Ubuntu 18.10 arrelia tty3
arrelia login:
```

`arrelia` ist in diesem Fall der Hostname der Maschine, und `tty3` ist das Terminal, das nach Verwendung der obigen Tastenkombination verfügbar ist, plus die Taste `F3`, also `Ctrl`+`Alt`+`F3`.

Präsentationen und Projekte

Das wichtigste Werkzeug für Präsentationen unter Linux ist ***LibreOffice Impress***. Es ist Teil der Open-Source-Office-Pakets namens *LibreOffice*. Denken Sie an LibreOffice als Open-Source-Ersatz für das gleichwertige *Microsoft Office*. Es kann sogar dessen **PPT- und PPTX-Dateien öffnen und speichern**, die nativ zu *Powerpoint* gehören. Trotzdem ist dringend empfohlen, das **native ODP Impress-Format** zu verwenden.

ODP ist Teil des größeren *Open Document Format*, einem internationalen Standard für diese Art von Datei. Dies ist besonders wichtig, wenn Sie Ihre Dokumente über viele Jahre hinweg zugänglich halten und sich weniger um Kompatibilitätsprobleme

kümmern wollen. Da es sich um einen offenen Standard handelt, ist es für jeden möglich, das **Format ohne Lizenzgebühren** oder Lizenzen zu implementieren. Dies macht es Ihnen auch möglich, andere Präsentationssoftware auszuprobieren, die Ihnen vielleicht besser gefällt, und Ihre Dateien mitzunehmen, da es sehr wahrscheinlich ist, dass sie mit diesen neueren Softwareprodukten kompatibel sind.

Aber wenn Sie Code den grafischen Oberflächen vorziehen, gibt es ein paar Werkzeuge zur Auswahl: ***Beamer* ist eine *LaTeX*-Klasse, die Folienpräsentationen aus LaTeX-Code erstellt. LaTeX selbst ist ein Satzsystem, das hauptsächlich zum Schreiben wissenschaftlicher Dokumente** verwendet wird, insbesondere wegen seiner Fähigkeit, komplexe mathematische Formeln zu verarbeiten, mit denen andere Softwareprogramme Schwierigkeiten haben. Wenn Sie an der Universität sind und sich mit Gleichungen und anderen mathematischen Problemen befassen müssen, kann Beamer Ihnen eine Menge Zeit sparen.

Wenn Sie einen Ersatz für *Microsoft Project* suchen, probieren Sie ***GanttProject*** oder ***ProjectLibre*** aus. Beide sind ihrem proprietären Gegenstück sehr ähnlich und mit Projektdateien kompatibel.

Industrielle Linux-Anwendungen

Linux spielt eine große Rolle in der Software- und Internetbranche. Websites wie W3Techs berichten, dass etwa **68% der Webserver im Internet unter Unix** laufen und der allergrößte Teil davon unter **Linux**.

Diese große Akzeptanz ist nicht nur auf die freie Natur von Linux (sowohl im Sinne von Freibier als auch im Sinne von Meinungsfreiheit) zurückzuführen, sondern auch auf seine Stabilität, Flexibilität und Leistung. Sie machen es Anbietern möglich, ihre Dienste kostengünstiger und besser skalierbar anzubieten. Ein bedeutender Teil der Linux-Systeme läuft heute in der Cloud, also in einem **IaaS- (Infrastructure as a Service), PaaS- (Platform as a Service) oder SaaS- (Software as a Service) Modell.**

IaaS ist eine Möglichkeit, die **Ressourcen** eines großen Servers **zu verteilen**, indem man ihnen Zugang zu virtuellen Maschinen bietet. **Das nennen wir *Virtualisierung***. Im IaaS-Modell bezahlen Sie nur für den Teil der Ressourcen, den Ihre Infrastruktur nutzt.

Linux hat **drei bekannte Open-Source-Hypervisoren**: ***Xen*, *KVM* und *VirtualBox***. Xen ist wahrscheinlich der älteste von ihnen. KVM überholte Xen als prominentester Linux-Hypervisor. RedHat hat seine Entwicklung unterstützt und nutzte es — ebenso wie andere Anbieter — in Public-Cloud-Diensten wie auch in privaten Cloud-Setups verwendet. VirtualBox gehört seit der Übernahme von Sun Microsystems zu Oracle und wird in der Regel von Endbenutzern wegen seiner einfachen Bedienung und Administration eingesetzt.

PaaS und SaaS hingegen bauen technisch und konzeptionell auf dem IaaS-Modell auf: In **PaaS haben die Anwender** statt einer virtuellen Maschine **Zugriff auf eine Plattform**, auf der sie ihre Anwendungen deployen und ausführen, um den Aufwand für Systemadministrationsaufgaben und Betriebssystem-Updates zu verringern. Heroku ist ein gängiges PaaS-Beispiel, bei dem Programmcode nur ohne Pflege der zugrunde liegenden Container und virtuellen Maschinen ausgeführt werden kann.

Schließlich ist **SaaS das Modell**, bei dem Sie normalerweise für ein **Abonnement bezahlen**, um eine Software zu nutzen, ohne sich um etwas anderes zu kümmern. ***Dropbox* und *Salesforce* sind zwei gute Beispiele für SaaS**. Die meisten dieser Dienste werden über einen Webbrowser aufgerufen.

Ein Projekt wie ***OpenStack*** ist eine Sammlung von Open-Source-Software, die verschiedene Hypervisoren und andere Tools nutzt, um eine komplette IaaS-Cloud-Umgebung anzubieten, indem sie die Leistungsfähigkeit von Computer-Clustern in ihrem eigenen Rechenzentrum nutzt. Der Aufbau einer solchen Infrastruktur ist jedoch nicht trivial.

Datenschutzprobleme bei der Nutzung des Internets

Der Webbrowser ist heute eine grundlegende Software auf jedem Desktop, aber vielen Anwendern fehlt das Wissen, ihn sicher zu nutzen. Während immer mehr Dienste über einen Webbrowser aufgerufen werden, werden fast alle Aktionen, die über einen Browser ausgeführt werden, von verschiedenen Stellen verfolgt und analysiert. Die Sicherung des Zugangs zu Internetdiensten und die Verhinderung von Tracking ist ein wichtiger Aspekt der sicheren Nutzung des Internets.

Cookie Tracking

Wie erscheint die passende Anzeige auf einer anderen Webseite? Die Antwort auf diese Fragen heißt ***Cookie Tracking*.**

Cookies sind kleine Dateien, die eine Website auf Ihrem Computer ablegen kann, um Informationen zu speichern und abzurufen, die für Ihre Navigation nützlich sein können. Das ist in der Regel in Ordnung, da die Website Ihnen ein nützliches Feature bietet und keine Daten an Dritte weitergibt.

Aber was ist mit den Anzeigen, die erscheinen, während Sie auf anderen Webseiten surfen? Hier kommen die Werbenetzwerke ins Spiel. Werbenetzwerke sind Unternehmen, die Anzeigen für E-Commerce-Sites wie die in unserem Beispiel auf der einen Seite und Monetarisierung für Websites auf der anderen Seite anbieten. Content-Ersteller wie z.B. Blogger können etwas Platz für diese Werbenetzwerke auf ihrem Blog zur Verfügung stellen, gegen eine Provision für den Umsatz, der durch diese Werbung generiert wird.

Aber woher wissen sie, welches Produkt sie Ihnen zeigen sollen? Indem sie in der Regel auch ein **Cookie aus dem Werbenetzwerk speichern**, das sie bei Ihrem Besuch oder bei der Suche nach einem bestimmten Produkt auf der E-Commerce-Website gespeichert haben. **So ist das Netzwerk in der Lage, Informationen über dieses Cookie überall dort abzurufen, wo das Netzwerk Werbung hat**, und die Korrelation mit den Produkten herzustellen, die Sie interessiert haben. Das ist eine der häufigsten Wege, jemanden über das Internet zu verfolgen. Das oben genannte Beispiel nutzt E-Commerce, um die Dinge greifbarer zu machen, aber Social-Media-Plattformen tun dasselbe mit ihren “Like”- oder “Share”-Buttons und ihrem sozialen Login.

Eine Möglichkeit, das zu vermeiden, besteht darin, **Websites von Drittanbietern das Speichern von Cookies in Ihrem Browser zu verbieten**. Auf diese Weise kann nur

die von Ihnen besuchte Website ihre Cookies speichern. Beachten Sie jedoch, dass einige “legitime” Funktionen dann möglicherweise nicht mehr gut funktionieren, da viele Websites heute auf Dienste von Drittanbietern angewiesen sind. Suchen Sie im Add-On-Repository Ihres Browsers nach einem **Cookie-Manager**, um genaue Kontrolle darüber zu haben, welche Cookies auf Ihrem Computer gespeichert werden.

Do Not Track (DNT)

Ein weiterer häufiger Irrtum betrifft eine bestimmte Browserkonfiguration, bekannt als “**Do Not Track**” oder kurz DNT. **Es kann grundsätzlich in jedem aktuellen Browser eingeschaltet werden.** Ähnlich wie beim privaten Modus glauben sehr viele, sie könnten mit dieser Konfiguration nicht verfolgt werden. Leider ist dem nicht immer so. Derzeit ist DNT nur eine Möglichkeit für Sie, den von Ihnen besuchten Websites mitzuteilen, dass Sie von ihnen nicht verfolgt werden möchten. **Aber tatsächlich entscheiden immer noch die Websites, ob sie Ihren Wunsch respektieren oder nicht.** Mit anderen Worten, mit DNT können Sie sich vom Website-Tracking abwählen, aber es gibt keine Garantie für diese Wahl.

Technisch gesehen geschieht dies einfach durch Senden eines zusätzlichen Flags im Header des HTTP-Request-Protokolls (`DNT: 1`) bei der Anforderung von Daten von einem Webserver. Wenn Sie mehr über dieses Thema erfahren möchten, ist die Website https://allaboutdnt.com ein guter Ausgangspunkt.

“Private” Fenster

Sicher haben Sie die Anführungszeichen in der Überschrift bemerkt, denn diese Fenster sind nicht so privat, wie die viele denken. Die Namen können variieren, aber sie heißen “**Privatmodus**”, “**Inkognito**” oder “**Anonym**”, je nach Browser, den Sie verwenden.

In Firefox nutzen Sie es ganz einfach, indem Sie die Tastenkombination `Strg`+`Shift`+`P` drücken. In Chrome drücken Sie einfach `Strg`+`Shift`+`N`. Tatsächlich wird dadurch eine neue Sitzung geöffnet, die normalerweise keine Konfiguration oder Daten aus Ihrem Standardprofil enthält. Wenn Sie das **private Fenster** schließen, **löscht der Browser automatisch alle von dieser Sitzung erzeugten Daten** und hinterlässt keine Spuren auf dem verwendeten Computer. Das bedeutet, dass auf diesem Computer keine personenbezogenen Daten wie Verlauf, Passwörter oder Cookies gespeichert werden.

Das richtige Passwort wählen

Eine der schwierigsten Situationen für jeden Benutzer ist die Wahl eines sicheren Passworts für die von ihm genutzten Dienste. Sie haben sicherlich schon einmal gehört, dass Sie weder gängige Kombinationen wie `qwerty`, `123456` oder `654321` noch leicht zu erratende Zahlen wie Ihren Geburtstag (oder den eines Verwandten) oder Ihre Postleitzahl verwenden sollten, denn das sind alles sehr naheliegende Kombinationen und die ersten Versuche, die ein Eindringling unternehmen wird, um Zugang zu Ihrem Konto zu erhalten.

Es gibt bekannte Techniken zur Erstellung eines sicheren Passworts. Eine der bekanntesten ist die Zusammenstellung eines Satzes, der Sie an diesen Dienst erinnert und die Anfangsbuchstaben jedes Wortes aufnimmt. Nehmen wir an, Sie

möchten beispielsweise ein gutes Passwort für Facebook erstellen. In diesem Fall könnten Sie sich einen Satz wie "**Ich wäre glücklich, wenn ich 1000 Freunde wie Mike hätte**" ausdenken. Wählen Sie den ersten Buchstaben jedes Wortes und das endgültige Passwort lautet `Iwgwi1000FwMh`. Dies würde zu einem 13-stelligen Passwort führen, das lang genug ist, um schwer zu erraten und gleichzeitig leicht zu merken ist (solange Sie sich an den Satz und den "Algorithmus" zum Abrufen des Passworts erinnern). Sätze sind in der Regel leichter zu merken als Passwörter.

Einer der heute sichersten Ansätze ist die Verwendung eines so genannten ***Passwortmanagers***. Passwortmanager sind eine Software, die im Wesentlichen alle Ihre Passwörter und Benutzernamen in einem verschlüsselten Format speichert, das mit einem Master-Passwort entschlüsselt werden kann, so dass Sie sich nur ein gutes Passwort merken müssen, da der Manager alle anderen für Sie sicher verwahrt.

***KeePass* ist einer der bekanntesten und funktionsreichsten Open-Source-Passwortmanager.** Es speichert Ihre Passwörter in einer verschlüsselten Datei in Ihrem Dateisystem. Dass es sich um Open-Source-Software handelt, ist in diesem Zusammenhang wichtig, weil das garantiert, dass Ihre Daten nicht anderweitig genutzt werden, denn jeder Entwickler kann den Code überprüfen und weiß genau, wie er funktioniert. Dieses Maß an Transparenz ist mit proprietärem Code nicht zu erreichen. **KeePass** steht für die meisten Betriebssysteme zur Verfügung, einschließlich **Windows**, **Linux** und **macOS** — ebenso wie für **mobile Systeme wie iOS und Android**. Es umfasst auch ein Plugin-System, das seine Funktionalität weit über die Standardeinstellungen hinaus erweitert.

Bitwarden ist eine weitere Open-Source-Lösung mit einem ähnlichen Ansatz, aber statt Ihre Daten lokal in einer Datei zu speichern nutzt es einen **Cloud-Server**. So halten Sie alle Ihre Geräte synchron greifen über das Internet leichter auf Ihre Passwörter zu. Bitwarden ist eines der wenigen Projekte, das nicht nur die Clients, sondern **auch den Cloud-Server als Open-Source-Software zur Verfügung stellt**. Sie können also Ihre eigene Version von Bitwarden hosten und sie anderen zur Verfügung stellen, etwa Ihrer Familie oder den Mitarbeitern Ihres Unternehmens. Dies gibt Ihnen Flexibilität, aber auch die volle Kontrolle darüber, wie ihre Passwörter gespeichert und verwendet werden.

Eines der wichtigsten Dinge, die Sie bei der Verwendung eines Passwortmanagers beachten sollten, ist die Erstellung eines zufälligen Passworts für jeden einzelnen Dienst, da Sie sich die Passwörter ohnehin nicht mehr merken müssen. Es wäre nutzlos, einen Passwortmanager zu verwenden, um recycelte oder leicht zu erratende Passwörter zu speichern. Darum bieten Ihnen die meisten einen Zufalls-passwortgenerator an, mit dem Sie diese erstellen.

Verschlüsselung

Wann immer Daten übertragen oder gespeichert werden, sind Vorkehrungen zu treffen, damit Dritte nicht darauf zugreifen können. Über das Internet übertragene Daten passieren eine Reihe von Routern und Netzwerken, in denen Dritte auf den Netzwerkverkehr zugreifen können. Ebenso lassen sich auf physischen Datenträgern gespeicherte Daten von jedem lesen, der in den Besitz dieser Datenträger gelangt. Zur Vermeidung eines solchen Zugriffs sollten vertrauliche Informationen verschlüsselt werden, bevor sie einen Rechner verlassen.

TLS

***Transport Layer Security* (TLS) ist ein Protokoll, das Sicherheit von Netzwerkverbindungen** durch den Einsatz von Kryptographie bietet. **TLS ist der Nachfolger von *Secure Sockets Layer* (SSL),** das wegen schwerwiegender Fehler nicht mehr eingesetzt wird. TLS wurde immer wieder überarbeitet, um sich anzupassen und sicherer zu werden, und liegt aktuell in Version 1.3 vor. Es bietet durch so genannte symmetrische und Public-Key-Kryptographie sowohl **Vertraulichkeit** als auch **Authentizität**. Das bedeutet, dass **niemand** Ihre Kommunikation mit diesem Server während dieser **Sitzung abhören oder verändern** kann.

Die wichtigste Aufgabe besteht darin herauszufinden, ob eine Website vertrauenswürdig ist. Sie sollten nach dem Symbol “Sperren” in der Adressleiste des Browsers suchen, auf das Sie bei Bedarf klicken, um das Zertifikat zu überprüfen, das eine wichtige Rolle im HTTPS-Protokoll spielt.

TLS ist das, was im HTTPS-Protokoll (*HTTP über TLS*) verwendet wird, um den Versand sensibler Daten (zum Beispiel Ihre Kreditkartennummer) über das Internet zu gewährleisten. Die Erklärung, wie TLS funktioniert, geht weit über das Thema dieser Lektion hinaus, aber weitere Informationen finden Sie auf Wikipedia und im Mozilla wiki.

Datei- und E-Mail-Verschlüsselung mit GnuPG

Es gibt viele Tools zur Absicherung von E-Mails, aber eines der wichtigsten ist sicherlich *GnuPG*. GnuPG steht für ***GNU Privacy Guard* und ist eine Open-Source-Implementierung von PGP (*Pretty Good Privacy*),** die proprietär ist.

GnuPG dient dazu, Texte, E-Mails, Dateien, Verzeichnisse und sogar ganze Festplattenpartitionen zu signieren, zu verschlüsseln und zu entschlüsseln. Es nutzt Public-Key-Kryptographie und ist weit verbreitet. Kurz zusammengefasst, GnuPG erstellt Paar von Dateien mit Ihrem **öffentlichen und Ihrem privaten Schlüssel**. Wie der Name schon sagt, ist der öffentliche Schlüssel jedermann zugänglich, während der private Schlüssel geheim zu halten ist. Andere verwenden Ihren öffentlichen Schlüssel, um Daten zu verschlüsseln, die nur Ihr privater Schlüssel entschlüsseln kann.

Festplattenverschlüsselung

Eine gute Möglichkeit, Ihre Daten zu schützen, besteht in der Verschlüsselung Ihrer gesamten Festplatte oder Partition. Es gibt dafür viele Open-Source-Lösungen. Sie unterscheiden sich zum Teil erheblich in der Funktionsweise und im Grad der Verschlüsselung. Grundsätzlich gibt es **zwei Methoden: *Stacked*-** und ***Block*-Device-Verschlüsselung**.

Stacked-Dateisystemlösungen werden auf dem bestehenden Dateisystem implementiert. Hier werden Dateien und Verzeichnisse verschlüsselt, bevor sie auf dem Dateisystem gespeichert, und entschlüsselt, nachdem sie gelesen werden. Die **Dateien liegen also auf dem Host-Dateisystem in verschlüsselter Form** (ihr Inhalt und in der Regel auch ihre Datei-/Ordnernamen werden durch Zufallsdaten ersetzt),

aber sie existieren noch in diesem Dateisystem, wie sie ohne Verschlüsselung als normale Dateien, Symlinks, Hardlinks, etc. dort liegen.

***Bei Block*-Device-Verschlüsselung** erfolgt die Verschlüsselung von Block Devices **unterhalb der Dateisystemebene** und stellt sicher, dass alles, was auf ein Block Device geschrieben wird, verschlüsselt wird. Wenn Sie sich den Block ansehen, während er offline ist, sieht er wie ein Haufen von Zufallsdaten aus und Sie können **nicht einmal den Dateisystemtyp erkennen**, ohne zuvor zu entschlüsseln. Sie können also nicht sagen, was eine Datei oder ein Verzeichnis ist, wie groß sie ist und um welche Art von Daten es sich handelt, denn Metadaten, Verzeichnisstruktur und Berechtigungen sind ebenfalls verschlüsselt.

Wenn Sie auf Daten auf verschiedenen Plattformen zugreifen müssen, schauen Sie sich schließlich ***Veracrypt*** an, den Nachfolger von **Truecrypt**. Es erstellt verschlüsselte Medien und Dateien, die sowohl unter Linux als auch unter macOS und Windows verwendet werden können.

Geführte Übungen

1. Verwenden Sie in Ihrem Browser ein “privates Fenster”, um:

völlig anonym im Internet zu surfen
keine Spuren auf dem Computer zu hinterlassen, den Sie verwenden
TLS zu aktivieren, um das Verfolgen von Cookies zu vermeiden
DNT zu verwenden
Kryptographie bei der Datenübertragung zu nutzen

2. Was ist OpenStack?

Ein Projekt für den Aufbau von privatem IaaS
Ein Projekt für den Aufbau von privatem PaaS
Ein Projekt für den Aufbau von privatem SaaS
Ein Hypervisor
Ein Open-Source-Passwortmanager

3. Welche der folgenden Optionen sind gültige Festplattenverschlüsselungssoftware?

RevealJS, EncFS und dm-crypt
dm-crypt und KeePass
EncFS und Bitwarden
EncFS und dm-crypt
TLS und dm-crypt

4. Wählen Sie wahr oder falsch für die dm-crypt Geräteverschlüsselung:

Dateien werden verschlüsselt, bevor sie auf die Festplatte geschrieben werden
Das gesamte Dateisystem ist ein verschlüsselter Blob
Es werden nur Dateien und Verzeichnisse verschlüsselt, nicht Symlinks
Kein Root-Zugriff erforderlich

Ist eine Block-Device-Verschlüsselung

5. Beamer ist:

Ein Verschlüsselungsmechanismus
Ein Hypervisor
Eine Virtualisierungssoftware
Eine OpenStack-Komponente
Ein LaTeX-Präsentations-Tool

Offene Übungen

1. Die meisten Distributionen werden standardmäßig mit Firefox installiert (ist das bei Ihnen nicht der Fall, müssen Sie Firefox zuerst installieren). Wir werden eine Firefox-Erweiterung namens *Lightbeam* installieren, indem Sie entweder `Strg`+`Shift`+`A` drücken und “Lightbeam” in das Suchfeld eingeben, das auf dem geöffneten Tab angezeigt wird, oder indem Sie die Erweiterungsseite mit Firefox aufrufen und auf die Schaltfläche “Install” klicken: https://addons.mozilla.org/en-US/firefox/addon/lightbeam. Anschließend starten Sie die Erweiterung, indem Sie auf das Symbol klicken, und besuchen Sie einige Webseiten auf anderen Tabs, um zu sehen, was passiert.
2. Was ist das Wichtigste bei der Verwendung eines Passwortmanagers?
3. Verwenden Sie Ihren Webbrowser, um https://haveibeenpwned.com/ aufzurufen. Finden Sie den Zweck der Website heraus und überprüfen Sie, ob Ihre E-Mail-Adresse in einigen Datenlecks enthalten war.

Zusammenfassung

Das Terminal ist eine leistungsstarke Möglichkeit, mit dem System zu interagieren, und es gibt viele nützliche und sehr ausgereifte Tools, die Sie in dieser Umgebung nutzen können. Sie gelangen zum Terminal, indem Sie in Ihrer Desktop-Umgebung nach einem grafischen Terminal suchen oder kbd drücken:[Strg+Alt+F#].

Linux wird hauptsächlich in der Technologiebranche eingesetzt, um IaaS-, PaaS- und SaaS-Dienste anzubieten, wobei vor allem drei Hypervisoren eine wichtige Rolle bei der Unterstützung spielen: Xen, KVM und Virtualbox.

Der Browser ist heute ein unverzichtbares Werkzeug auf Computern, aber man muss einige Dinge verstehen, um ihn sicher zu benutzen. DNT ist nur eine Möglichkeit, einer Website zu signalisieren, dass Sie nicht verfolgt werden wollen, aber es gibt keine Garantie. Private Fenster sind nur für den Computer, den Sie benutzen, privat, aber genau das kann Sie vor Cookie Tracking bewahren.

TLS kann Ihre Kommunikation im Internet verschlüsseln, aber Sie müssen erkennen, wann es verwendet wird. Starke Passwörter sind zur Absicherung ebenfalls sehr wichtig, weshalb Sie diese Verantwortung am besten einem Passwortmanager übertragen und der Software erlauben, Zufallspasswörter für jede Website zu erstellen, an der Sie sich anmelden.

Eine weitere Möglichkeit, Ihre Kommunikation zu sichern, besteht darin, Ihre Dateiordner und E-Mails mit GnuPG zu signieren und zu verschlüsseln. dm-cypt und EncFS sind zwei Alternativen zur Verschlüsselung ganzer Festplatten oder Partitionen, die Block- bzw. Stack-Verschlüsselung verwenden.

Schließlich ist LibreOffice Impress eine sehr vollständige Open-Source-Alternative zu Microsoft Powerpoint, aber es gibt Beamer und RevealJS, wenn Sie Präsentationen lieber mit Code statt mit GUIs erstellen. ProjectLibre und GanttProject können die richtige Wahl sein, wenn Sie einen Ersatz für Microsoft Project benötigen.