STUDIENSKRIPT



## Cybersysteme und Netzwerkforensik

DLMCSECSNF01\_E



Übergeordnete Lernziele

##### Einführung 9



Bei fast jedem Vorfall, der bei der Netzwerkforensik untersucht wird, können digitale Beweise gefunden werden. Die ermittelnden Personen müssen vorsichtig mit diesen umgehen, weil sie beim Sammeln oder Analysieren leicht zerstört werden können. Statische Elektrizität kann ausreichen, um digitale Beweise zu verändern. Um sie im Rahmen einer Ermittlung zu nutzen, müssen wir verstehen, wie sie entstehen und wie sie sich mit bestimmten Nutzer:innen in Verbindung bringen lassen.

Digitale Beweise können aus verschiedenen Quellen stammen, wie zum Beispiel aus Netzwerken, von mobilen Geräten und traditionellen Computern wie Desktops oder Laptops. Die Art der digitalen Spuren kann je nach Quelle sehr unterschiedlich sein. Bei der Untersuchung von netzwerkbasiertem Beweismaterial müssen sich die Ermittler:innen darüber im Klaren sein, dass die Menge der zu untersuchenden digitalen Beweise überwältigend sein kann. Sie müssen irrelevante Daten ausblenden und sich auf die für ihre Ermittlung wichtigen Daten konzentrieren.

Der Kurs **Cybersysteme und Netzwerkforensik** vermittelt fundierte Kenntnisse im Sammeln und Untersuchen digitaler Beweise. Bei der Analyse von Laptops und Desktop-Computern müssen ermittelnde Personen die verschiedenen Betriebssysteme und deren Zusammenspiel mit den verschiedenen Dateisystemen und Speichergeräten verstehen. Durch die Erklärung und das Verständnis der Netzwerkprotokolle lassen sich die Taktiken von Angriffen besser verstehen. In jeder Lektion wird die praktische Anwendung untersucht und durch Beispiele aus der Praxis erläutert. Dies ermöglicht einen Einblick in die Beschaffung, Analyse und Verwendung digitaler Beweismittel in Gerichts- und Verwaltungsverfahren.



# Lektion 1

## Betriebssysteme

#### LERNZIELE

Nach Abschluss dieser Lektion werden Sie in der Lage sein, …

... zu erklären, warum Betriebssysteme (OS) notwendig sind.

... die Funktionen eines Betriebssystems zu benennen.

... den Zweck der Datenträgerverwaltung zu erklären.

... die mehrschichtige Struktur von Eingabe- und Ausgabe-Software (E/A) zu beschreiben.

... Multi-Programmiersysteme und Multi-Tasking-Systeme zu nutzen.

DL-E-DLMCSECSNF01\_E-U01

1. Betriebssysteme

### Einführung

Im einundzwanzigsten Jahrhundert beeinflussen Computersysteme fast alle Bereiche unseres täglichen Lebens. Das Fernsehen, das Abrufen von E-Mails und sogar das Starten unserer Autos erfolgt über ein Computersystem. Die Nutzung mobiler Geräte hat so stark zugenommen, dass sogar der Besitz mehrerer Geräte notwendig sein kann.

Für den Betrieb dieser Computersysteme werden Betriebssysteme (OS) genutzt. Das am weitesten verbreitete Betriebssystem auf dem Heimcomputermarkt ist Microsoft Windows *(Marktanteil Desktop-Betriebssysteme weltweit*, 2021). Durch technologische Fortentwicklung ändert sich auch das Betriebssystem ständig. Die aktuellen Windows-Versionen (Windows 10 und 11) sind weitaus fortschrittlicher, und auch die Computersysteme selbst haben sich seit Beginn des neuen Jahrhunderts erheblich weiterentwickelt.

Das Betriebssystem fungiert als Vermittler zwischen der Hardware des Systems und den Anwender:innen. Es bietet ein unkompliziertes Benutzererlebnis, weil nicht mehr alle angeschlossenen Hardwarekomponenten konfiguriert werden müssen. Das Betriebssystem verwaltet alle angeschlossenen Geräte im Hintergrund und bietet dadurch eine effiziente Erfahrung.

### Konzepte

**Speicher mit wahlfreiem Zugriff (RAM = *Random Access Memory*)**   
Diese Art Computerspeicher ermöglicht es, Daten in beliebiger Reihenfolge zu lesen und zu ändern.

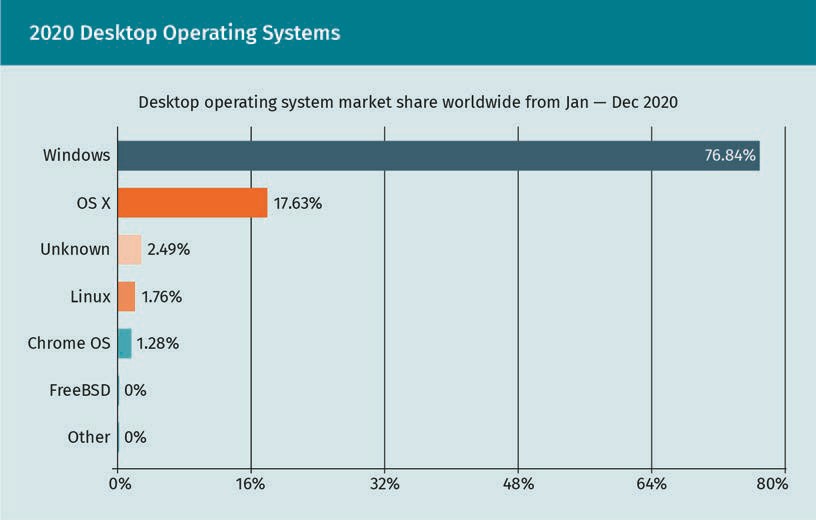
**Grafische Benutzeroberfläche**   
Dies ist eine visuelle Art der Interaktion mit einem Computer.

Was kommt uns in den Sinn, wenn wir an das Wort „Computer“ oder „Rechner“ denken? Wir können uns einen Monitor vorstellen, der an ein Gehäuse mit Tastatur und Maus angeschlossen ist. Die Nutzer:innen steuern den Computer mit der Tastatur und der Maus, und ihre Eingaben werden auf dem Monitor angezeigt. Die meisten User sind mit den jeweiligen Anwendungen, wie z. B. Textverarbeitung, Webbrowser und E-Mail-Program­men, vertraut, jedoch wissen viele nicht genau, wie das Gerät (die „Box“) die Eingaben entgegennimmt und verarbeitet. Werfen wir also zunächst einen Blick in diese Box. Im Inneren finden wir eine Hauptplatine („Motherboard“). Die Hauptplatine beherbergt die zentrale Verarbeitungseinheit (CPU = *Central Processing Unit*), den **Speicher mit wahlfreiem Zugriff (oder Direktzugriffsspeicher, RAM)**, die Grafik- und Soundkarten sowie verschiedene andere integrierte Schaltkreise (Chips) und Anschlüsse, die als Hardware bezeichnet werden. Die bereits erwähnten Benutzeranwendungen (Webbrowser, E-Mail-Programme usw.) gelten als Software. Zwischen der Hardware und der Software gibt es eine Zwischenschicht: das Betriebssystem. Das Betriebssystem läuft, sobald das System mit Strom versorgt wird, und verwaltet dann die Hardware-Ressourcen. Viele Benutzer haben schon mit einem Windows-, macOS- oder Linux-Rechner gearbeitet und wissen dennoch kaum etwas über die Unterschiede zwischen den jeweiligen Betriebssystemen. Die drei unterschiedlichen bekannten Betriebssysteme sind einander so ähnlich, dass ein durchschnittlicher Benutzer die grundlegenden Funktionen leicht erlernen kann. Ein Grund dafür ist, dass über eine **grafische Benutzeroberfläche** (GUI = *Graphical User Interface*) mit dem Betriebssystem interagiert wird.

Es gibt noch eine weitere Methode, um mit dem Betriebssystem zu interagieren: die Befehlszeilenschnittstelle (CLI = *Command Line Interface*). Bei der CLI geben Nutzer:innen die Befehle und die zugehörigen Modifikatoren (Optionen) über die Tastatur ein. Ein Beispiel für eine solche Schnittstelle ist das frühere MS-DOS-Betriebssystem oder die meisten Linux-Systeme.

Die Anwender:innen können als Schnittstelle entweder GUI oder CLI nutzen. Die Befehlszeilenschnittstelle (CLI) mag so manchen Einsteiger abschrecken, da sie mehr Kenntnisse des Betriebssystems erfordert und weniger intuitiv ist als die grafische Benutzeroberfläche.

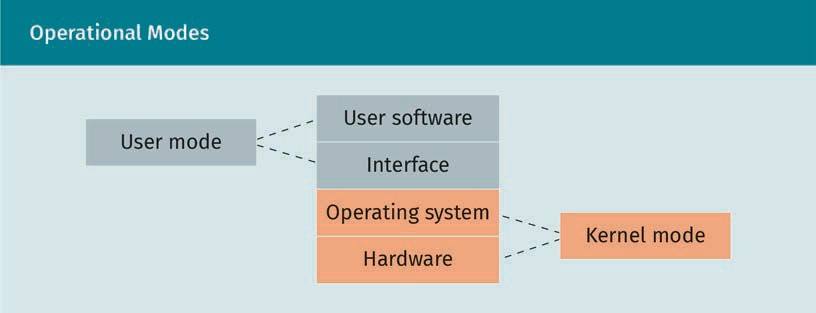
Microsoft Windows war im Jahr 2021 das am häufigsten verwendete Betriebssystem, mit macOS an zweiter Stelle, gefolgt von Linux und anderen Varianten *(Desktop operating system market share worldwide*, 2021). Trotz der Unterschiede zwischen diesen Betriebssystemen leisten sie letztlich alle dasselbe: die Steuerung der an die Hauptplatine angeschlossenen Hardware. Auch Ihr mobiles Gerät hat ein Betriebssystem, zum Beispiel Android oder iOS.



Die folgende Abbildung zeigt eine grafische Darstellung der hier besprochenen Computerstruktur. Ganz unten befindet sich die Hardware-Schicht (oder Ebene). Durchschnittliche Benutzer:innen haben normalerweise keinen Zugang zu dieser Ebene. Über der Hardware-Schicht befindet sich das Betriebssystem, über das sie je nach Berechtigung auf bestimmte Komponenten der Hardware-Schicht zugreifen können. Oberhalb des Betriebssystems befindet sich die Benutzeroberfläche, über welche die Nutzer in der Regel mit dem Betriebssystem interagieren. „**Superuser**“ verfügen über erhöhte Sicherheitsberechtigungen, mit denen sie Aufgaben ausführen können, die durchschnittliche Nutzende nicht ausführen können. Die oberste Ebene ist die der Benutzersoftware bzw. der Anwendungen. Seitlich von diesen Schichten (oder Stapel = „Stack“) sehen wir den Benutzermodus und den Kernelmodus.

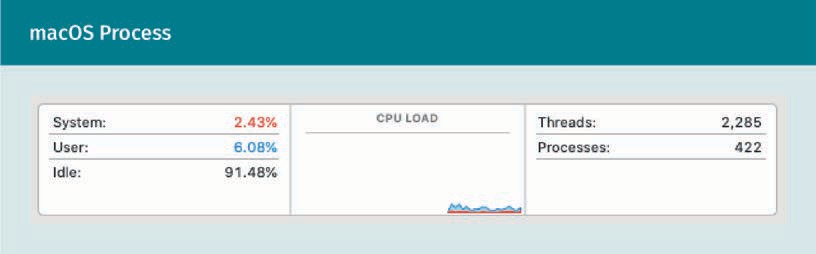
**Superuser**

Nutzer:innen eines Computersystems mit besonderen Privilegien (Berechtigungen).



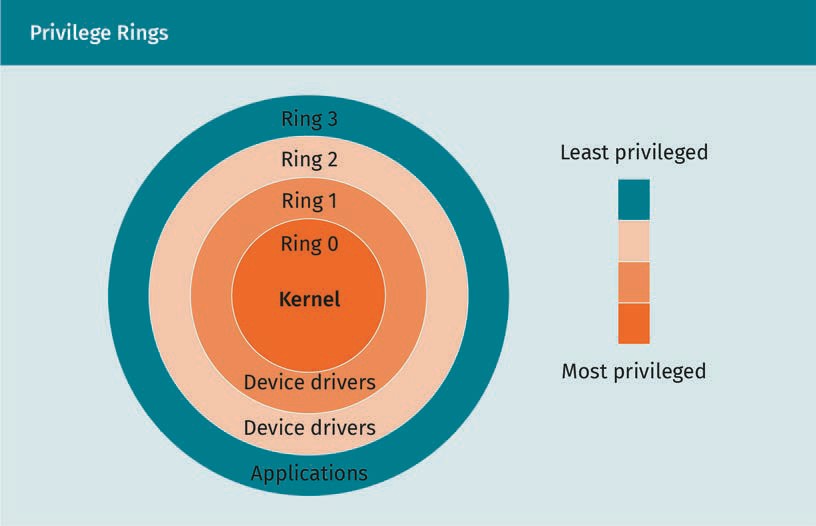
**Kernelmodus**   
Dies ist der vertrauenswürdigste Sicherheitsmodus, der den Zugriff auf alle Geräte ermöglicht.

Bei der Ausführung von Anwendungen gibt es zwei Sicherheitsmodi, den „**Kernelmodus**“ und den „Benutzermodus“. Im Kernelmodus hat die Anwendung vollständigen Zugriff auf die Systemhardware. In diesem Modus kann die Anwendung CPU-Befehle ausführen und auf alle Speicherbereiche zugreifen. Dieser Modus ist die höchste Vertrauensstufe für die Anwendungen und das Betriebssystem. Ein Systemabsturz in diesem Modus kann katastrophale Folgen haben. Im Benutzermodus hat die Anwendung nur begrenzten Zugriff auf die Hardware und muss Anfragen über eine Systemprogrammierschnittstelle (API) stellen. Wenn die Anwendung abstürzt, hat dies normalerweise keine Auswirkungen auf das System. In der folgenden Abbildung, die von einem macOS-System stammt, hat der Aktivitätsmonitor die Prozesse in „System-“ und „Benutzerprozesse“ unterteilt. Im Aktivitätsmonitor sind Systemprozesse in Rot und Benutzerprozesse in Blau dargestellt.



Dies kann auch durch ein Ringmodell dargestellt werden, wie in der folgenden Abbildung zu sehen ist. Ring Null, in der Mitte, ist am sichersten. Hier werden die vertrauenswürdigen Anwendungen ausgeführt, damit sie vollen Zugriff auf CPU- und Speicheradressen erhalten. Ring drei ist der am wenigsten sichere der vier Ringe. Hier werden normalerweise Benutzerawendungen ausgeführt, die nicht direkt auf die CPU- und Speicheradressen zugreifen. Die Ringe eins und zwei werden in der Regel nicht verwendet.

Betriebssysteme



Abgesehen von der Ausführung von Anwendungen verfügen Betriebssysteme über viele einzigartige Funktionen und Möglichkeiten, die nun im Detail betrachtet werden sollen.

###### Arten von Betriebssystemen

Es gibt verschiedene Arten von Betriebssystemen. Ein Singletasking-Betriebssystem zum Beispiel erlaubt nur die Ausführung eines einzigen Programms zu einem bestimmten Zeitpunkt. Ein Multitasking-Betriebssystem hingegen ermöglicht die Ausführung von mehr als einer Aufgabe. Das Betriebssystem erreicht dies durch Time-Sharing, wobei das Betriebssystem die CPU-Verfügbarkeit und die Prozesse überwacht. Das Betriebssystem verwendet entweder präemptives oder kooperatives Multitasking. Das präemptive Multitasking erstellt Zeitschlitze oder ‑scheiben („Slices“) und weist jedem Prozess eine bestimmte Scheibe zu. Kooperatives Multitasking verteilt die Scheiben auf viele Prozesse. Andere Kategorien von Betriebssystemen sind Systeme für einzelne und mehrere Benutzer:innen, verteilte und eingebettete Systeme sowie Echtzeitsysteme.

Betriebssysteme für einzelne und mehrere Benutzer:innen

Einzelnutzungs-Betriebssysteme können nicht von mehr als einer Person gleichzeitig verwendet werden. Ein Multi-User-Betriebssystem hingegen ermöglicht es mehreren Personen, sich gleichzeitig am System anzumelden. Das Betriebssystem weist dann den einzelnen Benutzer:innen ihre Ressourcen wie CPU-Leistung und Festplattenspeicher durch Time-Sharing zu. Das Betriebssystem verfügt über interne Buchhaltungsmechanismen zur Überwachung der zugewiesenen Rechenzeit, des Speicherplatzes und der Druckaufträge.

Verteilte Betriebssysteme

Ein verteiltes Betriebssystem verwaltet eine Gruppe verschiedener Hosts und lässt sie wie einen einzigen Computer-Host erscheinen. Das verteilte Modell kam auf, als vernetzte Computersysteme sich verbreiteten. Bei einem vernetzten System mussten die Nutzer:innen die verschiedenen Hosts im Netzwerk kennen, um Aufgaben ausführen zu können. Bei einem verteilten Betriebssystem ist dies nicht notwendig.

Eingebettete Betriebssysteme

Eingebettete Betriebssysteme werden auf Geräten, die selbst keine Computer sind, installiert und erlauben keine von den Benutzer:innen installierte Software. Diese Geräte können komplex sein und spezielle Funktionen haben. Eingebettete Geräte sind überall zu finden, auch in Smartwatches, Kühlschränken und Fernsehern. Eingebettete Betriebssysteme führen die Kernfunktionen des Systems (wie Konfiguration, Auftragsverwaltung und Speicherverwaltung) mit geringer Benutzerinteraktion aus. Die grundlegende Eigenschaft eingebetteter Systeme ist, dass keine nicht vertrauenswürdige Software auf ihnen laufen kann.

Echtzeitbetriebssysteme

Ein Echtzeitbetriebssystem verarbeitet Daten, um Aufgaben innerhalb eines bestimmten Zeitraums zu erledigen. In der Industrie sammelt das Betriebssystem beispielsweise Informationen während der Produktion. Während sich das Produkt auf dem Fließband bewegt, müssen bestimmte Aktionen zu bestimmten Zeiten stattfinden. Ein hartes Echtzeitsystem wird dazu verwendet, damit bestimmte Aktionen garantiert pünktlich stattfinden. Bei weichen Echtzeitgeräten gilt das Verpassen einer Frist als unerwünscht, aber zulässig und ohne langfristige Folgen. Benutzer:innen können keine Anwendungen auf Echtzeitgeräten installieren.

### Speicherverwaltung

Der Direktzugriffsspeicher oder Arbeitsspeicher (RAM) ist eine wichtige vom Betriebssystem verwaltet Ressource. RAM-Speicher ist nicht dasselbe wie Festplattenspeicher. Festplattenspeicher sind nicht flüchtig und dafür ausgelegt, Informationen während der Lebensdauer des Geräts zu speichern. RAM hingegen ist ein flüchtiger Speicher, der Daten nur speichert, wenn das System mit Strom versorgt wird. Sobald die Stromversorgung unterbrochen wird, sind die auf den Chips gespeicherten Daten nicht mehr vorhanden.

Die Speicherverwaltung des Betriebssystems zeichnet auf, welche Teile des Speichers genutzt werden, und weist bei Bedarf Speicherplatz zu bzw. gibt ihn frei. Frühe Computersysteme (d. h. vor den 1980er Jahren) nutzten physischen Speicherplatz *(Timeline of computer history: Memory and storage*, 2021), wobei jeder Prozess den Speicherplatz nach Bedarf nutzte. Der Nachteil dabei war, dass nur ein Prozess zu einer bestimmten Zeit den Speicherplatz nutzen konnte. So kam es zur Idee der Auslagerungsdatei („Swap-File“). Diese Auslagerungsdatei ist ein Bereich auf einem nichtflüchtigen Speichergerät wie z. B. einer Festplatte, in dem das Betriebssystem Daten zwischen dem flüchtigen Speicherbereich (RAM) und dem nichtflüchtigen Speicherbereich (Festplatte) austauscht. Der freie Zugriff auf den physischen Speicherplatz birgt jedoch einige potenzielle Sicherheitsprobleme. Wenn ein Prozess jedes Byte des physischen Speicherplatzes adressieren kann und etwas schief geht, kann dies zum Absturz des Prozesses (und möglicherweise des gesamten Systems) führen.