esse

Introduction to Security – VO 9: Betriebssystemsicherheit

Florian Fankhauser, Thomas Stipsits, Philipp Habinger

INSO – Industrial Software
Institut für Information Systems Engineering | Fakultät für Informatik | Technische Universität Wien

Agenda

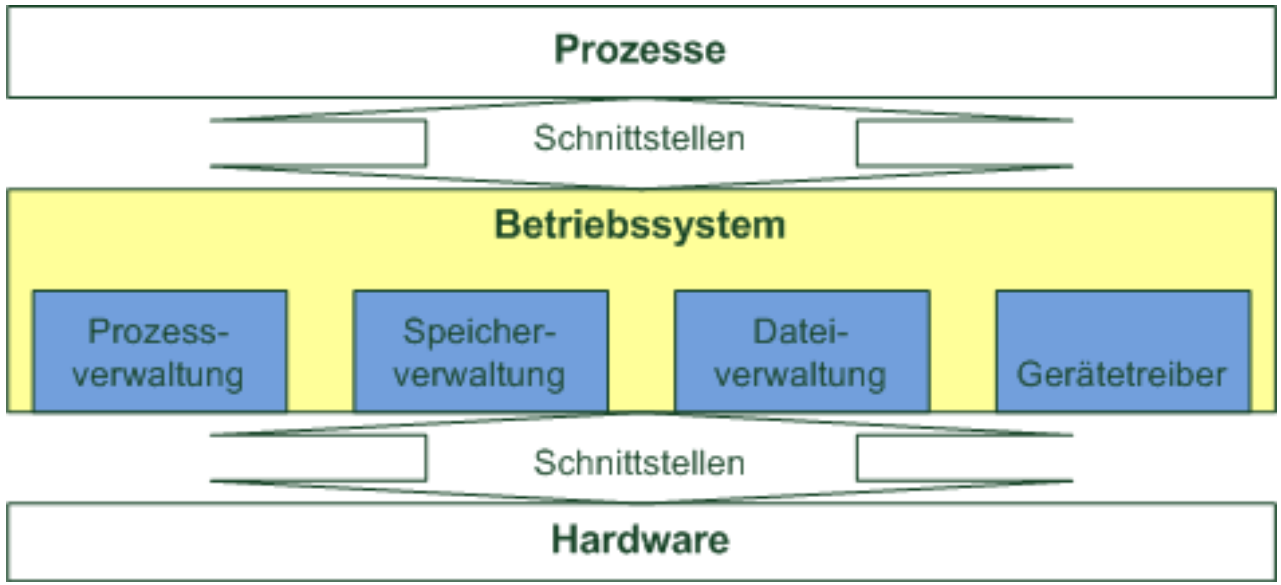
- Aktuelles
- Grundlagen
- Sicherheitsziele von Betriebssystemen
- Maßnahmen zur Erhöhung der IT-Sicherheit bei Betriebssystemen
  - Härtung von Systemen
  - Beispiele für Unix/Linux Security Konzepte
  - Grundlegende Strategie zur Sicherung von Windows
  - Beispiele für Windows Security Konzepte
  - Logging, Auditing
- Backdoors, Rootkits
- Zusammenfassung

(Nicht mehr ganz so) Aktuelles zur IT-Sicherheit von Betriebssystemen

- Sicherheitslücken: Updates auch für ältere macOS-Versionen
- Internet der Dinge: Google bringt Android Things
- Root-Rechte durch Linux-Lücke
- Android-Apps können Sperrbildschirm beliebig abschalten
- Auch der Sperrbildschirm von iOS 7 hat ein Leck
- Mac-OS-X-Finder mit Pfeiltasten ausgetrickst
- Notfall-Patch für Windows & Co.: Kritische Sicherheitslücke im Virenscanner von Microsoft
- Android-Verteilung: Android 7 nähert sich 25 Prozent

Aufgaben eines Betriebssystems

„Ein Betriebssystem umfasst die Programme eines digitalen Rechensystems, die zusammen mit den Eigenschaften der Rechenanlage die Grundlage der möglichen Betriebsarten des digitalen Rechensystems bilden und insbesondere die Abwicklung von Programmen steuern und überwachen.“ (DIN44300)



(Vergleiche Schiffmann, Wolfram: Technische Informatik 3, 2011)

Mögliche Klassifikationen und Beispiele für Betriebssysteme

- Multiuser
- Singletasking, Multitasking
- Desktop, Mobile
- Real-Time, Embedded

- Microsoft Windows (z.B. PC, IoT)
- Linux (z.B. Debian GNU/Linux, Grml, Qubes OS, Tails, Ubuntu, CentOS. . .)
- Apple OS X
- BSD-Varianten (z.B. OpenBSD, FreeBSD,. . .)
- Android, iOS
- CISCO IOS, NX-OS
- BeOS, z/OS, Solaris,. . .

Sicherheitsziele von Betriebssystemen

- Übliche Sicherheitsziele wie
  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit
- → Was bedeutet das für Betriebssysteme?
- → Wie würden Sie Betriebssysteme angreifen?

Maßnahmen zur Erhöhung der IT-Sicherheit bei Betriebssystemen

- Berechtigungssysteme
- Firewalls
- Speicherverwaltung, z.B.
  - Address Space Layout Randomization (ASLR)
  - Non Executable Stack
- Verschlüsselung von Filesystemen
- Jails/Sandboxes (z.B. chroot), Virtualisierung
- Härtung von Systemen

Minimierung der Anzahl von Angriffsvektoren/der *Attack Surface*

- Grundgedanken für die Härtung eines Systems
  - Ein nicht installiertes Service kann nicht angegriffen werden.
  - Ein nicht vorhandenes Tool kann nicht für einen Angriff verwendet werden.
  - Ein nicht vorhandenes Recht kann nicht missbraucht werden.
- Ausgewählte Methoden der Minimierung der Anzahl von Angriffsvektoren
  - Ausschließlich Services installieren, die erforderlich sind
  - Ausschließlich Tools installieren, die erforderlich sind
  - Nur BenutzerInnen anlegen, die erforderlich sind
  - Rechte restriktiv vergeben (BenutzerInnen, Files,. . . → Concept of Least Privilege)

Härtung von Systemen

- „‚Härten‘ (engl. Hardening) bedeutet in der IT-Sicherheit die Entfernung aller Softwarebestandteile und Funktionen, die zur Erfüllung der vorgesehenen Aufgabe durch das Programm nicht zwingend notwendig sind.“ (BSI: Leitfaden IT-Sicherheit, 2012)
- Ziel: Verringerung der Möglichkeiten für Angriffe
- Hardening ist prinzipiell auf allen (konfigurierbaren) Systemen möglich, unabhängig vom Betriebssystem
- Hardening ist eine zusätzliche Maßnahme, *kein* Ersatz für andere Sicherheitsmaßnahmen (wie z.B. Security Patches etc.)

Offene TCP-Ports in einer Debian Standardinstallation mit Serverdiensten

```
$ nmap [...]

Starting Nmap 5.00 ( http://nmap.org ) at 2010-04-30 06:12 CEST
Interesting ports on 192.168.1.38:
Not shown: 990 closed ports
PORT     STATE SERVICE     VERSION
53/tcp   open  domain      ISC BIND 9.5.1-P3
80/tcp   open  http        Apache httpd 2.2.9 ((Debian) PHP/5.2.6-1+lenny8 with Suhosin-Patch mod\_python/3.3.1
|\_Python/2.5.2 mod\_perl/2.0.4 Perl/v5.10.0)
|\_ html-title: Site doesn't have a title (text/html).
110/tcp  open  pop3        Qpopper pop3d 4.0.9
|\_ pop3-capabilities: USER EXPIRE(NEVER) UIDL X-MANGLE APOP TOP AUTH-RESP-CODE RESP-CODES IMPLEMENTATION
    (Qpopper-version-4 0 9) X-LOCALTIME(Fri 30 Apr 2010 08 14 42 0200) LOGIN-DELAY(0) X-MACRO
111/tcp  open  rpcbind
|  rpcinfo:
|  100000  2        111/udp  rpcbind
|  100003  2,3,4   2049/udp  nfs
[...]
139/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
143/tcp  open  imap?
|\_ imap-capabilities: LOGIN-REFERRALS THREAD=ORDEREDSUBJECT ESEARCH UNSELECT SCAN LOGINDISABLED MAILBOX-REFERRALS
    WITHIN CHILDREN BINARY IMAP4REV1 THREAD=REFERENCES STARTTLS UIDPLUS SASL-IR SORT I18NLEVEL=1 LITERAL+ IDLE
    NAMESPACE MULTIAPPEND
445/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
901/tcp  open  http        Samba SWAT administration server
|\_ html-title: 401 Authorization Required
|  http-auth: HTTP Service requires authentication
[...]
```

Offene TCP-Ports in einer OpenBSD Standardinstallation

```
$ nmap [...]

Starting Nmap 5.00 ( http://nmap.org ) at 2010-04-30 06:29 CEST
Interesting ports on 192.168.1.39:
Not shown: 987 closed ports
PORT     STATE    SERVICE VERSION
13/tcp   open     daytime
22/tcp   open     ssh     OpenSSH 5.3 (protocol 2.0)
|  ssh-hostkey: 1024 e9:01:93:36:3e:ca:fc:aa:fd:e7:f2:a3:c9:87:38:88 (DSA)
|\_ 2048 f5:aa:ce:f5:f7:2a:a0:7a:63:63:37:17:08:ac:ad:47 (RSA)
37/tcp   open     time?
113/tcp  open     ident
6000/tcp filtered X11
6001/tcp filtered X11:1
6002/tcp filtered X11:2
6003/tcp filtered X11:3
6004/tcp filtered X11:4
6005/tcp filtered X11:5
6006/tcp filtered X11:6
6007/tcp filtered X11:7
6009/tcp filtered X11:9
```

Offene TCP-Ports Win Vista/7/8/8.1/10 Standardinstallation

Offener Port	Protokoll	OS	Profil	Prozess
135	TCP	Windows Vista/7/8/8.1/10	Domäne	svchost.exe (RPC Service)
139, 445	TCP	Windows Windows 10	All	netbios-ssn
443	TCP	Windows Vista/7	Domäne/Privat	System

Standardmäßig aktivierte Funktionalitäten/einige mitgelieferte Apps öffnen diverse TCP-Ports:

Beliebig	TCP	Windows 8/8.1/10	All	Mail-, Kalender/ Kontake/ Nachrichten- App
Beliebig	TCP	Windows 8.1/10	All	Skype-App
Beliebig	TCP	Windows 8/8.1/10	Domäne/Privat	Store-App
Verschiedene	TCP	Windows 8/8.1/10	All	Diverse Ports für Play-To-Funktionalität
Beliebig	TCP	Windows 8.1/10	All	VPN-Apps
Beliebig	TCP	Windows 8.1/10	Öffentlich	Diverse Ports für WiFi-Direct-Funktionalität
Beliebig	TCP	Windows 8.1/10	Privat/Öffentlich	WUDFHost.exe

Offene TCP-Ports Win Server 2008/2008 R2/2012/2012 R2 Standardinstallation

Offener Port	Protokoll	OS	Profil	Prozess
135	TCP	Windows Server 2008/ Windows Server 2008 R2	Domäne/Privat/Öffentlich	svchost.exe
445	TCP	Windows Server 2008/ Windows Server 2008 R2	Domäne/Privat/Öffentlich	System
Beliebig	TCP	Windows Server 2008/ Windows Server 2008 R2	Domäne/Privat/Öffentlich	dfsfrsHost.exe
Beliebig	TCP	Windows Server 2008/ Windows Server 2008 R2	Domäne/Privat/Öffentlich	svchost.exe
5985	TCP	Windows Server 2012/ Windows Server 2012 R2	Öffentlich	System

Härten – in einer idealen Welt

- Erstellung eines Minimal-Systems
  - Auswahl sicherer Hardware
  - Service(s)
  - (Remote) Admin Utilities
  - Support Libraries
  - Betriebssystem
  - System Monitoring
- Eingeschränkte, sichere Konfiguration
- Beispiel für ein Minimalsystem und gutes Know-How
  - Linux From Scratch (LFS)

Härten – in der realen Welt

- . . . selten möglich
- Gründe dafür sind beispielsweise
  - Fehlendes Know-How
  - Budget
  - Zeit
  - 3rd Party Software
  - Proprietäre Systeme

Härten bestehender Systeme – Umsetzung in der realen Welt

- Erforderliche Funktionen festlegen
- System installieren, updaten (nicht immer eine Option)
- Nicht erforderliche Software entfernen
- Falls nicht löschbar: nicht erforderliche Dienste deaktivieren
- Zugriffsrechte strenger setzen
- Konfigurationen überprüfen
- Default Passwörter/Geheimnisse ändern
- ...

Linux: Paketverwaltung

- viele Varianten (apt, rpm, emerge, ipkg)
- Einfache (De)Installation von Softwarepaketen des Distributors
- Paket Verwaltung verwaltet Abhängigkeiten, nicht immer perfekt (z.B. bind erfordert dbus in CentOS)
- Beispiel Centos System
  - „Minimale Installation“ → ca. 400 Pakete
  - `rpm -qa # Liste der installierten Pakete`
  - `yum remove make alsa-lib cpp ... patch wget zip`
  - Durch manuelle Entfernung von nicht erforderlichen Paketen ca. 200 Pakete incl. gewünschtes Service
  - Manche Services lassen sich nicht entfernen z.B. sendmail → Start als Service verhindern oder gegen „sicherere“ Programme tauschen

Beispiele für Unix/Linux Security Konzepte

- Berechtigungen (ls, chmod, chown, chgrp)
  - User, Group, Others
  - Weitere Modelle, unterschiedlich weit verbreitet
    - erweiterte Berechtigungen (lsattr, chattr)
    - ACL granulare Berechtigungen
    - SELinux/AppArmor
- Chroot/Jailroot, Linux Container, Docker
- suid/sgid
- Alle BenutzerInnen sind diesen Sicherheitskonzepten unterworfen, i.A. Ausnahme root
- Unterschiedliche Maßnahmen, um Speicher zu schützen

Berechtigungen

- Zugang zu IT-System
- Filesystem
- Memory
- → siehe auch VO zu Authentifizierung

Berechtigungen – Principle of Least Privilege

- Principle of Least Privilege: The principle of least privilege states that a subject should be given only those privileges that it needs in order to complete its task. (M. Bishop: Computer Security: Art and Science)
- Daraus folgt mindestens
  - Nicht-priviligierte User-Accounts
  - Priviligierte(r) Administrations-Account(s), z.B. `root` in Linux oder `Administrator` in Windows
- Für unterschiedliche Aktionen sind besondere Rechte erforderlich, z.B. Installation von Programmen oder Änderung von Passwörtern
  - z.B. `sudo` in Linux
  - z.B. `Runas` in Windows

Berechtigungen von root

- Files/Directories Lesen
- Änderung von Zugriffsberechtigungen
- Wechsel der UID
- Prozesssteuerung
- Verändern von Systemparametern (Limits f. Prozesse, Filesysteme,. . .)
- User-Management
- System-Management (Shutdown, Reboot,. . .)
- Aktivierung Promiscous Mode v. Netzwerk Interfaces
- Filesysteme (un)mounten
- chroot
- . . .

suid

- Viele Systemprogramme nutzen das suid-Bit
- Theoretisch kein Sicherheitsproblem
- Praktisch jedoch immer wieder fehlerhaft implementiert (z.B. Buffer Overflows)
- suid wird oft verwendet, obwohl nicht erforderlich
- Suchen von suid Programmen (als `root`!): `find / -perm -4000 -print`

chroot

- change root: / wird geändert
- z.B. `/var/www` → /
- Verwendung für Testumgebung
- Erhöhung der Sicherheit
- richtige Anwendung beachten – Benutzer root
- Minimierung der Tools in einer Jail-Umgebung

Bibliotheken und chroot

- Bei dynamisch gelinkten Applikationen müssen die Bibliotheken alle aus dem Jail erreichbar sein, d.h. in der neuen durch `chroot` erzeugten Umgebung
- Statisch gelinkte Applikationen funktionieren ohne weitere Bibliotheken
- Beispiel:

```
$ ldd /usr/bin/whoami
    linux-gate.so.1 =>  (0xffffe000)
    libc.so.6 => /lib/tls/i686/cmov/libc.so.6 (0xb7dc7000)
    /lib/ld-linux.so.2 (0xb7f08000)
```

Linux-Firewall

- Backend derzeit `iptables`
- Frontends: Commandline, GUIs
- Überwacht und filtert gesamten Datenverkehr über TCP/IP
- Einfacher Packet-Filter oder Stateful Inspection
- Hohe Flexibilität

Remote-Zugriff auf Linux

- SSH als Standard
  - Deaktiviertes X-Forwarding
  - Aktiviertes X-Forwarding
  - Verwendung von Programmen wie screen/tmux/...
- Weitere Tools wie Remote Desktop/VNC usw. ebenfalls möglich

Grundlegende Strategie zur Sicherung von Windows

- Das Starten von Programmen/Services ist standardmäßig verboten und nur für zugelassene Programme erlaubt
- Ausgehender und eingehender Netzwerkverkehr ist grundsätzlich verboten und nur für festgelegte Ausnahmen erlaubt
- Die automatische Nutzung von administrativen Rechten für administrativen Konten ist deaktiviert
- Weitere unterstützende Maßnahmen:
  - Durchführen von (kontrollierten) Windows Updates
  - Isolierung von Software (AppContainer)
  - Einsatz der Windows Defender Advanced Threat Protection (ATP)
  - ...

Windows Zugriffssteuerung

- Berechtigungen
  - Festlegung des gewährten Zugriffs auf ein Objekt oder eine Objekteigenschaft für BenutzerInnen/Gruppen
  - Prinzipiell Lesen, Ändern, Eigentümer ändern, Löschen
- BenutzerInnenrechte / Kontorechte
  - BenutzerInnen und Gruppen erhalten innerhalb der Computerumgebung spezielle Privilegien und Anmelderechte
  - z.B. Anmelderechte lokal / über NW / über RDP,...
- Objektüberwachung von abgesicherten Objekten
  - Überwachen von BenutzerInnenzugriffen auf Objekte
  - Sicherheitsereignisse werden im Sicherheitsprotokoll registriert
- Globale Überwachungsrichtlinien
  - Für alle Objekte im Dateisystem / Registry-Keys oder beides

BenutzerInnenverwaltung in Windows

- Verwaltung von Konto/Nutzerrechte, Kennwortrichtlinien, Systemüberwachung, Authentifizierung, ...
- Lokale Nutzerverwaltung
  - Local Security Authority Subsystem Service (LSASS) verwaltet lokale Systemsicherheitsrichtlinie
  - Security Accounts Manager (SAM) verwaltet lokale NutzerDB
  - 'Administrator' (SID S-1-5-21*-500) ist der erste lokale Benutzer am System
- Verzeichnis-basierte Nutzerverwaltung - Active Directory
  - Nutzer, Gruppen, Computer in der Windows Domäne (Netzwerk-Domäne)
  - Zugriffsteuerung von Nutzer und Gruppen auf lokale und Domänen-Ressourcen
  - Group Policy Objects (GPOs) - sowohl local als auch global

Administrative und nicht-administrative Gruppen

Die BenutzerInnenverwaltung unter Windows kann grob in privilegierte (administrative) Gruppen und nicht-privilegierte (nicht-administrative) Gruppen eingeteilt werden.

Administrator	Vollzugriff, zuweisen von Rechten und Berechtigungen
Benutzer	allgemeine berechtigte Aufgaben
Gäste	temporäres Profil, standardmäßig deaktiviert
Hauptbenutzer	BenutzerInnenkonten erstellen, lokale Gruppen,...

Windows Access Token

- Nach erfolgreicher lokaler Anmeldung erstellt LSASS ein Windows-Zugriffstoken
- Art des Tokens je nach Sicherheitskontext zu Konto, Gruppen & Rechte unterschiedlich
- Jeder vom System für den angemeldeten Nutzer erzeugte Prozess erhält eine Kopie
- Informationen aus dem Token werden benutzt, um Zugriffsrechte des Prozesses auf das jeweilige Zielobjekt zu ermitteln

- Nutzung von Kerberos Tickets und des Kerberos Authentifzierungsprotokolls in der Windows Domäne

Windows Firewall

- Überwacht und filtert gesamten Datenverkehr über TCP/IP
- Ist eine Stateful Inspection Firewall
  - Zuordnung der Pakete zu aktiver Session
  - Für alle Verbindungen, welche der PC nach außen initiiert, ist eine Rückverbindung nach innen zulässig
- Erwünschter eingehender Datenverkehr muss ausdrücklich zugelassen werden
  - Ausnahmeliste mittels Portnummer, Anwendungsname oder Dienstname

Gruppenrichtlinien

- Steuerung von (Sicherheis)einstellungen auf dem System
- Zentralisierte Verwaltung der Computer in einer Domäne
  - Konfiguruation über Gruppenrichtlinienobjekte (GPO)
  - Regelmässige Aktualisierung der Gruppenrichtlinien aus der Domäne
  - Lokale GPO – Gilt nur für eine Maschine
  - Globale GPO – Gilt für alle Maschinen in Domäne
- Administrative Vorlagen für eine Vielzahl an Einstellungen, z.B.
  - Richtline für sichere Kennwörter
  - Konfiguration der Windows Firewall
  - Zugriffe auf Wechselmedien regulieren

UAC – die BenutzerInnenkontensteuerung von Windows

- User Account Control, basiert auf Integrity Levels (MIC) und Access Tokens
- Explizite Zustimmung zur Nutzung administrativer Rechte
- Nutzung von administrativen Rechten erst durch Zustimmungsabfrage
  - Rechtereduzierung beim Zugriff auf nicht vertrauenswürdiger Datenquellen
  - Zusätzliche Hürde um Malware mit administrativen Rechten auszuführen
  - Jedoch kein Schutz vor Malware, die mit reduzierten Zugriffsrechten ausführbar ist

Mandatory Integrity Control (MIC)

- Kernkomponente der Windows Sicherheitsarchitektur
- Separierung unterschiedlicher Prozesse eines Nutzerkontos
- Definieren das maximale Zugriffsrecht, das ein Prozess auf ein Windows-Objekt ausüben darf
- Bei einem Aufruf wird der Aufrufer (Prozess) einem Integrity Level zugeordnet
- Unterscheidung der Integrity Levels gemäß Security Identifier (SID) S-1-16-xxxx:
  - S-1-16-0 - Untrusted (0x0000)
  - S-1-16-4096 - Low (0x1000)
  - S-1-16-8192 - Medium (0x2000)
  - S-1-16-12288 - High (0x3000)
  - S-1-16-16384 - System (0x4000)
  - S-1-16-20480 - Protected (0x5000, derzeit defaultmäßig nicht verwendet)

Logging, Auditing

- Linux
  - primär Logfiles, z.B. `/var/log/`
    - `messages`, `syslog`, `auth`, ...
  - AIDE, Snort, ...
  - Diverse System-Tools zum Auditing (`lsof`,...)
- Windows
  - Windows erzeugt Event Logs (Ereignisprotokolle)
  - Aufgetretene Ereignisse einsichtbar per Event Viewer (Ereignisanzeige)
    - Anwendungsereignisse
    - Sicherheitsbezogene Ereignisse
    - Setupereignisse
    - Systemereignisse
    - Weitergeleitete Ereignisse

Windows Spezifisches: Absicherung von Remotedesktopzugängen

- Remote Desktop / WinRM ist für viele AdministratorInnen unverzichtbar für die tägliche Arbeit
- Zugriff auf den Windows-Desktop und Einstellungen mit den Privilegien des Benutzers
- Mögliche Maßnahmen zur Absicherung von RD Zugriffen:
  - Einschränkung der Reichweite des RD-TCP-Ports
  - Härten des RDP-Protokolls (Verschlüsselung, Ciphers)
  - Unterbinden administrativer Anmeldungen per Remotedesktop mittels RDP-ACLs
  - Aktivierung der Network Level Authentication

Backdoors, Rootkits

„You can't trust code that you did not totally create yourself. ... No amount of source-level verification or scrutiny will protect you from using untrusted code."

- Ständige Problematik von Hintertüren
- Absicht ist unentdeckt und/oder illegal
  - geschützte Daten einzulesen, und/oder
  - Änderungen an geschützten Daten vorzunehmen
- Lösung Open Source?
- Rootkit
  - Start direkt zu Beginn des Systems
  - Änderung von tiefgreifenden OS-Funktionen
  - möglichst unbemerkt von BenutzerIn

Literatur 1/2

- Herbert H. Thompson. Why security testing is hard. *IEEE Security & Privacy Magazine*, 1(4):83–86, 2003. ISSN 1540-7993. doi: 10.1109/MSECP.2003.1219078
- Bundesamt für Sicherheit in der Informationstechnik. Leitfaden informationssicherheit, 2012. `https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzUeberblick/LeitfadenInformationssicherheit/leitfaden_node.html`
- Matt Bishop. *Computer Security: Art and Science*. Pearson Education, Inc, 2003. ISBN 0-201-44099-7
- Ed Skoudis and Tom Liston. *Counter Hack Reloaded. A Step-by-Step Guide to Computer Attacks and Effective Defenses*. Pearson Education, Inc., 2 edition, 2006. ISBN 0-13-148104-5
- LFS (Linux From Scratch) `http://www.linuxfromscratch.org/`

Literatur 2/2

- Darril Gibson. *Microsoft Windows Security Essentials*. Sybex, 2011. ISBN 978-0-7356-2174-9
- Derrick Rountree. *Security for Microsoft Windows System Administrators: Introduction to Key Information Security Concepts*. Syngress, 2011. ISBN 978-1-59749-595-0
- Microsoft TechNet `http://technet.microsoft.com`
- Gentoo. Project:hardened, 2017. `https://wiki.gentoo.org/wiki/Project:Hardened`

Zusammenfassung

- Angriffe auf Betriebssysteme finden statt
- Unterschiedliche Beispiele für Betriebssysteme
- Sicherheitsziele von Betriebssystemen
- Maßnahmen zur Erhöhung der IT-Sicherheit bei Betriebssystemen
  - Linux
  - Windows
- Härtung von Systemen
- Backdoors, Rootkits

Vielen Dank!

https://security.inso.tuwien.ac.at/