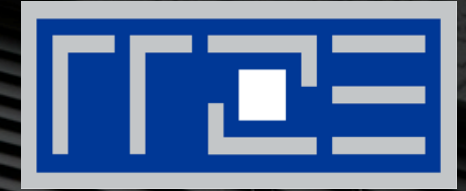


REGIONALES RECHENZENTRUM ERLANGEN [RRZE]

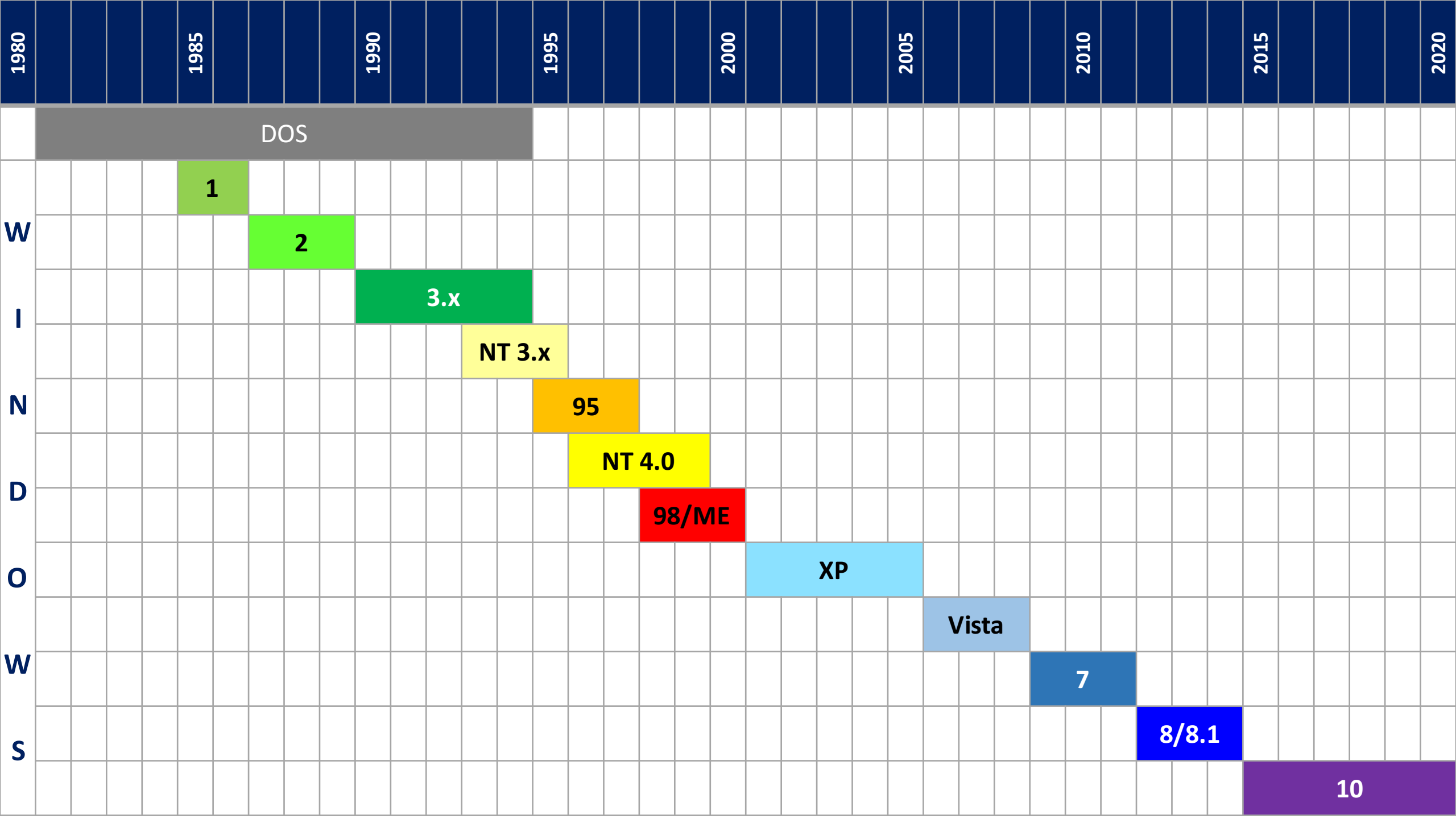


Windows-Betriebssysteme

Systemausbildung – Grundlagen und Aspekte von
Betriebssystemen und System-nahen Diensten, 11.05.2016
Sonja Schmidt, Sebastian Schmitt, RRZE

Agenda

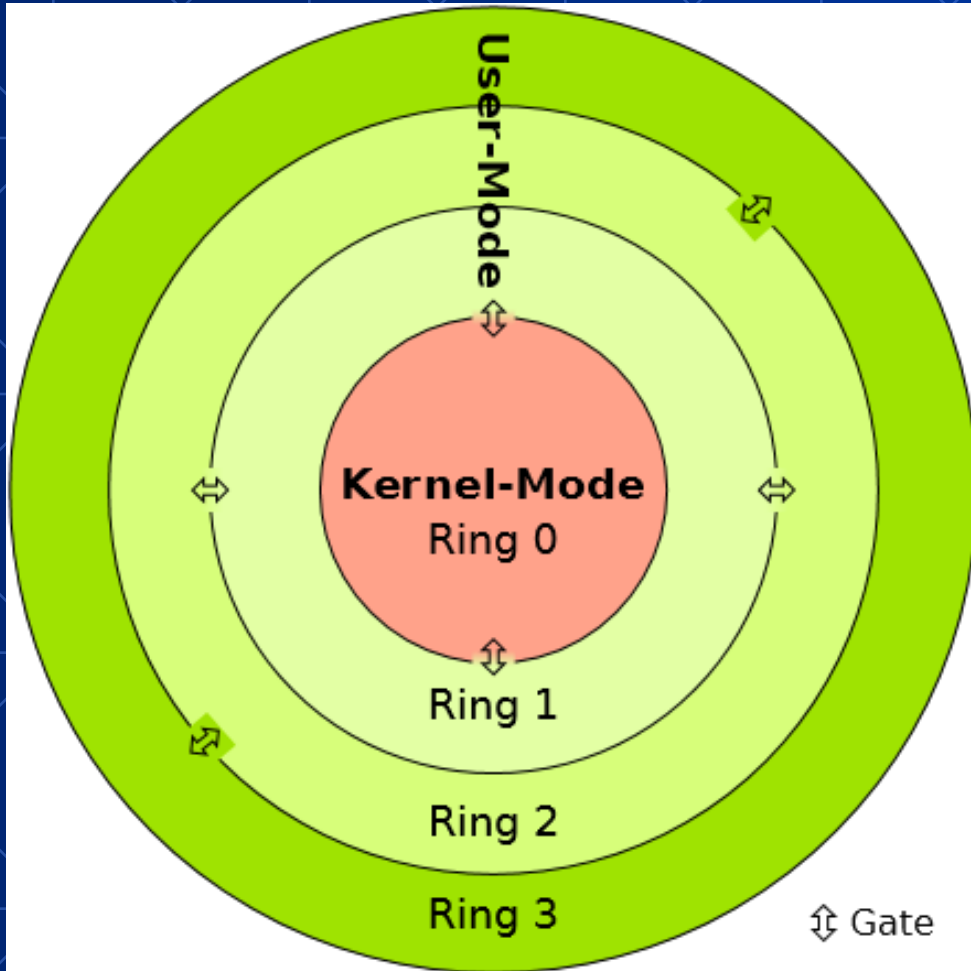
- Einführung
- Aufbau
- Verzeichnisstruktur
- Benutzer/Gruppen, Dateien und Rechte
- Prozesse, Last und Speicher
- Registry
- Fehlersuche – Hilfe zur Selbsthilfe



Aufbau – Betriebssystem

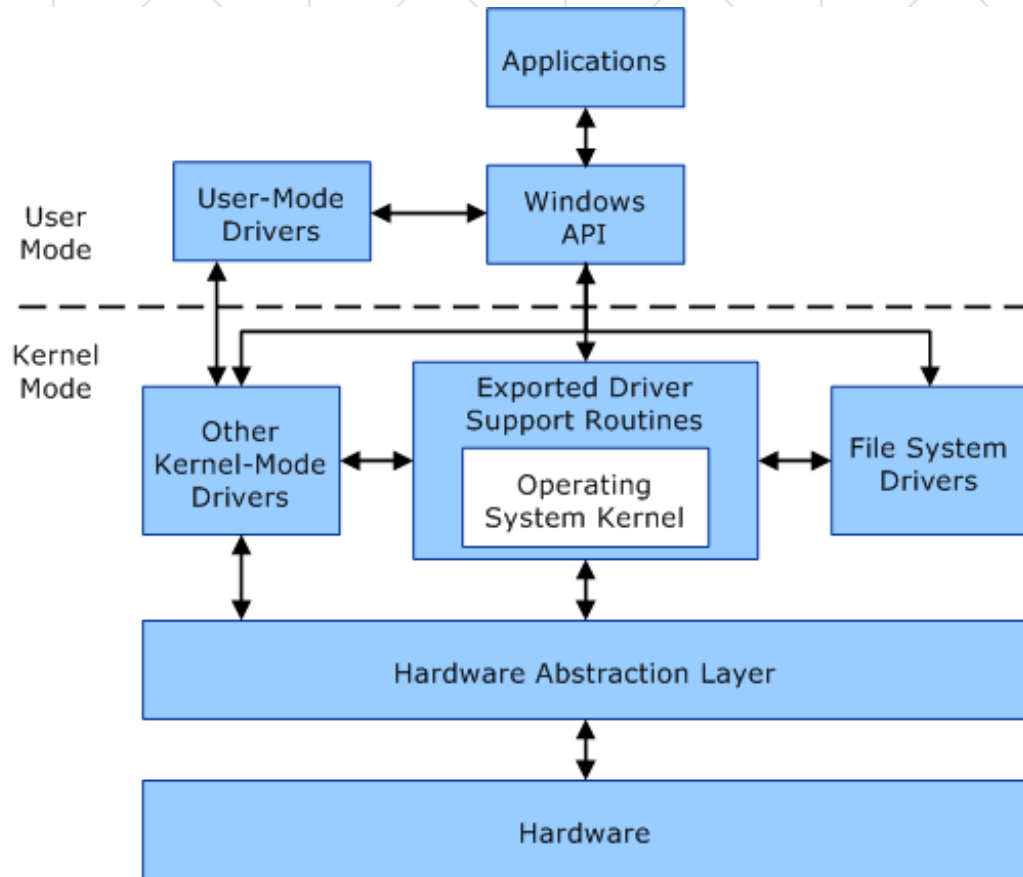
- Das Ringmodell
- Allgemeiner Aufbau
- Mehr Rechte unter Windows
 - Arbeiten als Administrator
 - Ausführen als („Run as“)
 - User Access Control

Das Ringmodell



- Eingeführt mit Betriebssystem Multics
- Trennung zwischen User- und Kernelmode
- Kommunikation nur über „Gates“; erfordern CPU-Kontextwechsel
- Supervisor-Mode-Flag
- DOS, Windows, Linux nutzen nur 2 Ringe – Ring 0 und Ring 3
- Virtualisierung wird möglich

Windows – struktureller Aufbau



- Trennung zwischen Kernel- und User-Mode
- Modulare Struktur
- Objektorientiert
- Treiber gibt es in „beiden Welten“

Quelle: [https://msdn.microsoft.com/en-us/library/windows/hardware/ff554836\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/hardware/ff554836(v=vs.85).aspx)

Rechte unter Windows

- Arbeiten als lokaler Administrator
 - Sehr bequem, denn es geht (fast) alles
 - Alle Programme, haben Admin-Rechte, auch Viren und Rootkits!
 - Nicht zu empfehlen, da höchste Berechtigungsstufe auf lokalem System → sehr sparsam verwenden!
- Ausführen als („Run as“)
 - Bessere Alternative, da nur Prozess mit Admin-Rechten läuft
 - Geht nicht immer

User Access Control (UAC)

- Eingeführt mit Windows Vista
- Immer Benutzerrechte – auch als Admin, es sei denn der Prozess fordert höhere Rechte explizit an
- Ähnlich zu „Ausführen als“
- Trotzdem User-Mode (Ring 3) – kein Kernelmode (Ring 0)
- Default: aktiviert
- Nur global abschaltbar – aber Vorsicht (siehe lokaler Admin)

Partitionierung Allgemein

- Abgrenzung der HDD/SSD in Bereiche um Betriebssystem verwendbar zu machen
- 2 Partitionsarten
 - Primäre Partition
 - Erweiterte Partition → Logische Laufwerke
- Windows benötigt Primäre Partition
- GPT und UEFI

Partitionen nach der Installation

Datenträgerverwaltung

Datei Aktion Ansicht ?

Volume	Layout	Typ	Dateisy...	Status	Kapazität	Freie...	% frei
	Einfach	Basis		Fehlerf...	300 MB	300 ...	100 %
	Einfach	Basis		Fehlerf...	22,99 GB	22,9...	100 %
	Einfach	Basis		Fehlerf...	1,00 GB	1,00 ...	100 %
(C:)	Einfach	Basis	NTFS	Fehlerf...	673,74 GB	626,...	93 %

CD 0
DVD (D:)
Kein Medium

Datenträger 0
Basis
698,51 GB
Online

500 MB	300 MB	(C:) 673,74 GB NTFS	22,99 GB	1,00 GB
Fehlerfrei (Wiederherstel	Fehlerfrei (EFI-System)	Fehlerfrei (Startpartition, Auslagerungsdatei, Absturzab	Fehlerfrei (Wiederherstellungspartition)	Fehlerfrei (Wiederherstellun

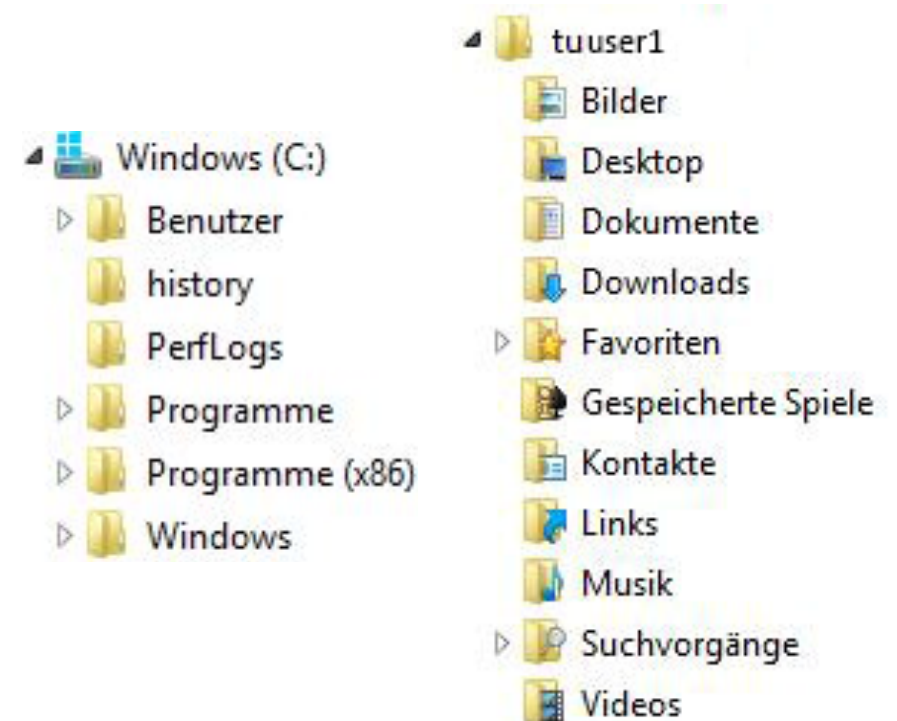
■ Nicht zugeordnet ■ Primäre Partition

BIOS vs. UEFI

- UEFI (Unified Extensible Firmware Interface) ist Nachfolger des BIOS (Basic Input Output System)
- Normales BIOS in UEFI enthalten zwecks Kompatibilität
- Schnittstelle zwischen Betriebssystem, Hardware und Firmware
- In UEFI ist Secure Boot enthalten
- Secure Boot prüft Signaturen um Schadsoftware „auszusperren“

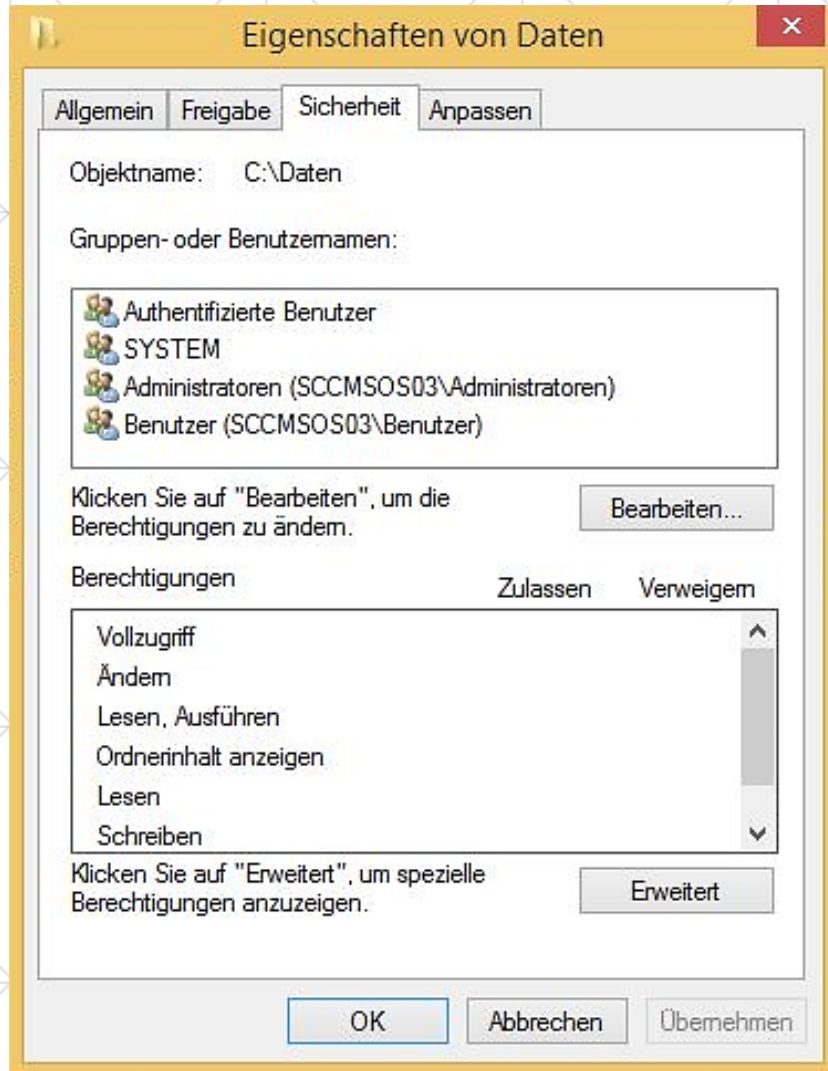
Filesystem

- NTFS (New Technology File System)
- Eingeführt mit Windows NT
- Baumstruktur
- Dateiberechtigungen von Windows werden festgelegt
- Journaling Funktion
- Bit Locker



Dateiberechtigungen

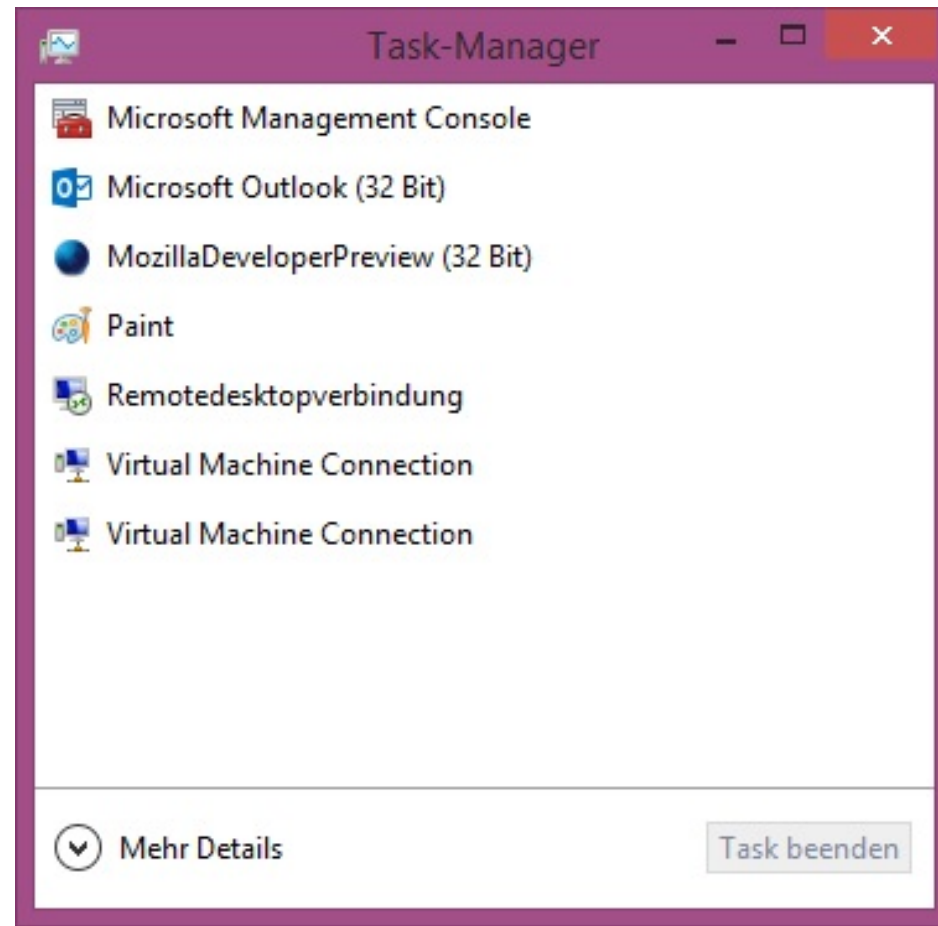
- Vererbung von „oben“ nach „unten“
- Verbieten schlägt Erlauben
- Flexible Rechte durch Gruppenberechtigung
- **Empfehlung:** Immer auf Gruppen
- Jeder hat Leserechte (Default)



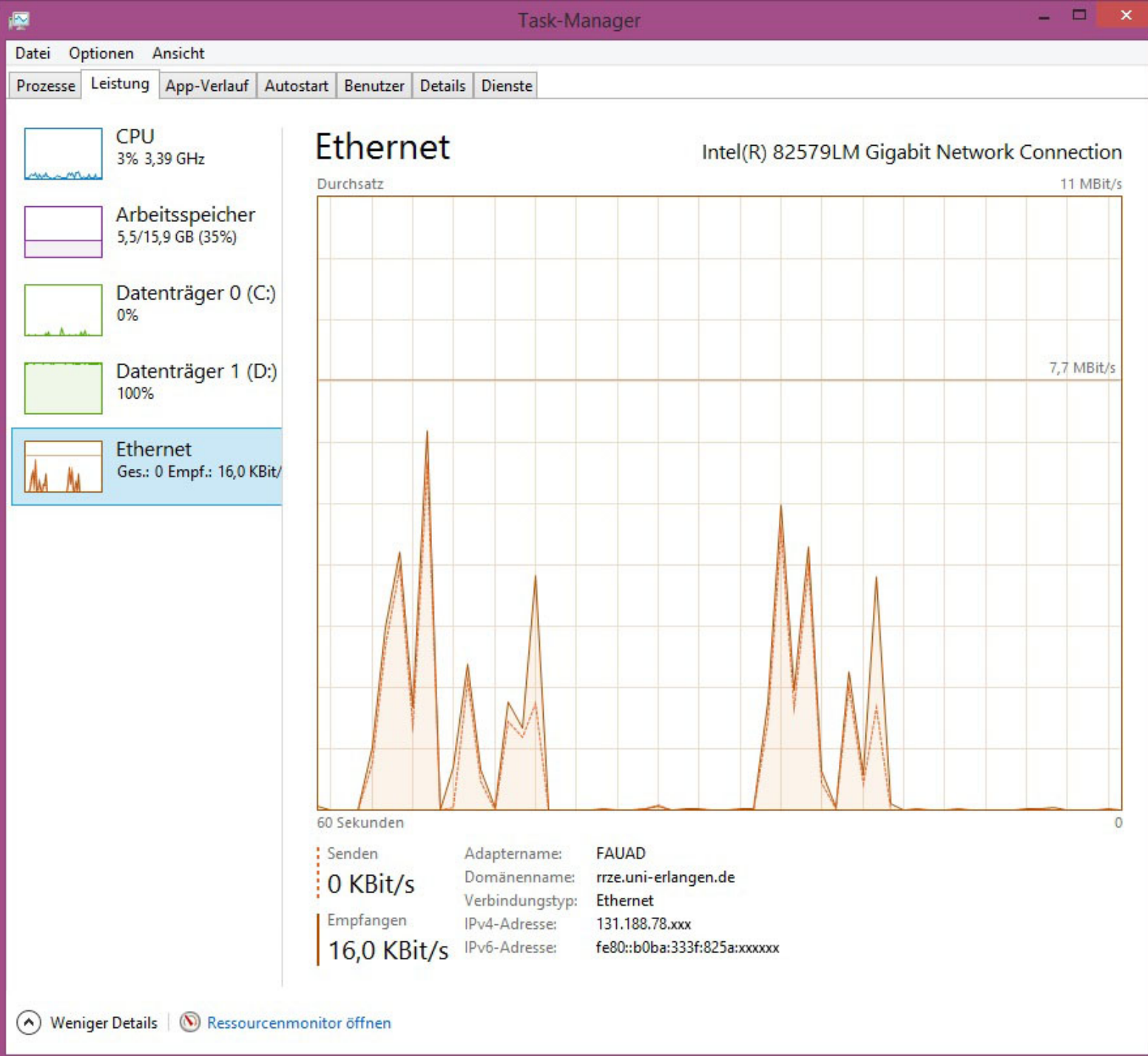
Prozesse, Last und Speicher

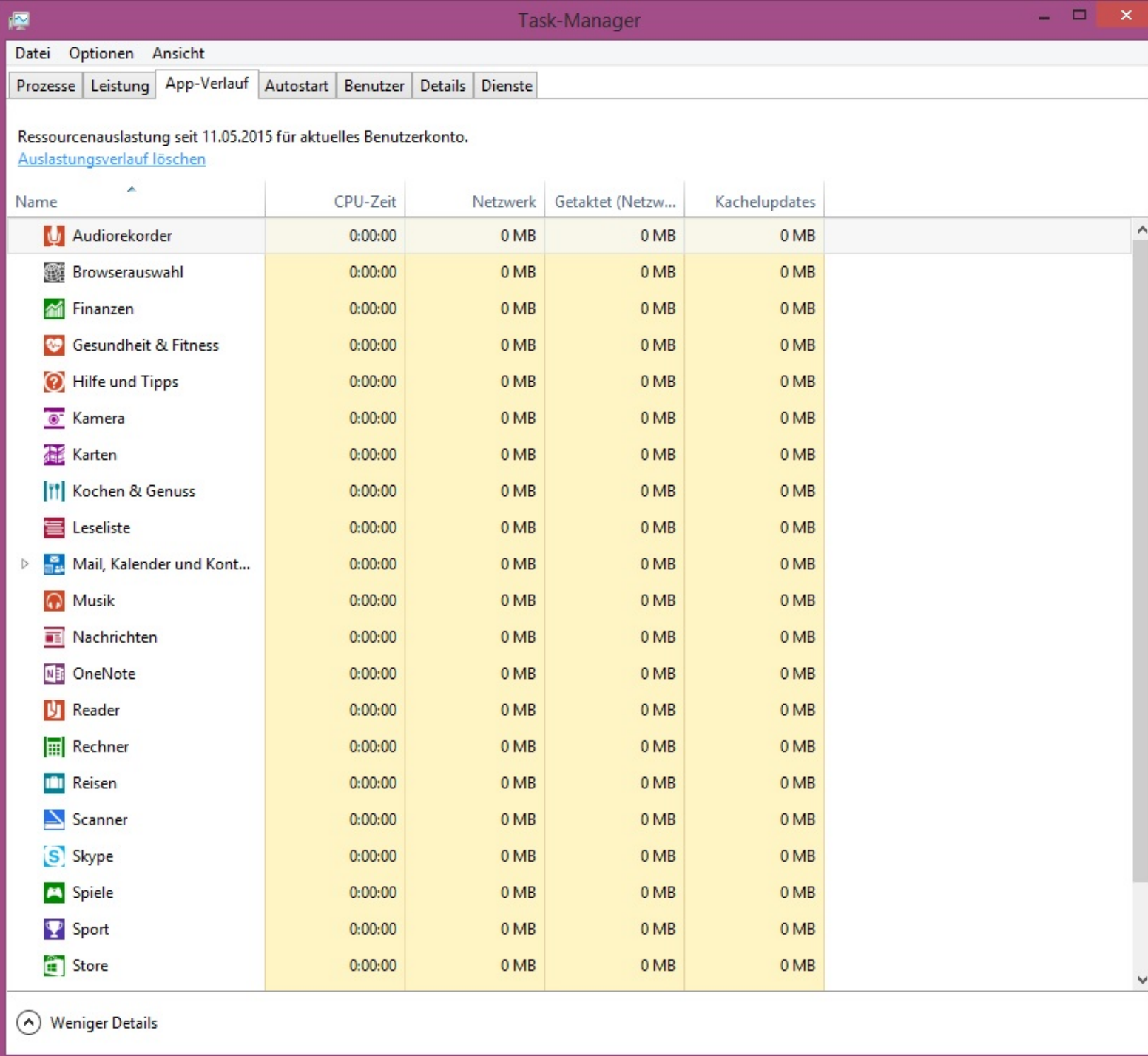
- Übersicht im Taskmanager
- Bei Fehler Prozesse über Taskmanager beenden (evtl. Dateiverlust)
- Ressourcenmonitor
 - Speicherauslastung
 - Datenträgersauslastung
 - Netzwerkauslastung
 - Prozessorauslastung






















Task-Manager



Task-Manager					
Datei Optionen Ansicht					
Prozesse Leistung App-Verlauf Autostart Benutzer Details Dienste					
Name	Status	5% CPU	33% Arbeitss...	42% Datenträ...	0% Netzwerk
Apps (8)					
Microsoft Management Console		0,9%	18,0 MB	0 MB/s	0 MBit/s
Microsoft Outlook (32 Bit)		0,2%	56,9 MB	0,1 MB/s	0,1 MBit/s
MozillaDeveloperPreview (32 Bit) (3)		0%	254,1 MB	0 MB/s	0 MBit/s
Remotedesktopverbindung		0%	159,6 MB	0 MB/s	0,1 MBit/s
Task-Manager		0,4%	10,2 MB	0 MB/s	0 MBit/s
Virtual Machine Connection		0%	114,8 MB	0 MB/s	0 MBit/s
Virtual Machine Connection		0%	114,9 MB	0 MB/s	0 MBit/s
Windows-Explorer (4)		2,0%	70,5 MB	0 MB/s	0 MBit/s
Hintergrundprozesse (48)					
AcroTray (32 Bit)		0%	0,9 MB	0 MB/s	0 MBit/s
Adobe Acrobat Update Service		0%	0,7 MB	0 MB/s	0 MBit/s
AMD External Events Client Module		0%	1,3 MB	0 MB/s	0 MBit/s
AMD External Events Service Module		0%	0,5 MB	0 MB/s	0 MBit/s
Arbeitsprozess für virtuelle Computer		0%	13,4 MB	0 MB/s	0 MBit/s
Arbeitsprozess für virtuelle Computer		0%	13,0 MB	0 MB/s	0 MBit/s
Bing Desktop updating service		0%	1,6 MB	0 MB/s	0 MBit/s
Bonjour Service		0%	0,9 MB	0 MB/s	0 MBit/s
Cisco AnyConnect User Interface (32 Bit)		0%	3,7 MB	0 MB/s	0 MBit/s
Conexant High Definition Audio Filter Agent		0%	0,8 MB	0 MB/s	0 MBit/s
Device Association Framework Provider Host		0%	0,7 MB	0 MB/s	0 MBit/s
Host Process for Microsoft Configuration Manager		0%	11,7 MB	0 MB/s	0 MBit/s
Weniger Details					
Task beenden					





Task-Manager				
Datei Optionen Ansicht				
Prozesse Leistung App-Verlauf Autostart Benutzer Details Dienste				
Name	Herausgeber	Status	Startauswirkun...	
 AcroTray	Adobe Systems Inc.	Aktiviert	Mittel	
 Adobe CS6 Service Manager	Adobe Systems Incorpor...	Aktiviert	Mittel	
▶  Adobe Reader and Acrobat ...	Adobe Systems Incorpor...	Aktiviert	Mittel	
▶  Adobe Updater Startup Utilit...	Adobe Systems Incorpor...	Aktiviert	Hoch	
 APSDaemon		Aktiviert	Nicht gemessen	
▶  Cisco AnyConnect User Inte...	Cisco Systems, Inc.	Aktiviert	Mittel	
 Conexant High Definition A...	Conexant Systems, Inc.	Aktiviert	Mittel	
 Greenshot	Greenshot	Deaktiviert	Keiner	
 iTunesHelper	Apple Inc.	Aktiviert	Mittel	
 KeePass	Dominik Reichl	Aktiviert	Hoch	
 Microsoft Outlook	Microsoft Corporation	Aktiviert	Hoch	
 Pidgin	The Pidgin developer co...	Aktiviert	Hoch	
 Remotedesktopverbindung	Microsoft Corporation	Aktiviert	Hoch	
 Send to OneNote Tool	Microsoft Corporation	Aktiviert	Mittel	
 Skype for Business	Microsoft Corporation	Deaktiviert	Keiner	
▶  SmartAudio CPL (32bit) (8)	Conexant Systems, Inc.	Aktiviert	Hoch	
▶  Sony PC Companion (2)	Sony	Aktiviert	Hoch	
▶  Sophos Endpoint Security a...	Sophos Limited	Aktiviert	Mittel	
 SwitchBoard Server (32 bit)	Adobe Systems Incorpor...	Aktiviert	Mittel	
 ucfgTexmaker.exe		Aktiviert	Niedrig	
<div>  Weniger Details <div>Deaktivieren</div> </div>				

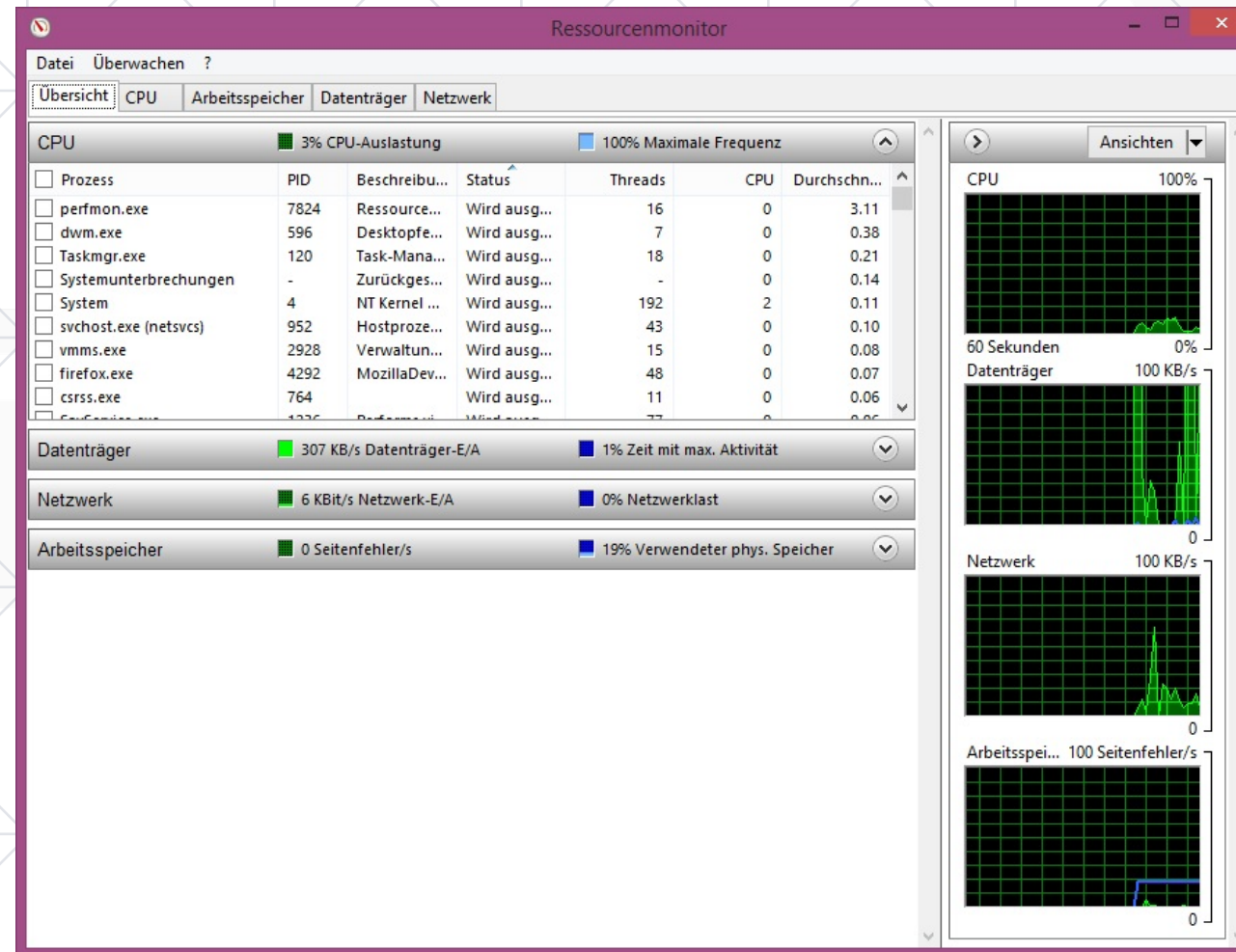
Task-Manager						
Datei Optionen Ansicht						
Prozesse Leistung App-Verlauf Autostart Benutzer Details Dienste						
Benutzer		Status	4% CPU	19% Arbeitss...	0% Datenträ...	0% Netzwerk
User1 (24)			4,0%	836,6 MB	0,1 MB/s	0,1 MBit/s
AcroTray (32 Bit)			0%	0,9 MB	0 MB/s	0 MBit/s
AMD External Events Client...			0%	1,3 MB	0 MB/s	0 MBit/s
Cisco AnyConnect User Int...			0,1%	3,7 MB	0 MB/s	0 MBit/s
Client-Server-Laufzeitproz...			0,1%	1,2 MB	0 MB/s	0 MBit/s
Conexant High Definition ...			0%	0,8 MB	0 MB/s	0 MBit/s
Desktopfenster-Manager			0,7%	24,0 MB	0 MB/s	0 MBit/s
Host Process for Setting Sy...			0%	0,4 MB	0 MB/s	0 MBit/s
Hostprozess für Windows-...			0%	3,0 MB	0 MB/s	0 MBit/s
Microsoft Management C...			0%	16,6 MB	0 MB/s	0 MBit/s
Microsoft Outlook (32 Bit)			0%	55,5 MB	0,1 MB/s	0,1 MBit/s
MozillaDeveloperPreview (...)			0%	376,7 MB	0 MB/s	0 MBit/s
Paint			1,7%	23,5 MB	0 MB/s	0 MBit/s
Remotedesktopverbindung			0%	177,3 MB	0 MB/s	0,1 MBit/s
SCNotification (32 Bit)			0%	8,3 MB	0 MB/s	0 MBit/s
Send to OneNote Tool (32 ...)			0%	0,4 MB	0 MB/s	0 MBit/s
Sink to receive asynchrono...			0%	1,0 MB	0 MB/s	0 MBit/s
SmartAudio (32 Bit)			0%	33,0 MB	0 MB/s	0 MBit/s
Sophos Endpoint Security ...			0%	0,3 MB	0 MB/s	0 MBit/s
Task-Manager			1,1%	15,4 MB	0 MB/s	0 MBit/s
TortoiseSVN status cache			0%	1,8 MB	0 MB/s	0 MBit/s
USBDM helper applicatio...			0%	0,1 MB	0 MB/s	0 MBit/s
Virtual Machine Connection			0%	17,8 MB	0 MB/s	0 MBit/s
Windows-Anmeldeanwen...			0%	0,8 MB	0 MB/s	0 MBit/s
Windows-Explorer			0,4%	73,0 MB	0 MB/s	0 MBit/s
Weniger Details						
						Trennen

Task-Manager						
Datei Optionen Ansicht						
Prozesse	Leistung	App-Verlauf	Autostart	Benutzer	Details	Dienste
Name	PID	Status	Benutzerna...	CPU	Arbeitsspei...	Beschreibung
acrotray.exe	5516	Wird ausgeführt	User1	00	916 K	AcroTray
ALMon.exe	5672	Wird ausgeführt	User1	00	348 K	Sophos Endpoint Security and Control
ALsvc.exe	2436	Wird ausgeführt		00	756 K	ALsvc
AppleMobileDeviceS...	2036	Wird ausgeführt		00	2.072 K	AppleMobileDeviceService
armsvc.exe	1996	Wird ausgeführt		00	692 K	Armsvc
atieclxx.exe	4172	Wird ausgeführt		00	1.304 K	Atieclxx
atiesnox.exe	628	Wird ausgeführt		00	480 K	Atiesnox
BingDesktopUpdater...	1256	Wird ausgeführt		00	1.604 K	BingDesktopUpdater
CAudioFilterAgent64...	5236	Wird ausgeführt	User1	00	844 K	Conexant High Definition Audio Filter Agent
CcmExec.exe	4556	Wird ausgeführt		00	12.020 K	CcmExec
csrss.exe	612	Wird ausgeführt		00	1.372 K	Csrss
csrss.exe	764	Wird ausgeführt		00	1.240 K	Csrss
dasHost.exe	3568	Wird ausgeführt		00	752 K	DasHost
dwm.exe	596	Wird ausgeführt	User1	00	24.696 K	Dwm
explorer.exe	1872	Wird ausgeführt	User1	00	74.880 K	Windows-Explorer
firefox.exe	4292	Wird ausgeführt		00	385.120 K	MozillaDeveloperPreview
iPodService.exe	5552	Wird ausgeführt		00	1.436 K	iPodService
Leerlaufprozess	0	Wird ausgeführt	SYSTEM	97	4 K	Zeit in Prozent, die der Prozessor im Leerlauf ist
lsass.exe	816	Wird ausgeführt		00	9.096 K	Lsass
ManagementAgent...	2344	Wird ausgeführt		00	2.584 K	ManagementAgentNT
mDNSResponder.exe	1636	Wird ausgeführt		00	892 K	MDNSResponder
mmc.exe	5188	Wird ausgeführt	User1	00	17.320 K	Microsoft Management Console
mspaint.exe	6508	Wird ausgeführt	User1	00	32.944 K	Paint
mstsc.exe	5500	Wird ausgeführt	User1	00	181.572 K	Remotedesktopverbindung
ONENOTEM.EXE	5396	Wird ausgeführt	User1	00	376 K	Send to OneNote Tool
OUTLOOK.EXE	5468	Wird ausgeführt	User1	00	56.528 K	Microsoft Outlook
PresentationFontCac...	6280	Wird ausgeführt		00	5.644 K	PresentationFontCache
RouterNT.exe	2468	Wird ausgeführt		00	2.204 K	RouterNT
SASrv.exe	2204	Wird ausgeführt		00	768 K	SASrv
SAVAdminService.exe	2240	Wird ausgeführt		00	1.096 K	SAVAdminService
SavService.exe	1236	Wird ausgeführt		00	193.468 K	SavService
SCNotification.exe	2568	Wird ausgeführt	User1	00	8.528 K	SCNotification
SearchIndexer.exe	4724	Wird ausgeführt		00	25.688 K	SearchIndexer
services.exe	808	Wird ausgeführt		00	4.248 K	Services

Weniger Details
Task beenden

Task-Manager				
Datei Optionen Ansicht				
Prozesse	Leistung	App-Verlauf	Autostart	Benutzer
Details	Dienste			
Name	PID	Beschreibung	Status	Gruppe
AdobeARMservice	1996	Adobe Acrobat Update Service	Wird ausgeführt	netsvcs
AdobeFlashPlayerUpdateSvc		Adobe Flash Player Update Service	Beendet	
AeLookupSvc		Anwendungserfahrung	Beendet	
ALG		Gatewaydienst auf Anwendungsebene	Beendet	LocalServiceN...
AMD External Events Utility	628	AMD External Events Utility	Wird ausgeführt	
AppIDSvc		Anwendungsidentität	Beendet	
Appinfo		Anwendungsinformationen	Beendet	netsvcs
Apple Mobile Device Service	2036	Apple Mobile Device Service	Wird ausgeführt	
AppMgmt		Anwendungsverwaltung	Beendet	
AppReadiness		App-Vorbereitung	Beendet	AppReadiness
AppXSvc		AppX-Bereitstellungsdienst (AppXSVC)	Beendet	
AudioEndpointBuilder	1104	Windows-Audio-Endpunkterstellung	Wird ausgeführt	
Audiosrv	860	Windows-Audio	Wird ausgeführt	LocalServiceN...
AxInstSV		ActiveX-Installer (AxInstSV)	Beendet	
BDESVC		BitLocker-Laufwerkverschlüsselungsdienst	Beendet	
BFE	1816	Basisfiltermodul	Wird ausgeführt	LocalServiceN...
BingDesktopUpdate	1256	Bing Desktop Update service	Wird ausgeführt	
BITS	952	Intelligenter Hintergrundübertragungsdienst	Wird ausgeführt	
Bonjour Service	1636	Bonjour Service	Wird ausgeführt	DcomLaunch
BrokerInfrastructure	940	Infrastrukturdienst für Hintergrundaufgaben	Wird ausgeführt	
Browser	952	Computerbrowser	Wird ausgeführt	
BthHFSrv		Bluetooth-Freisprechdienst	Beendet	LocalServiceA...
bthserv		Bluetooth-Unterstützungsdienst	Beendet	
CcmExec	4556	SMS-Agent-Host	Wird ausgeführt	
ccmsetup		ccmsetup	Beendet	netsvcs
CertPropSvc	952	Zertifikatverteilung	Wird ausgeführt	
CmRcService		Configuration Manager-Remotesteuerung	Beendet	
COMSysApp		COM+ -Systemanwendung	Beendet	NetworkService
CryptSvc	1564	Kryptografiedienste	Wird ausgeführt	
CscService		Offlinedateien	Beendet	
DcomLaunch	940	DCOM-Server-Prozessstart	Wird ausgeführt	DcomLaunch
defragsvc		Laufwerke optimieren	Beendet	
DeviceAssociationService	1104	Gerätezuordnungsdienst	Wird ausgeführt	
DeviceInstall		Geräteinstallationsdienst	Beendet	DcomLaunch

Ressourcen-Monitor

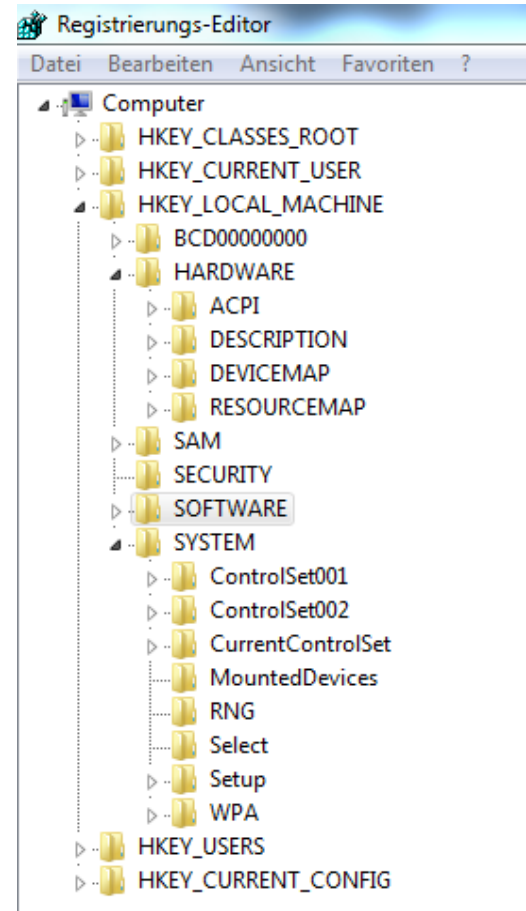


Die Registry – eine Datenbank

- Zentrale Datenbank für Informationen über Hardware und Software
- Baumstruktur
- **Vorsicht:** Änderungen können weitreichende Folgen haben und sind (oft) nicht notwendig!

Die Registry

- 5 Hauptschlüssel
 - HKEY_Classes_Root
 - HKEY_Current_User
 - HKEY_Local_Machine
 - HKEY_Users
 - HKEY_Current_Config



Name	Typ	Daten
(Standard)	REG_SZ	
test	REG_SZ	asdfas

Die Registry

- **HKEY_Local_Machine**

Informationen über lokales System

- › Hardware – Treiber, wird zur Laufzeit erzeugt und im Speicher gehalten
- › SAM (Security Account Manager) – Benutzernamen, Gruppen, Passwörter
- › Security – Sicherheitsrichtlinien
- › Software – Konfigurationen für Programme

- **HKEY_Users**

- Benutzerspezifische Informationen
- Profile aller Benutzer

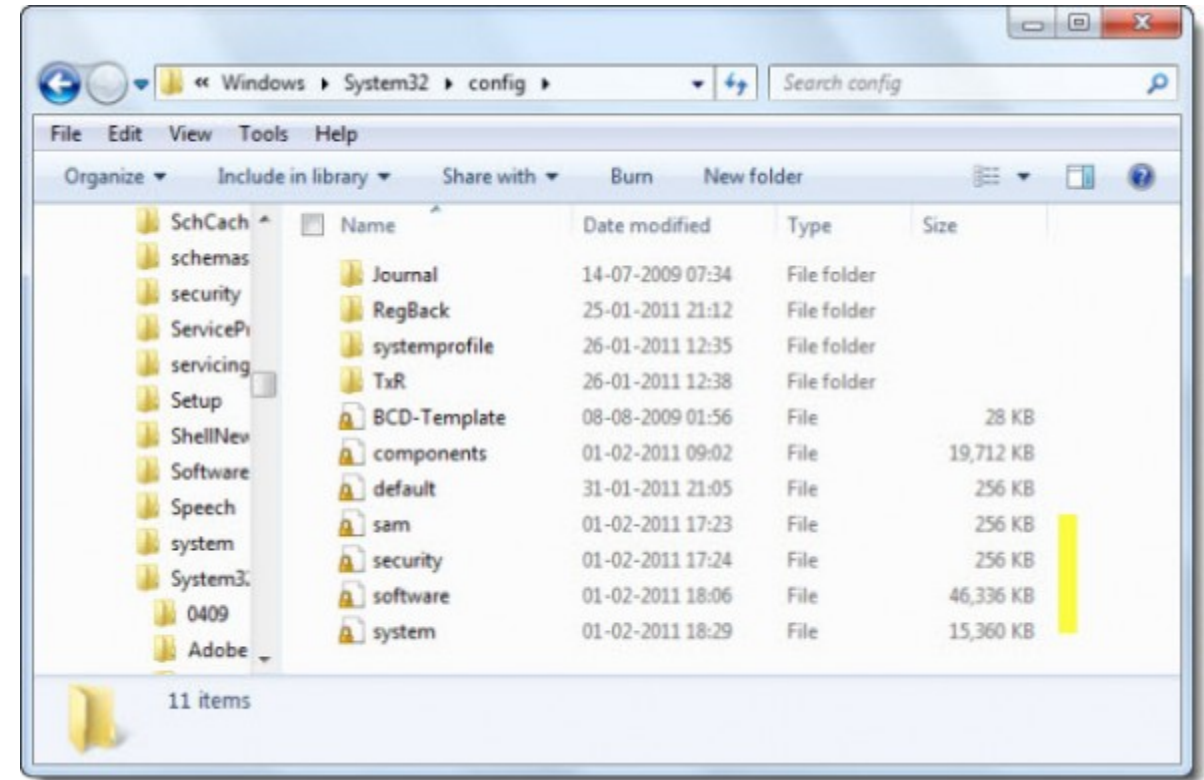
Die Registry

- HKEY_Classes_Root
 - Link auf HKLM\Software\Classes
 - Zuordnung Dateitypen ↔ Anwendung
- HKEY_Current_User
 - Link zu aktuellem Benutzerprofil von HKEY_Users\Benutzerprofil
- HKEY_Current_Config
 - Einstellungen des aktuellen Hardwareprofils
 - Kopie des Schlüssels HKLM\System\Current Control Set\Hardware Profiles\Current

Die Registry

Wo ist die Registry physikalisch gespeichert ?

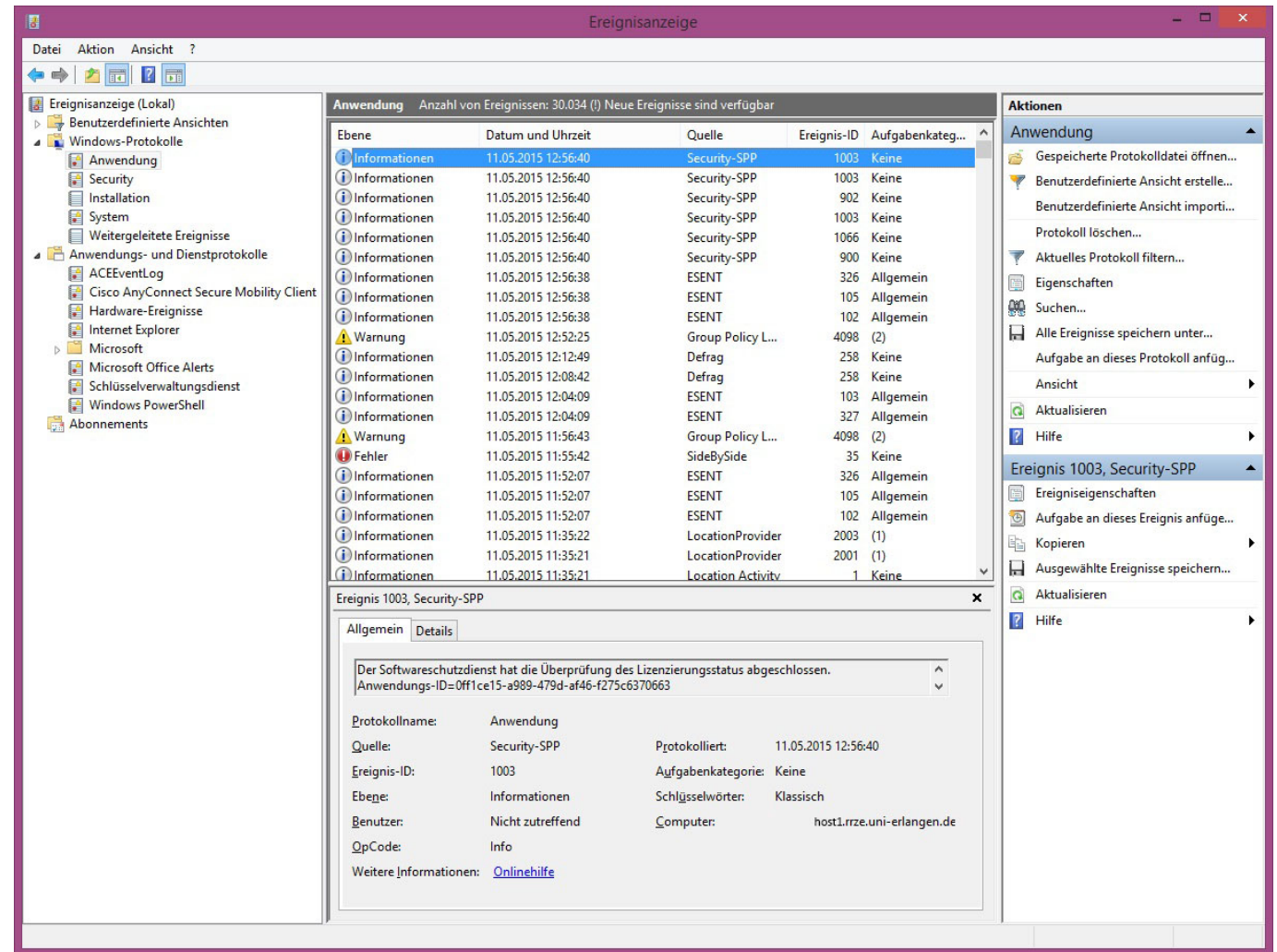
- C:\Windows\System32\config
- Wird beim Herunterfahren des Systems geschrieben
- Infos eines Benutzer: NTUSER.DAT im „Home“



Quelle: <http://www.thewindowsclub.com/where-are-the-windows-registry-files-located-in-windows-7>

Fehlersuche – Hilfe zur Selbsthilfe

- Windows-Event-Log
 - Anwendung
 - Security
 - Installation
 - System
- Programmspezifische Logs



Fehlersuche – Hilfe zur Selbsthilfe

- Festplatte voll?
- Stehen Updates aus?
- Ein Reboot tut immer gut 😊
- Rechner herunterfahren wenn nicht gebraucht
- Problem schon mal im Internet gesucht?
 - Der „Google-Admin“ weiß (fast) alles 😊
 - Gibt es einen Patch vom Hersteller?

Fehlersuche – Hilfe zur Selbsthilfe

- Bevor ich mich beim Support/Admin melde

Informationen sammeln:

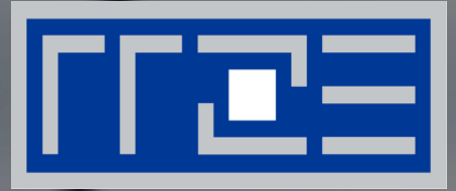
- **Hostname** (cmd: hostname)
- **IP-Adresse** (cmd: ipconfig)
- **Betriebssystemversion**

3 W-Fragen 😊

- **Was ist das Problem?**
- **Seit wann tritt es auf?**
- **Was hat das Problem verursacht?**



ORGANISATORISCHES



- Die Vorträge im Überblick
- Andere Vortragsreihen des RRZE
- Ablageorte Vortragsfolien
- RRZE-Veranstaltungskalender / Mailingliste abonnieren
- Themenvorschläge & Anregungen

Weitere Vorträge zur „Systemausbildung“

20.04.2016 – Geschichte der Betriebssysteme

27.04.2016 – Unixoiden Betriebssysteme (Unix, Linux, OS X)

04.05.2016 – Benutzerverwaltung: LDAP

11.05.2016 – Windows-Betriebssysteme

01.06.2016 – Benutzerverwaltung: MS Active Directory

08.06.2016 – Storage / Filesysteme

15.06.2016 – Virtualisierung

22.06.2016 – Backup / Archiv

29.06.2016 – Systemüberwachung, Monitoring

06.07.2016 – High Performance Computing

13.07.2016 – IT-Sicherheit

Immer mittwochs
(ab 14 c.t.),
Raum 2.049 im
RRZE

Andere Vortragsreihen des RRZE

Campustreffen

- immer donnerstags ab 15 Uhr c.t.
- vermittelt Informationen zu den Dienstleistungen des RRZE
- befasst sich mit neuer Hard- & Software, Update-Verfahren sowie Lizenzfragen
- ermöglicht den Erfahrungsaustausch mit Spezialisten

Netzwerkausbildung „Praxis der Datenkommunikation“

- immer mittwochs in den Wintersemestern, ab 14 Uhr c.t.
- Vorlesungsreihe, die in die Grundlagen der Netztechnik einführt
- stellt die zahlreichen aktuellen Entwicklungen auf dem Gebiet der (universitären) Kommunikationssysteme dar

Vortragsfolien

Die Vortragsfolien werden nach der Veranstaltung auf der Webseite des RRZE abgelegt:

<http://www.rrze.fau.de/news/systemausbildung.shtml>

RRZE-Veranstaltungskalender & Mailinglisten

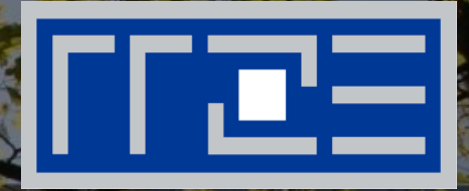
- Kalender abonnieren oder bookmarken
 - Alle Infos hierzu stehen auf der Webseite des RRZE unter:
<http://www.rrze.fau.de/news/kalender.shtml>
- Mailingliste abonnieren
 - Wöchentliche Terminhinweise werden zusätzlich an die Mailingliste [RRZE-Aktuelles](#) gesendet.
 - Auch diese Liste kann man abonnieren:
<https://lists.fau.de/mailman/listinfo/rrze-aktuelles>

Themenvorschläge & Anregungen

Themenvorschläge und Anregungen nehmen wir gerne entgegen!

Bitte schreiben Sie uns einfach eine E-Mail an:
rrze-zentrale@fau.de (Betreff: Systemausbildung)

REGIONALES RECHENZENTRUM ERLANGEN [RRZE]



Vielen Dank für Ihre Aufmerksamkeit!

Regionales RechenZentrum Erlangen [RRZE]

Martensstraße 1, 91058 Erlangen

<http://www.rrze.fau.de>