

GNU/Linux/Ubuntu im sicheren und virtuellen Netz



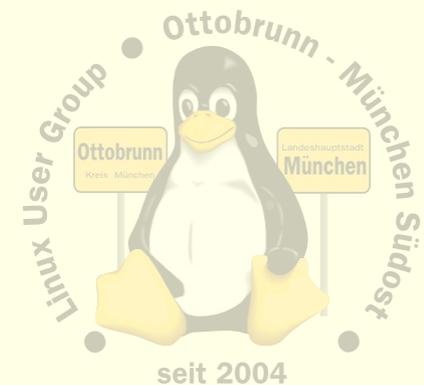
GNU/Linux/Ubuntu im sicheren Netz



über mich

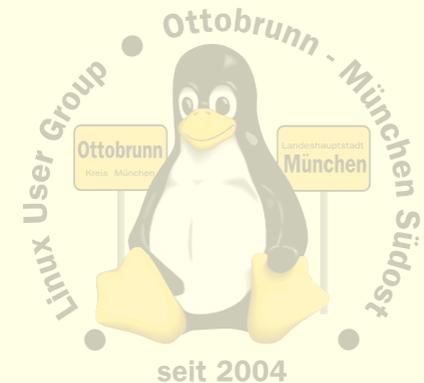
- **Richard Albrecht, Jahrgang 49**
 - Physiker / Uni Halle-Wittenberg
 - Fernstudium Theologie (in der DDR)
 - 1988 - 2000 am MPI für Biochemie Martinsried
 - 3-D Licht-Mikroskopie in der Zellbiologie
 - Bildverarbeitung, C Entwicklung
 - Bis 2011: Middleware, Datenbanken, .NET, Webanwendungen
 - jetzt: Migrationen, Vorträge, Linuextage

- **Ubuntu 10.10, 64 bit, 8 GB RAM (für KVM)**
- **HP 625, 8GB, Demo PC**
- **Migration von PCs, privat und kleine Firmen**
 - **kein** Virens Scanner, **keine** Firewall, **keine** Viren, **keine** Trojaner
 - Installation wird von mir vorbereitet
 - einen Abend Einweisung
 - weitere Wartung durch Benutzer
 - 'Altlasten' umlagern nach Windows 7 mit KVM
 - bisher ältestes Ubuntu-System läuft seit 2005 (Breezy Badger)
 - heute 10.04, und 3 mal Hardware komplett getauscht



Themen

- **Warum GNU/Linux/Ubuntu?**
 - 'to go the Ubuntu Way'
 - Sicherheit
 - Unabhängigkeit
- **gemeinsame Rechnerwelt für die ganze Familie**
 - sicheres privates Netz in unsicheren Zeiten
 - Einsatz von SSH zum Aufbau eines sicheren Netzes unter Freunden
 - sicherer Zugriff über das unsichere Internet auf den PC zu Hause mit X2GO
 - Ressourcen bleiben zu Hause und sind von überall erreichbar
- **Virtualisierung für alle mit Linux 'out of the box'**
 - Was ist Virtualisierung?
 - Warum brauchen wir virtuelle PCs?
 - 'Altlasten', Linux Varianten testen, Mini-Server, uvam.
 - Installation und Betrieb mit einfachsten Linux Werkzeugen (KVM)



Paradigmenwechsel

- **PC ist zur Privatsphäre geworden**

- private Sicherheit der Daten wird immer wichtiger
- Bundesverfassungsgericht in DE, 27. Februar 2008
 - „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“
- Bericht CCC, 8.10.2011
 - Bundestrojaner entdeckt, Kollateralschaden der Computersicherheit

- **Linux hat sich in den letzten 10 Jahren sehr gewandelt**

- 40 Jahre Erfahrung (durch Unix)
- vom Uni-System zum ausgereiften Desktop
- hohe Sicherheit für den Desktopbenutzer
- in allen Sprachen verfügbar
- sehr gute Hardwareunterstützung
- sehr einheitlich, trotz der Vielfalt

debian

ubuntu
linux for human beings

xubuntu

mythbuntu
home entertainment just got entertaining again.



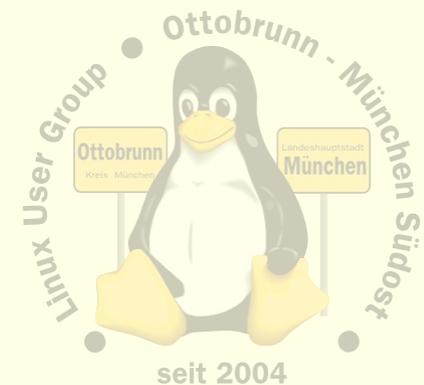
Paradigmenwechsel

- **KISS – 'Keep It Simple, Stupid'**
 - Ockhams Rasiermesser
 - möglichst einfache, minimalistische und leicht verständliche Lösung
 - optimale Systeme
 - z.B. Internet, Linux,
 - Eric Raymond <http://www.catb.org/~esr/>
 - The Art of Unix Programming
 - The Art of Unix Usability
 - the Cathedral and the Bazaar
- ... let's go to GNU/Linux/Ubuntu



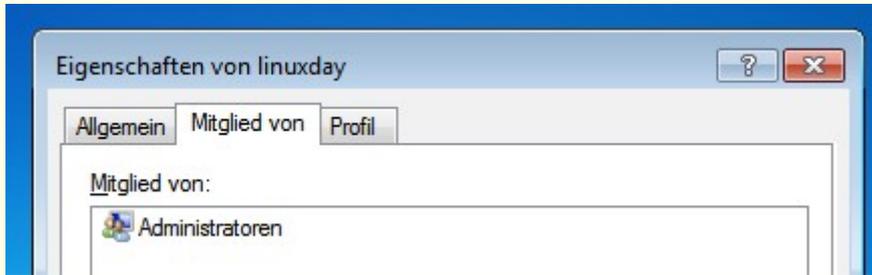
Warum Ubuntu?

- **keine** Fremdbestimmung durch Herstellerfirma oder deren Marketing
- **gleiches** System auf dem Netbook, Notebook, Desktop, Server
- **kein** Unterschied Home, Professional, Ultimate, Enterprise ...
- **hohe** lokale Sicherheit, kein Virens Scanner, keine Firewall nötig
- **sicherer** Zugang zu Software und Updates aller Komponenten
- **keine** Lizenzprobleme
- **saubere** Rechtstrennung
 - Windows: default User ist Admin
 - „It's like giving terrorists high-level government positions“.
(Katherine Noyes, PCWorld)
- **und**
Sie haben als kleiner Anwender eine Chance gegenüber der Übermacht großer Unternehmen.



Default Sicherheit, Beispiele aus Win7 und Ubuntu (unvollständig)

- 1. Benutzer nach Installation ist Admin (kein Hinweis)

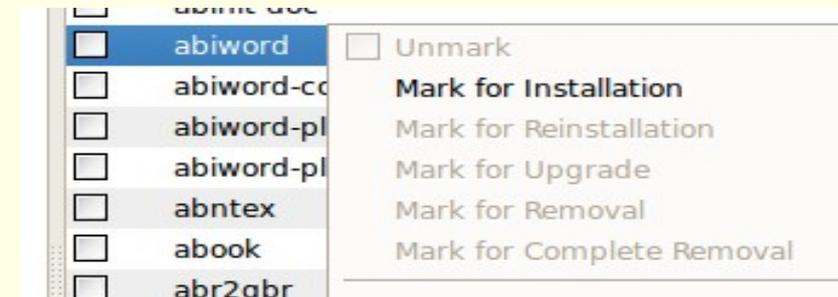
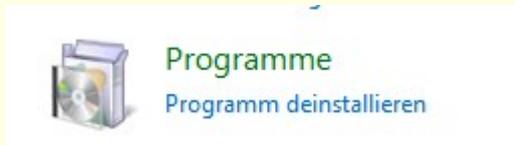


- kein SSH im Angebot, aber unsicheres Telnet

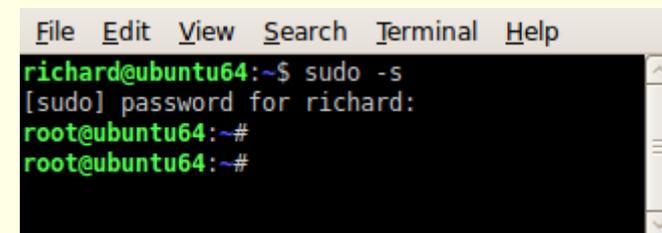
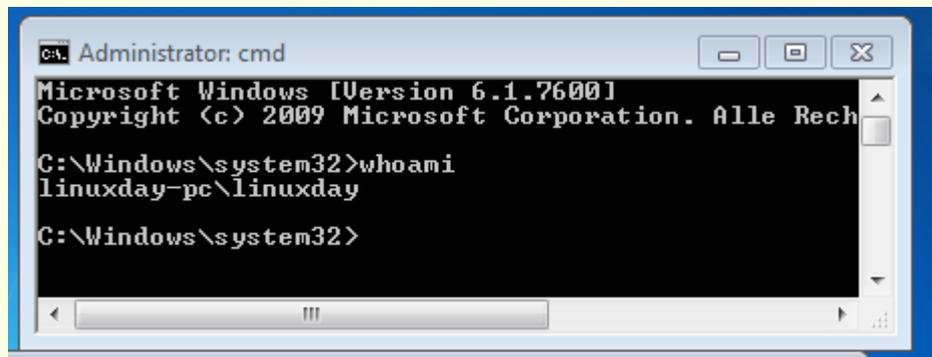


- Programme
- nur deinstallieren, nicht installieren

- In **Ubuntu** installieren und deinstallieren

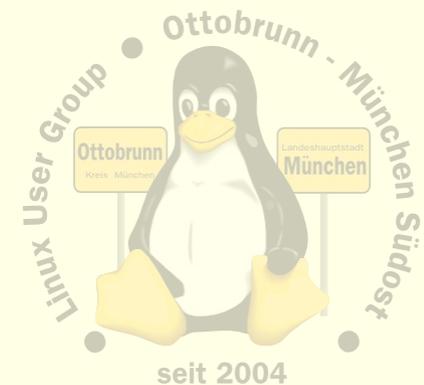


Admin Konsolen: Win7, **Ubuntu**



Warum Ubuntu?

- **Cyberwar**
 - Unsicherheit hat politische Folgen
 - Cyberabwehrzentrum (<http://neusprech.org/cyber-abwehrzentrum/>)
 - ...
 - stell Dir vor, es ist Cyberwar und wir gehen nicht hin
 - that's Ubuntu ...
- **Ökologie,**
 - weil es nicht immer der neueste Rechner sein muss
- **Filmhinweis:**
 - 'Kaufen für die Müllhalde', ARTE Mediathek
 - „ein Artikel, der nicht verschleißt, ist eine Tragödie fürs Geschäft“
 - Zitat von Printers Ink, New York, **1928** (aus dem Film)
 - Geplante Obsoleszenz <http://de.wikipedia.org/wiki/Obsoleszenz>
 - Drucker, Software, Hardware → **künstlich** 'alt' gemacht?



Warum Ubuntu?

- und, da fehlt noch etwas?
 - herkömmlicher PC ist Ursache für Bluthochdruck ;-)
 - Immer geht irgendetwas nicht :-)
 - bin ich heute schon überfallen worden?

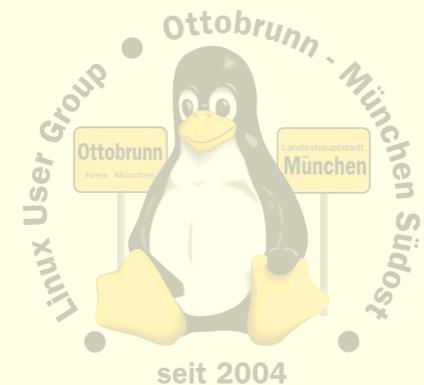
 - Ubuntu senkt den Blutdruck :-)
 - Ubuntu verbessert die Gesundheit
 - wir brauchen Ubuntu, um zu leben
 - ... denn Ubuntu ist stressfrei



Unsicherheit und eine verblüffende Lösung

- O-Ton MS (Übersetzung bei Heise)
 - „Um die wachsenden Probleme mit Botnetzen unter Kontrolle zu bekommen, sollen infizierte PCs vom Internet isoliert werden. „
 - Microsofts Vizepräsident für Trustworthy Computing, Scott Charney
 - <http://go.microsoft.com/?linkid=9746317>
 - Quelle: Heise online, 8.10.2010
-

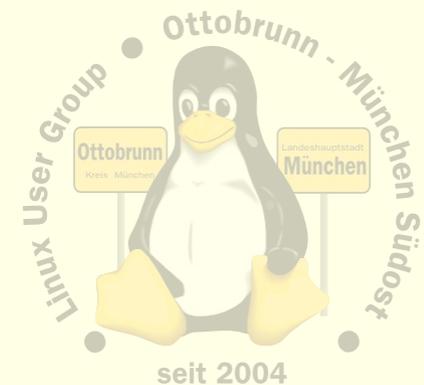
- **Configuring a Windows PC For a Senior Citizen**
 - mit Google nach diesen Worten suchen
 - <http://tech.slashdot.org/story/08/12/24/0138213/Configuring-a-Windows-PC-For-a-Senior-Citizen>
 - Ergebnis der langen Diskussion (823 Comments): **nimm Ubuntu**



erste Schritte mit Ubuntu, Motto: to go the Ubuntu Way

“I cannot teach anybody anything, I can only make them think.”, Socrates

- **einfach nur benutzen**
 - es geht alles wie von selbst
- **täglich damit arbeiten**
 - dem '**allwissenden PC-Guru**' kündigen (*Nachbar, PC-Freak, 'guter Freund'...*)
 - nie jemanden an den Linux-PC lassen, der sich '**mit PCs auskennt**'
 - Ubuntu ist nicht wie der bisherige PC
 - Erfahrungen aus der bisherigen PC Welt sind wertlos
 - Vorsicht! Sie können '**Freunde**' verlieren (**auch den Job, eigene Erfahrung**)
 - sich auf GNU/Linux/Ubuntu einlassen und **selbst** lernen
 - Wikis lesen (z.B. ubuntuusers.de)
 - Community kennenlernen (LUG vor Ort, Linuxtage)
- **und mit dem Terminal anfreunden**
 - es ist sehr effizient und hilft, Linux besser zu verstehen



Vorteile für Sie

- **Lernprozess**
 - besserer Umgang mit dem Internet
 - bessere Kenntnisse im Umgang mit dem Computer
 - vom 'Klick' zum Wissen
 - keine Limits durch Lizenzen
- **Ergebnis**
 - sicherer Umgang mit Computern, weil die Hintergründe transparent werden
 - und dann mit Ihren neuen Kenntnissen mit jemandem, *'der sich mit Computern auskennt'*, reden
 - **Sie** werden staunen, was **Sie** alles im Umgang mit **Ubuntu** gelernt haben
- **Links**
 - <http://lug-ottobrunn.de>
 - <http://www.lug-ottobrunn.de/wiki/Kategorie:Linuxeinsteiger>



**THE HIGHWAY TO
FREEDOM IS NOW
OPEN FOR
EVERYONE**



it's your turn to go ...

GNU/Linux/Ubuntu im sicheren Netz

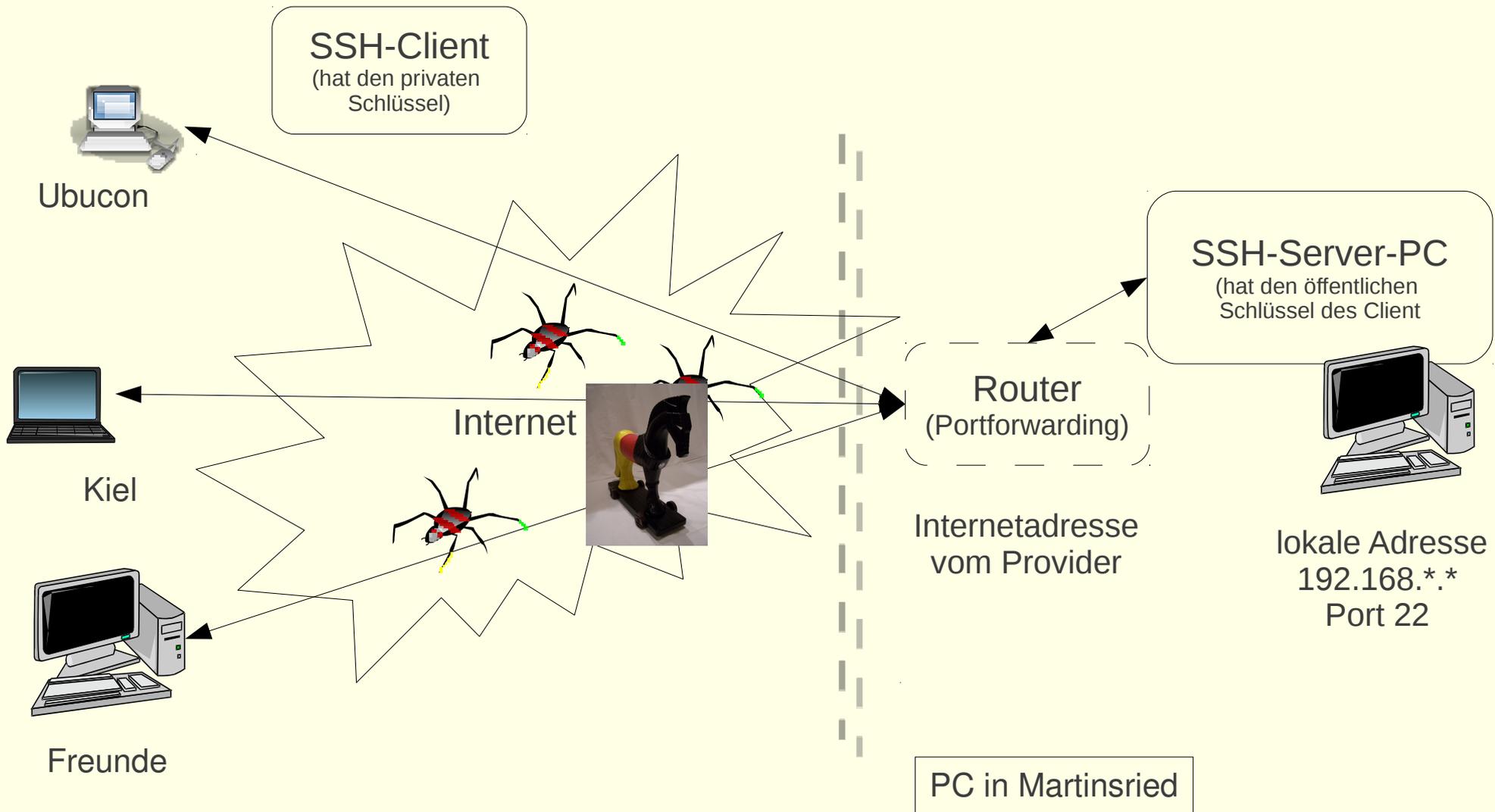


sicheres Netz für die Familie

- **Warum?**
 - Grundgesetz, s.o.
 - Überwachung des Traffic nimmt zu (z.B. De-Mail, keine vollst. Verschlüsselung)
 - 'Deep Paket Inspection' ist sehr wahrscheinlich (siehe MS Publikation)
 - Alvar Freude: Zwei Personen kontrollieren 250 Personen http://odem.org/insert_coin/
- **SSH**
 - universelle sichere Verbindung (verschlüsselt)
- **Was kann ich damit tun**
 - sichere Terminal Verbindung
 - Ausgabe von grafischen Programmen umleiten
 - Filemanager verteilt verwenden
 - mit Tunnel beliebige Programme sicher durch das Netz bringen
- **Familiennetzwerk mit SSH**
 - Netz zwischen Benutzern, die sich gegenseitig vertrauen
 - In Linux ohne Zusatzsoftware, '*out of the box*'
 - Zugriff auf den eigenen Desktop mit X2GO



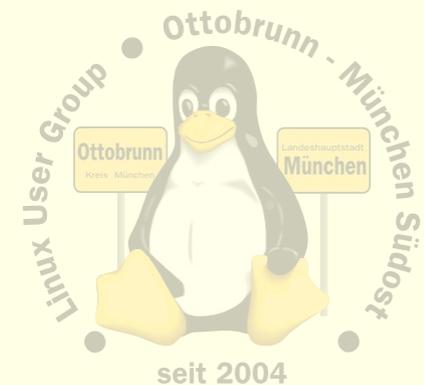
sicheres Netz in unsicheren Zeiten



<http://de.wikipedia.org/wiki/Datei:Bundestrojaner.jpg>, CC-by-sa

Voraussetzungen für die folgenden Abschnitte

- **Installieren von Programmen**
 - Synaptic, apt-get
 - Hilfesystem (man, info, Wikis)
- **Terminal**
 - öffnen, einfache Kommandos absenden
 - arbeiten als root, sudo -s
 - Editieren von Konfigurationen
- **Netzwerk**
 - Internetadressen, Namensauflösung, DynDNS
 - Dienste, Ports (in /etc/services)
 - Router, Modem
 - Rolle des Providers
 - Lieferant der Internetadresse



Remote Zugriff mit SSH, Installation

- **SSH installieren (auf allen beteiligten PCs)**

- # apt-get install **ssh**

- **Server absichern**

- **/etc/ssh/sshd_config editieren**

- Passwort-Login für alle Benutzer sperren

- steht alles in den Links unten

PermitRootLogin no

PasswordAuthentication no

- Schlüsselpaar erzeugen und sichern (\$ ssh-keygen)

- für jeden Benutzer auf dem Client

- öffentliche Schlüssel auf die Server verteilen

- Privater Schlüssel verbleibt auf dem Client

- Öffentlicher Schlüssel kommt auf den Server (~/.ssh/authorized_keys2)

- **Router freischalten**

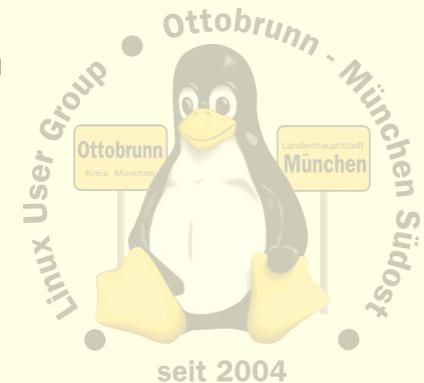
- Port 22 (bzw. der für SSH gewählte Port) muss zum Server-PC weitergeleitet werden

- Firewall im Router abschalten, bzw. den SSH Port freischalten

- **Links bei der LUG-Ottobrunn**

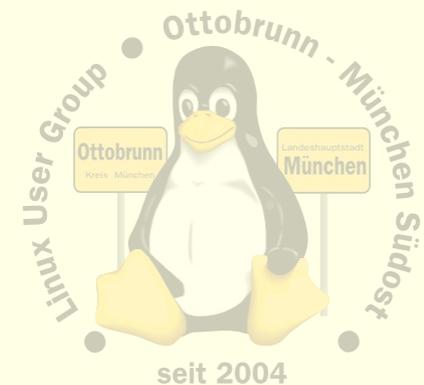
- http://www.lug-ottobrunn.de/wiki/SSH_Simple

- http://www.lug-ottobrunn.de/wiki/SSH_Spickzettel



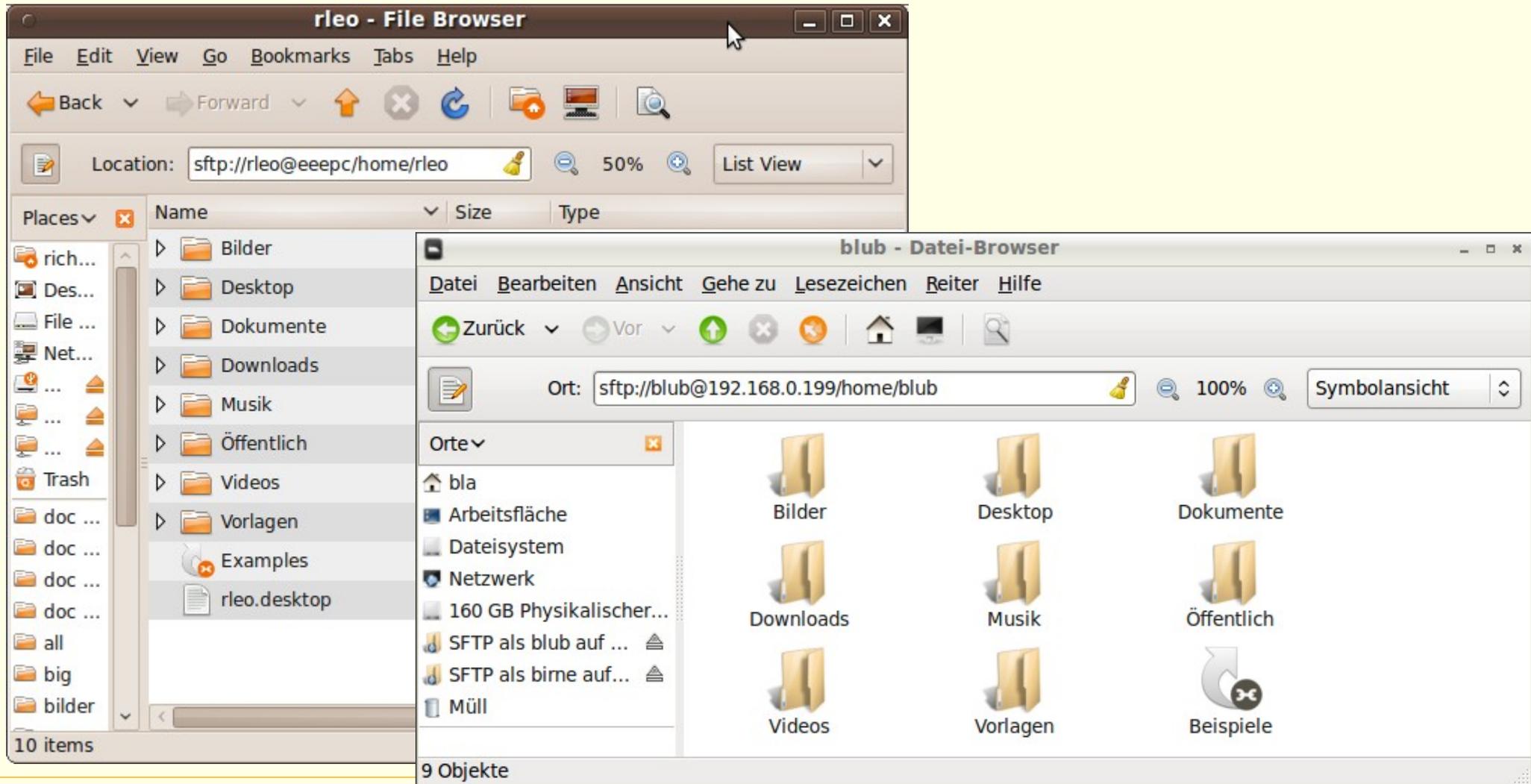
SSH-Netz

- **Client-Server Struktur**
 - jeder PC kann gleichzeitig Client und Server sein
 - Client-Benutzer hat beide Schlüssel
 - Server-Benutzer hat den öffentlichen Schlüssel des Client
- **Wer → Wohin ?**
 - Client initiiert Verbindung zu einem Benutzer auf dem Server
 - ***ssh benutzer@server_IP_Adresse***
 - Client bekommt die Rechte von '**benutzer**' auf dem Server
 - d.h. der '**benutzer**' am Server stellt seinen Account zur Verfügung
 - Vertrauen untereinander nötig (Familie, Freunde)
 - oder sicheren Account anlegen
- **Anwendungen**
 - Terminal, Filemanager, Desktop, Tunnel



SSH Anwendungen: Filemanager Nautilus

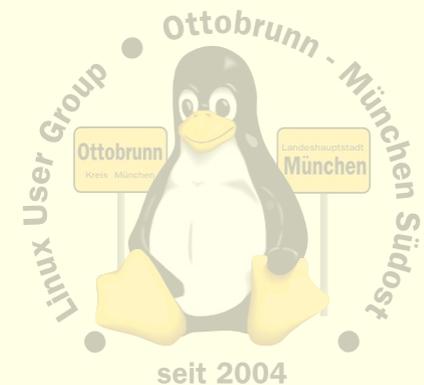
- Im Filemanager: `ssh://benutzer@IP-Adresse/home/benutzer`



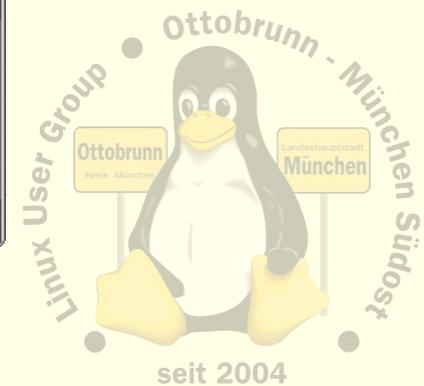
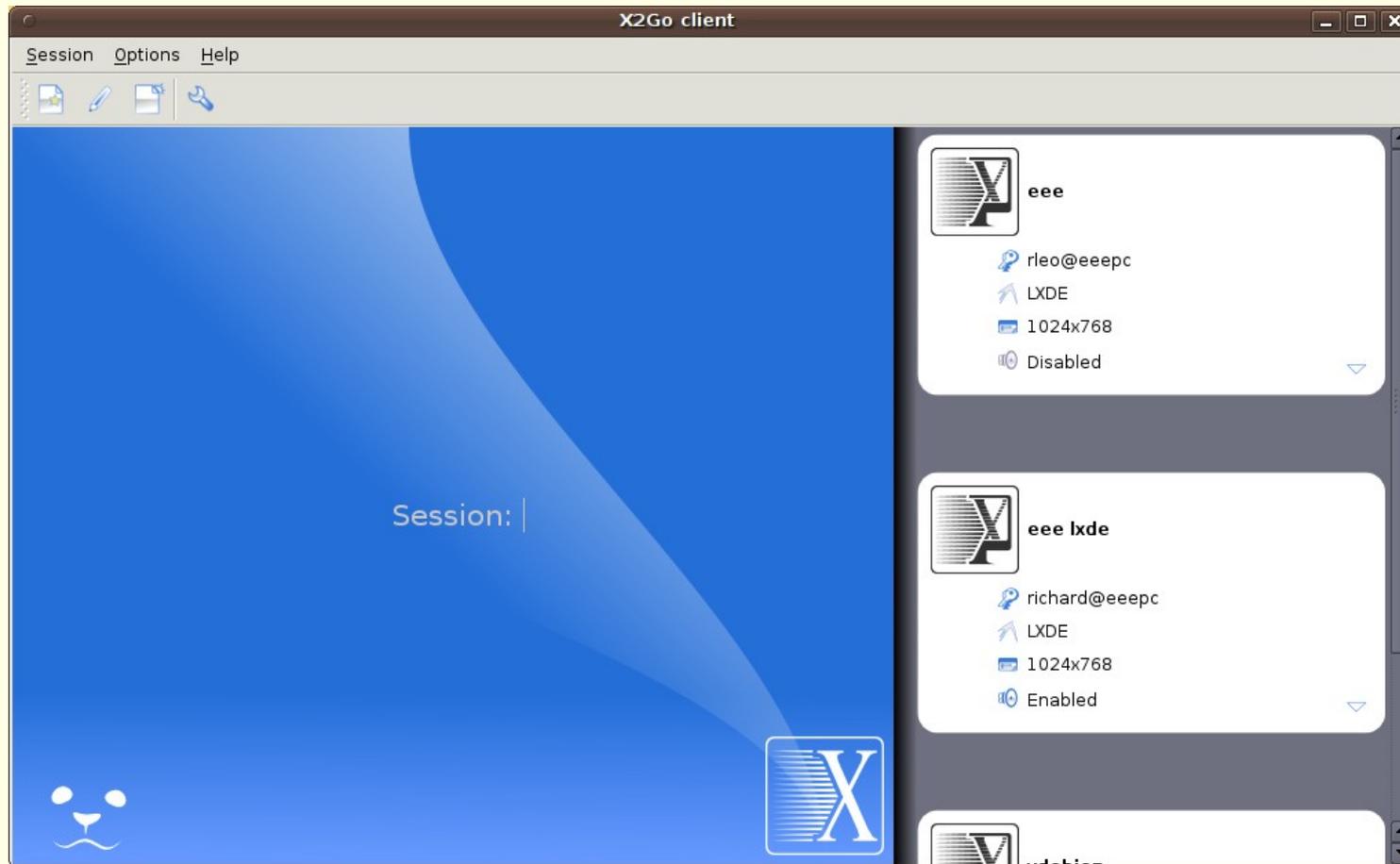
SSH Anwendungen: Remote Desktop mit X2GO

- **X2GO**
 - www.x2go.org
 - z.B. für den mobilen Einsatz
 - Server zu Hause installieren, fast keine Konfiguration
 - Repository erweitern
 - `# apt-get install x2goserver-home`
 - http://www.lug-ottobrunn.de/wiki/Remote_Desktop_mit_X2GO
 - Client auf portablen PC installieren und SSH Schlüssel konfigurieren

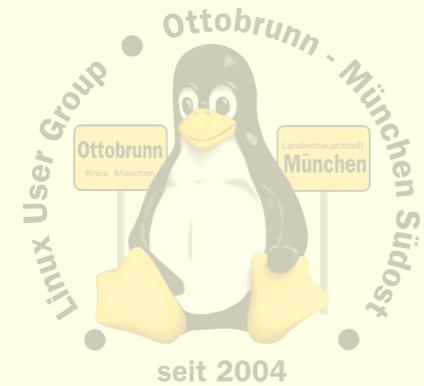
 - jetzt benötigt man nur noch ein Stück Internet, egal, wie unsicher
 - und man hat 'seinen' PC zu Hause, als wäre er vor Ort
 - Sicherheit des Traffics entsteht durch SSH
- **Vorteile**
 - eigene Session
 - Benutzer am Server muss nicht eingeloggt sein
 - ideal für unterwegs
- **Nachteil**
 - keine 'Fernsteuerung' des Desktops des Benutzers am Server



X2GO, so sieht es aus



Virtualisierung mit KVM

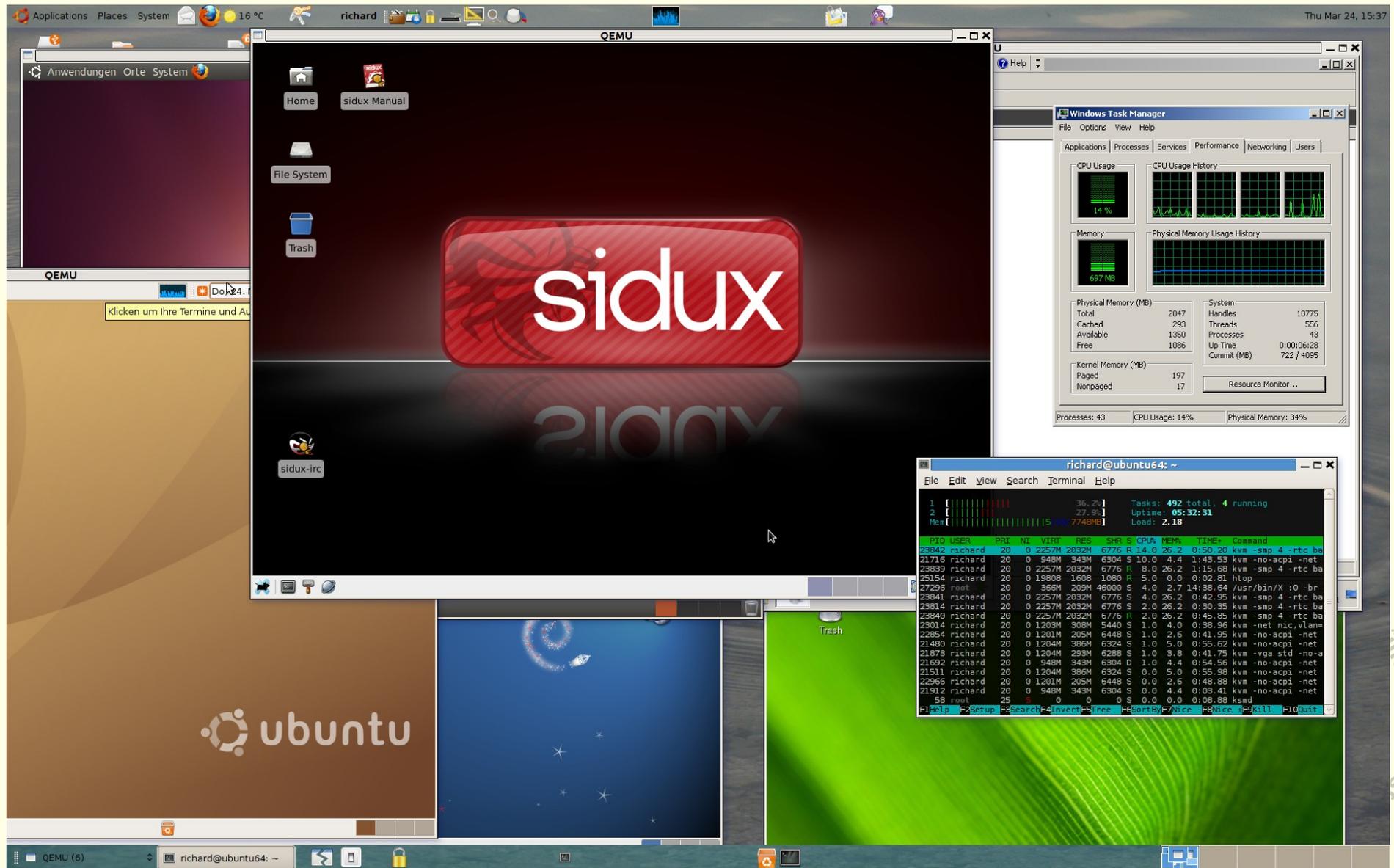


Was ist KVM ?

- **Kernel Based Virtual Machine**
 - Seit 2006 im Kernel, basiert auf QEMU, von Ubuntu favorisiert
 - KVM Buch: <http://qemu-buch.de/de/index.php/Hauptseite>
 - http://www.linux-kvm.org/page/Main_Page
 - http://www.lug-ottobrunn.de/wiki/Virtualisierung_mit_KVM
- **PC im PC**
 - alle Teile eines PC werden über Software simuliert
 - Festplatten, Maus, Netzwerk, Grafik usw.
- **Voraussetzung**
 - moderner PC, mit Virtualisierungserweiterung in der CPU
- **Performance (Beispiel aus der Praxis)**
 - **Vista**, native CPU, Intel Q9550, Quadcore, **4 GB RAM**, 32 bit
 - Laufzeit: 13m:12s
 - **XP in KVM**, nur **1 GB RAM**, 32 bit
 - Laufzeit: 12m:52s
 - **Host**: Ubuntu, 64 bit, AMD 4850e, Dualcore, **8 Gig RAM**
 - die VM ist etwas schneller als der gut ausgebaute PC



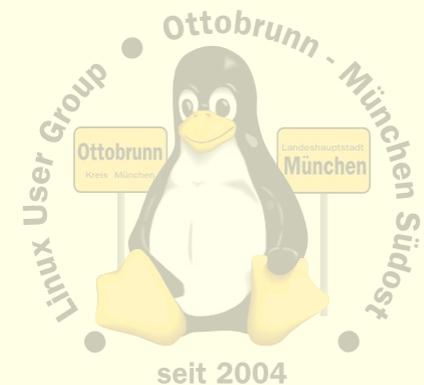
Virtualisierung mit KVM



richard@sidux

Installation von KVM unter Ubuntu

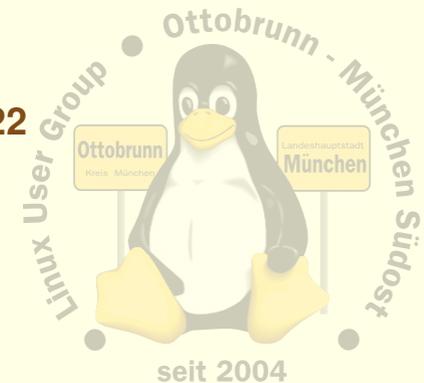
- **Siehe Webseiten von 'ubuntuusers.de' und 'ubuntu.com'**
 - <http://wiki.ubuntuusers.de/KVM>
 - <http://wiki.ubuntuusers.de/QEMU>
 - <https://help.ubuntu.com/community/KVM>
 - Install **qemu-kvm** und testen
 - `$ kvm-ok`
 - INFO: Your CPU supports KVM extensions
 - INFO: /dev/kvm exists
 - KVM acceleration can be used
 - Details auf den Webseiten
 - oder Email an mich
 - richard (punkt) albrecht (at) web (punkt) de
- **KSM Intervall erhöhen, oder abschalten**
 - 'Kernel same page merging' ist oft zu knapp eingestellt (alle 20 msec)
 - <http://www.linux-kvm.com/content/using-ksm-kernel-samepage-merging-kvm>
 - in `/etc/default/qemu-kvm`
 - `KSM_ENABLED=1`
 - `SLEEP_MILLISECS=200`



Einbinden in das lokale Netz

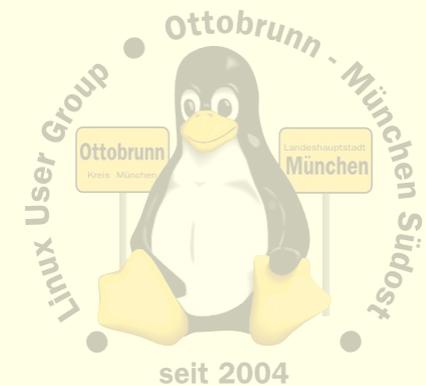
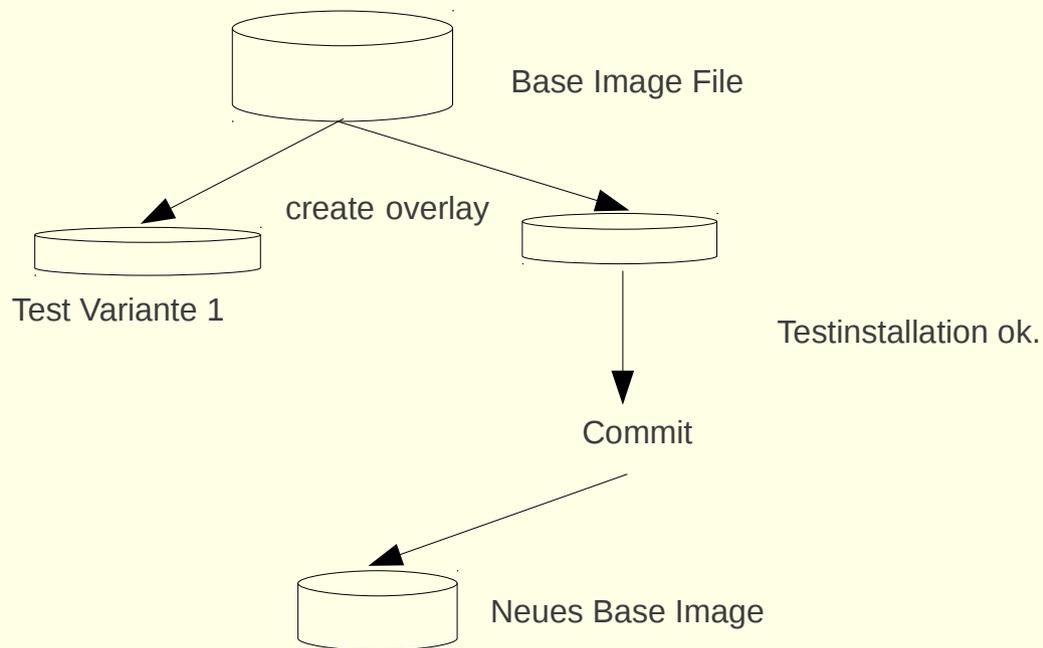
- **per default hat jede neue VM ein eigenes Netz hinter einem Router**
 - Sicherheit durch Software-Firewall im Router
 - VM kann Internet erreichen, aber nicht den Host
 - Host kann VM nicht erreichen
- **bridge utils** für Einbindung in das lokale Netz
 - <https://help.ubuntu.com/community/KVM/Networking>
 - siehe Workshop im Anschluss an diesen Vortrag
- **Demos**
 - Windows 2008 Server, im lokalen Netz zu Hause
 - Zugriff mit Remote Desktop
 - Windows kann kein SSH, Ubuntu schon
 - **ssh -L 10022:vwin2008desq1:3389 ron@meinPC.dyndns.org**
 - **rdesktop -x l -g 1100x720 -a 16 -k de -u rleofield -p passwort localhost:10022**

 - Windows 7 lokal
 - Zugriff mit Remote-Desktop

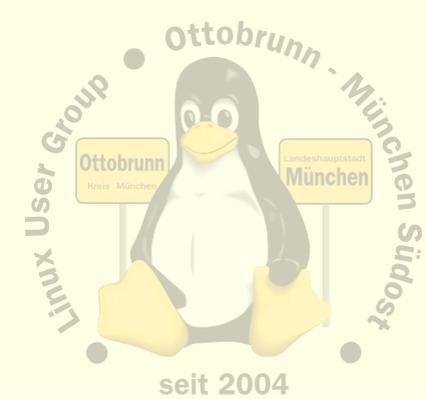
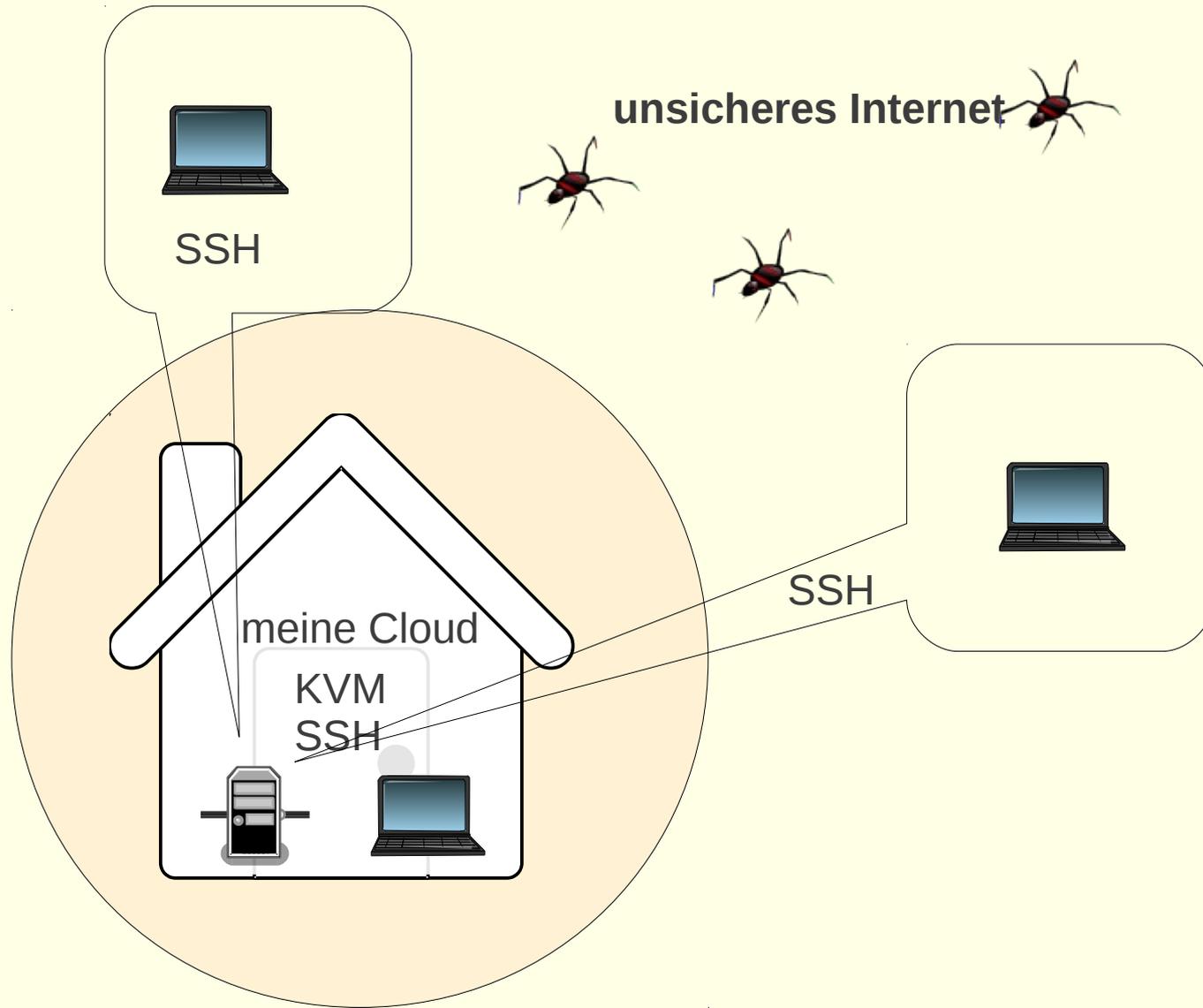


KVM Images und COW – copy on write

- **Copy On Write**
 - geänderte Blöcke werden nicht überschrieben
 - in „Overlay“ abgelegt
- **Kommandos**
 - `$ qemu-img create -b base.raw -f qcow2 overlay.ovl`
 - statt `base.img` jetzt `overlay.ovl` starten
 - `$ qemu-img commit overlay.ovl`



privates sicheres Netz Sie haben die Kontrolle



Ende des Vortrages, kein Ende mit Ubuntu ;-)

- 'to go the Ubuntu Way'
 - ist der Weg zu einem sicheren, einfachen und stabilen System
- Lernprozess
 - besserer Umgang mit dem Internet
 - bessere Kenntnisse im Umgang mit dem Computer
- Ergebnis
 - **Sie** werden staunen, was **Sie** alles im Umgang mit Ubuntu gelernt haben
- sicheres privates Netz
 - einfach, transparent, sicher
 - KISS (Ockham)
- KVM
 - alter PC lebt virtuell weiter
 - jedem sein PC, egal, wo man sich aufhält

*Vielen Dank für Ihre Aufmerksamkeit
und eine schöne Ubucon
Richard Albrecht, LUG-Ottobrunn*

