

LUG Ottobrunn - München Südost



GNU/Linux/Ubuntu im sicheren und virtuellen 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/C++ Entwicklung
- bis 2011: Middleware, Datenbanken, .NET, Webanwendungen
- jetzt: Software für CCD Kameras bei SVS-Vistek in Seefeld
- Linux ist seit 2006 Hobby Nr.1
- Vorträge, Linxutage

- **Hilfe bei der Umstellung von PCs nach Linux**

- **keine** Viren, **keine** Trojaner, **kein** Virens Scanner, **keine** Firewall
- Installation wird von mir vorbereitet
 - ein Abend Einweisung
 - weitere Wartung durch Benutzer
 - 'Altlasten' umlagern nach Windows 7 mit KVM
- www.rleofield.de

Themen

- Warum GNU/Linux/Ubuntu?
 - FSFE
 - wir lernen: 'to go the GNU/Linux/Ubuntu Way'
 - sich auf Linux einlassen
 - Sicherheit, Stabilität
 - Unabhängigkeit, freie Lizenz
- Verschlüsselung 'out of the box'
 - unkompliziert und mit Linux für alle einsetzbar
- gemeinsame Rechnerwelt für die ganze Familie
 - sicheres privates Netz in unsicheren Zeiten
 - Einsatz von SSH zum Aufbau eines sicheren Netzes unter Freunden
 - Ressourcen bleiben zu Hause und sind von überall erreichbar
- Virtualisierung für alle mit Linux
 - Was ist Virtualisierung?
 - Warum brauchen wir virtuelle PCs?
 - 'Altlasten', Linux Varianten testen, Surfstation, Mini-Server, uvam.
- Was zeige ich nicht?
 - technische Rezepte und Anleitungen, die gibt es im Netz
 - z.B. bei der LUG-Ottobrunn (<http://www.lug-ottobrunn.de>)

Ausflug in die Geschichte

- 1876 zitierte Karl Marx aus dem 'Quarterly Review' :
 - „Das Kapital hat einen Horror vor Abwesenheit von Profit ...
zehn Prozent sicher, und man kann es überall anwenden;
zwanzig Prozent, es wird lebhaft;
fünfzig Prozent, positiv waghalsig; ...“
 - <http://www.mlwerke.de>
- Übersetzung in unseren Alltag
 - hat ein Hersteller einen zu großen Marktanteil, kommt der Endkunde zu kurz
 - und das sind **Sie**
 - Qualität, Service, Datenschutz, Preis, technische Entwicklung ...

Antwort

- Bug Nr. 1 in Ubuntu

- <https://bugs.launchpad.net/ubuntu/+bug/1>
- Mark Shuttleworth, 20.08.2004

„Microsoft has a majority market share in the new desktop PC marketplace.
This is a bug, which Ubuntu is designed to fix.“

- Lösung, um sich aus dieser Abhängigkeit zu befreien

- 'to go the GNU/Linux/Ubuntu Way'
- Circle Of Friends
- Code Of Conduct (sei freundlich und helfe)
- Vielfalt der Linuxwelt (<http://distrowatch.com>)



es ist Ihre Entscheidung ■ ■ ■

Code Of Conduct

- <http://www.ubuntu.com/project/about-ubuntu/conduct>

(inoffizielle Übersetzung von ubuntuusers.de)

- Sei rücksichtsvoll
- Sei respektvoll
- Sei anderen behilflich
- Wenn wir Meinungsverschiedenheiten haben, besprechen wir sie mit anderen
- Wir bitten um Hilfe, wenn wir uns unsicher sind
- Wenn Du Dein Projekt abgibst, gib Deine Verantwortung weiter

Ubuntu ist ein Begriff aus Afrika und bedeutet:

'Menschlichkeit gegenüber Anderen'

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“
- **Sicherheit ist anders geworden**
 - Bericht CCC, FAZ 8.10.2011
 - Bundestrojaner entdeckt
 - Super GAU der Computersicherheit
 - es werden kommerziell Trojaner hergestellt
 - und man verliert die Kontrolle darüber
 - unsicher, wer macht etwas, wo passiert etwas, was hat das für Folgen, ...
 - Stuxnet
 - drohender 'Cyberwar' (in den Medien und bei Politikern)

Paradigmenwechsel

- 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 Desktop Benutzer
- in allen Sprachen verfügbar
- sehr gute Hardwareunterstützung
- sehr einheitlich, trotz der Vielfalt
- Vergleich 'Windows – Linux' nicht sinnvoll
 - es geht nicht darum, was ist besser
 - es geht um die anderen Konzepte
 - es geht um **unseren** Umgang mit dem System



Konzept

- KISS – 'Keep It Simple, Stupid'

- Ockhams Rasiermesser
- möglichst einfache, minimalistische und leicht verständliche Lösung
- optimale Systeme
- z.B. Internet, Linux
- Eric Raymond, **Unix/Linux Philosophie**
 - <http://www.catb.org/~esr/>
 - The Art of Unix Programming
 - The Art of Unix Usability
 - the Cathedral and the Bazaar

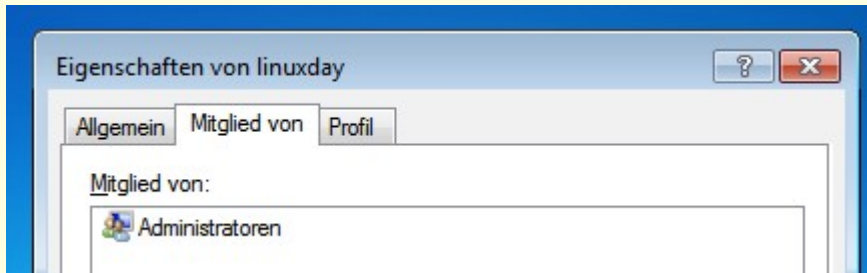
- ... starten wir, mit GNU/Linux/Ubuntu

Warum GNU/Linux/Ubuntu?

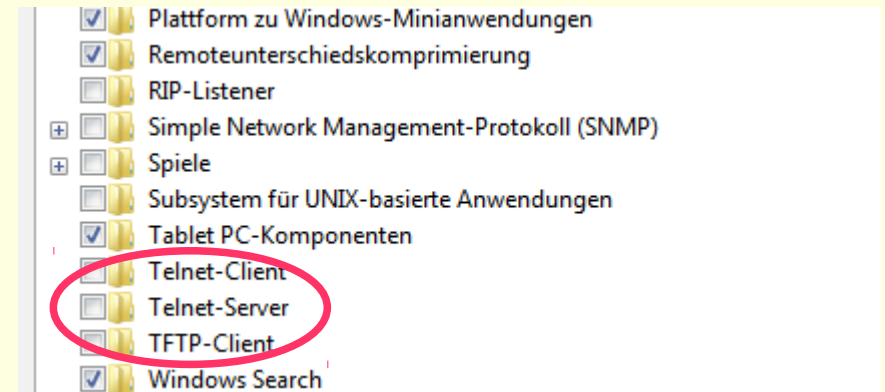
- **keine** Fremdbestimmung durch Herstellerfirma oder deren Marketing
- **gleiches** System auf dem Netbook, Notebook, Desktop, Server
- **kein** Unterschied Home, Professional, Ultimate, Enterprise ...
- **hohe** lokale Sicherheit, kein Virens Scanner, keine Firewall nötig
- **sicherer** Zugang zu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

Default Sicherheit, Beispiele aus Windows 7 und Ubuntu

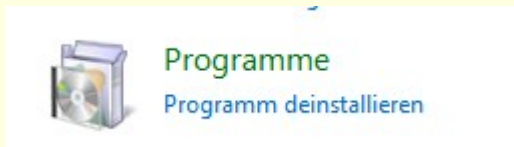
Benutzer nach Installation ist Admin, kein Hinweis
(sehr viele Nutzer wissen es nicht)



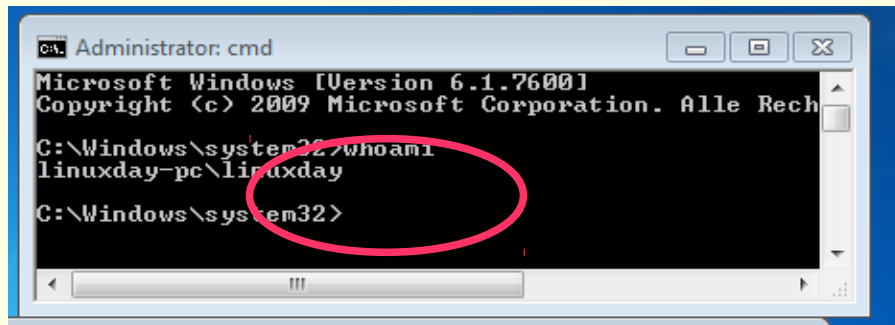
Windows kein SSH im Angebot, s.u.



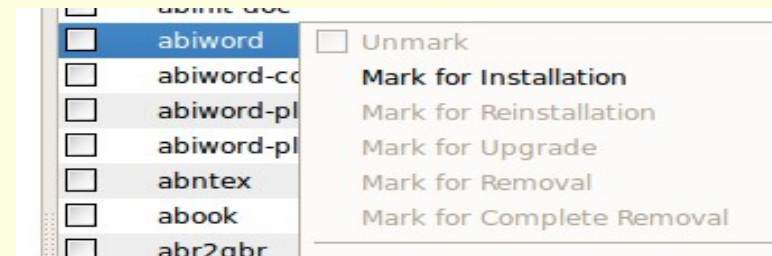
Programme, nur deinstallieren, nicht installieren



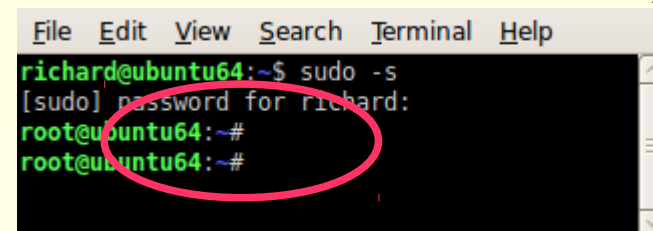
User **linuxday** wird **Administrator**, ohne PW, nur mit Klick
(Zustand ist nicht sichtbar)



in **Ubuntu** installieren und deinstallieren



User **richard** wird nicht **Administrator**
richard wird mit 'sudo' **root** und **Administrator**,
(nur mit Passwort, Zustand ist sichtbar '#',
alle Linux-Benutzer kennen den Unterschied)



Viren

- 'Computerviren' ?

- 'Computerviren' gibt es nicht, es sind immer Programme, die Fehler ausnutzen
 - Computerviren sind kein **medizinisches** Problem
 - diese Begriffe findet man bei 'Sicherheitsexperten'
 - Computerviren sind kein **militärisches** Problem
 - diese Begriffe findet man bei Politikern (Cyberwar, Abschreckung, milit. Gleichgewicht)
 - Computerviren sind ein Hinweis, dass das System defekt ist (Konzept, Design,...)

- Viren

- scheinbar fester Bestandteil eines PCs
- PC ohne Viren nicht vorstellbar (?)
- finanzstarker Markt, Monopolisierung
- nur ein BS wesentlich betroffen
- Virens Scanner können keine Sicherheit bringen (File 42.zip)
- „ein sicheres System braucht keine Viren-Scanner.
Viren-Scanner zeigen, dass generell etwas faul ist“ <http://www.danisch.de/blog/>
- **Linux ist nicht sicher, aber anders gesichert!**

(Sehen Sie bitte nach, was Ihnen Ihre Sicherheitsfirma empfiehlt.)

Sicherheit erhalten

• Firewall ist überflüssig

- Programme, die 'nach Hause' telefonieren
 - löschen oder gar nicht erst installieren, ist besser als Firewall
 - in Windows nur schwer möglich
- Ubuntu hat **keine** Programme mit 'Heimweh'
- **keine** offenen Ports
- Serverinstallationen sind ein anderes Thema (s.u.)

• Sicherheit erhalten

- keine **Voreinstellungen** ändern
- 'root' login nicht freischalten (ist in Ubuntu gesperrt)
- sichere Passwörter für alle Benutzer (mit 'pwgen' erzeugen)
- keine Software aus **Fremdquellen** (Ausnahmen bestätigen die Regel, X2GO)
- **Updates** täglich durchführen
- **Backups** mit 'rsync'
 - Wer hat ein Backup, und auch noch täglich?
 - Möglichkeiten bei der LUG-Ottobrunn
- sei nicht zu clever ... (kaputtadministrieren?)

Ergebnis

- 'Cyberwar' findet ohne uns statt
 - Computer-Unsicherheit hat politische Folgen
 - Cyberabwehrzentrum der Bundesregierung (?)
 - 'Frühwarnung gegen sogenannte **Cyber-Angriffe**'
 - „stell Dir vor, es ist Cyberwar und wir gehen nicht hin“ ;-)
 - das ist GNU/Linux/Ubuntu
- Ökologie,
 - weil es nicht immer der neueste Rechner sein muss
 - Hardware kann länger genutzt werden
- Filmhinweis
 - 'Kaufen für die Müllhalde', ARTE Mediathek
 - Geplante Obsoleszenz <http://de.wikipedia.org/wiki/Obsoleszenz>
 - Drucker, Software, Hardware → **künstlich** 'alt' gemacht?
 - „ein Artikel, der nicht verschleißt, ist eine Tragödie fürs Geschäft“

erste Schritte mit GNU/Linux/Ubuntu

- einfach nur benutzen

- es geht alles wie von selbst

- täglich damit arbeiten

- sich auf GNU/Linux/Ubuntu einlassen und **selbst** lernen
 - Wikis lesen (z.B. ubuntuusers.de)
 - Community kennenlernen (LUG vor Ort, Linuxtage)
- Ubuntu ist nicht wie der bisherige PC
 - Erfahrungen aus der bisherigen PC Welt sind wertlos
 - Vorsicht! Sie können 'Freunde' verlieren (und den Job!)
 - Ein Windows-Nutzer mit langer Erfahrung muss erkennen, dass er wieder ein Anfänger geworden ist
- dem '**allwissenden PC-Guru**' kündigen (*Nachbar, PC-Freak, 'guter Freund' ...*)
- nie jemanden an den Linux-PC lassen, der sich '**mit PCs auskennt**'

- und mit dem Terminal anfreunden

- es ist sehr effizient und hilft, Linux besser zu verstehen
- Linuxer haben ein schlechtes Gedächtnis ;-)
 - und bauen überall kleine, aber effiziente, Hilfen ein
 - Finden Sie diese Hilfen (History, Autovervollständigung, usw.)

erste Schritte mit GNU/Linux/Ubuntu

- etwas Neues ausprobieren

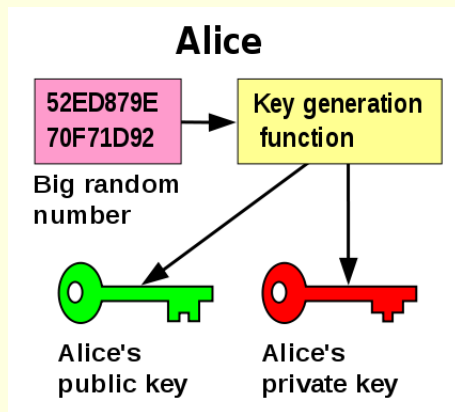
- andere Desktops
- LXDE, KDE, XFCE ...
 - Programme laufen mit jedem Desktop
- in Wikis 'ubuntuusers.de', 'ubuntu.com' sich informieren
- **apt-get** lernen – Updates, Install Remove
- **htop**, **yakuake**, **discus**, **vim**, **ssh**, **kvm** installieren
 - **htop** - Übersicht über alle Prozesse
 - **yakuake** – cleveres Terminal
 - **VIM** – Standard Editor, sehr schnell, ohne Grafik, im Terminal
 - **SSH** – private, sichere Verbindung mit Freunden (s.u.)
 - **kvm** – Virtualisierung von 'Altlasten'
- Bilder - **GIMP**
- Multimedia - Ubuntu installiert automatisch die Codecs

- Kommunikation und Sicherheit (PGP, TOR, SSH)

- mit Linux sehr einfach
- **Sie** müssen es nur machen

Public private Key Verschlüsselung, GPG (nicht nur Linux)

- <http://de.wikipedia.org/wiki/Public-Key-Verschlüsselungsverfahren>
- Produkt von sehr großen Primzahlen (z.B. $3 * 5 = 15$)

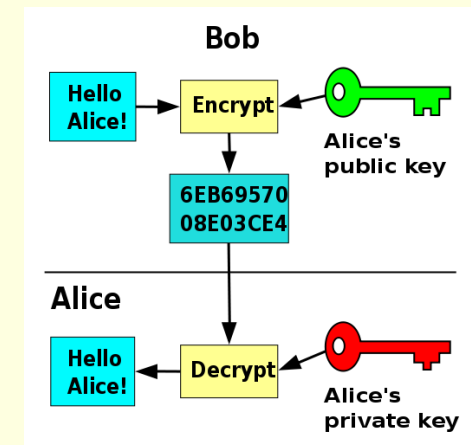


Alice:
erzeugt ein Keypair
sendet public Key zu Bob
Bob verschlüsselt mit diesem Key
nur Alice kann die Mail wieder lesen.

Bob: dto.

Public Key: öffentlich, kann jeder sehen
Private Key: streng geheim

Beide Schlüssel sind auf dem eigenen PC
Public Key auf dem PC des anderen



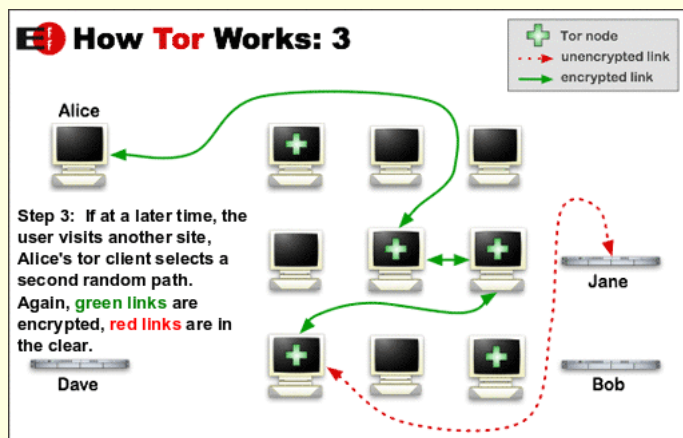
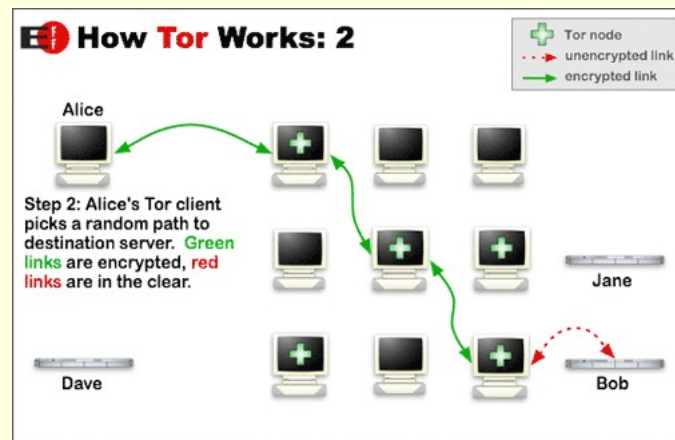
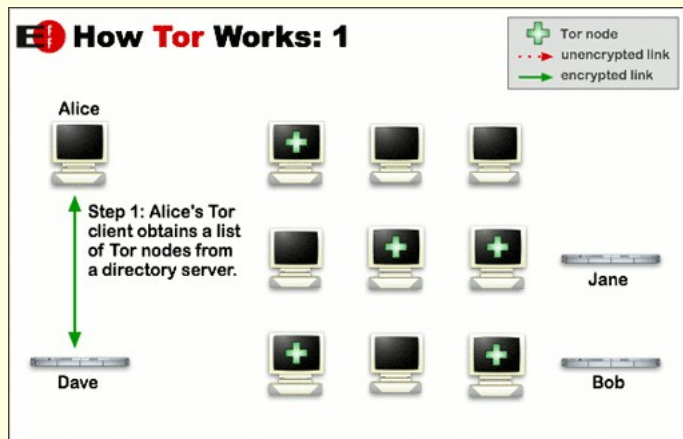
- How Public Key Cryptography (PKC) Works
 - http://www.livinginternet.com/i/is_crypt_pkc_work.htm

- Demo am Ende

Quelle:
<http://de.wikipedia.org/wiki/Public-Key-Verschl%C3%BCsselungsverfahren>
http://upload.wikimedia.org/wikipedia/commons/3/3f/Public_key_making.svg
http://upload.wikimedia.org/wikipedia/commons/f/f9/Public_key_encryption.svg

TOR (Plugin im Browser)

- <https://www.torproject.org/>
 - anonymisierter Zugriff auf eine Webseite



Tor verschleiert meine IP, aber nicht die Daten, die ich zum Webserver sende!

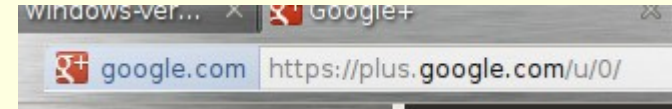
Der 'Exitnode' kann immer mitlesen.

Quelle:
<https://www.torproject.org/about/overview.html.en#thesolution>

HTTPS (im Browser)

- http://en.wikipedia.org/wiki/HTTP_Secure

- Traffic Verschlüsselung beim Zugriff auf Webseiten.
- Ein 'Lauscher' im Netz kann den Datenverkehr nicht mitlesen.
- Public Key ist im Browser und von einer CA signiert.
 - Sicherheit hängt vom Vertrauen in die CA ab
 - eigene Schlüssel mit CAcert (<http://www.cacert.org/>)
 - 'Web of Trust' bei CAcert



- PGP für Mails (Schlüssel unter voller Kontrolle)

- Mails müssen dabei unter eigener Kontrolle sein, nicht beim Provider

- HTTPS gegen 'abhören' (Schlüssel über CA, der man vertrauen muss ?)

- Surfen über unsichere Netze, eBanking, Shops, u.ä.

- TOR gegen Identifikation durch den Webserver (IP wird geändert)

- Schutz gegen Datensammler (nicht für Webportale, bei denen man sich anmeldet)

- SSH zur privaten Kommunikation unter Freunden (Schlüssel unter voller Kontrolle)

- sicherer Tunnel zum Zugriff auf andere Rechner, wenn der Besitzer es erlaubt

Linux intern, Einheitlichkeit durch Linux Standard Base (LSB)

- http://en.wikipedia.org/wiki/Filesystem_Hierarchy_Standard
 - folgende Verzeichnisse sind einheitlich angeordnet:
 - / root directory
 - /bin Befehle
 - /dev Geräte
 - **/etc Konfiguration System**
 - **/home/user Benutzerdaten und indiv. Konfiguration des Users**
 - /lib System
 - **/media USB Sticks, CDs**
 - /opt andere Software
 - /proc Virtuelles Filesystem, zeigt Systemzustand als simple ASCII-Files an
 - /usr alles, was nicht System ist, aber dazu gehört
 - **/var/log** Logfiles (auth.log, system.log, ...)
- Festplatten und Partitionen werden beim Start fest zugewiesen
 - Vergleichen Sie bitte mit anderen Betriebssystemen, ob das dort auch so übersichtlich ist?
 - es gibt keine 'Laufwerke', C: D: usw.
 - '/home/user' ist immer '/home/user'
 - „C:\Documents and Settings\[user name]“
 - C:\Users\[user name]\
 - http://en.wikipedia.org/wiki/My_Documents

Warum Ubuntu?

- und, da fehlt noch etwas?

- Erlebnis während meiner Kur im Januar 2011
- im Vortrag 'Bluthochdruck' ...
- herkömmlicher PC ist Ursache für Bluthochdruck ;-)
- Immer geht irgend etwas nicht :-)
- schon wieder eine Virenwarnung :-)
- Wer wird denn gleich in die Luft gehen?



- ***nimm Ubuntu***
- Ubuntu senkt den Blutdruck :-)
- Ubuntu verbessert unsere Gesundheit
- ... denn Ubuntu ist stressfreier



Vorteile für Sie

• Lernprozess

- besserer Umgang mit dem Internet
- bessere Kenntnisse im Umgang mit dem Computer
- der Weg geht vom 'Klick' zum Wissen
 - nicht nur 'Häkchen setzen', sondern wissen, was man konfiguriert, einstellt ...

• Ergebnis

- Besserer und 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 Linux/**Ubuntu** gelernt haben

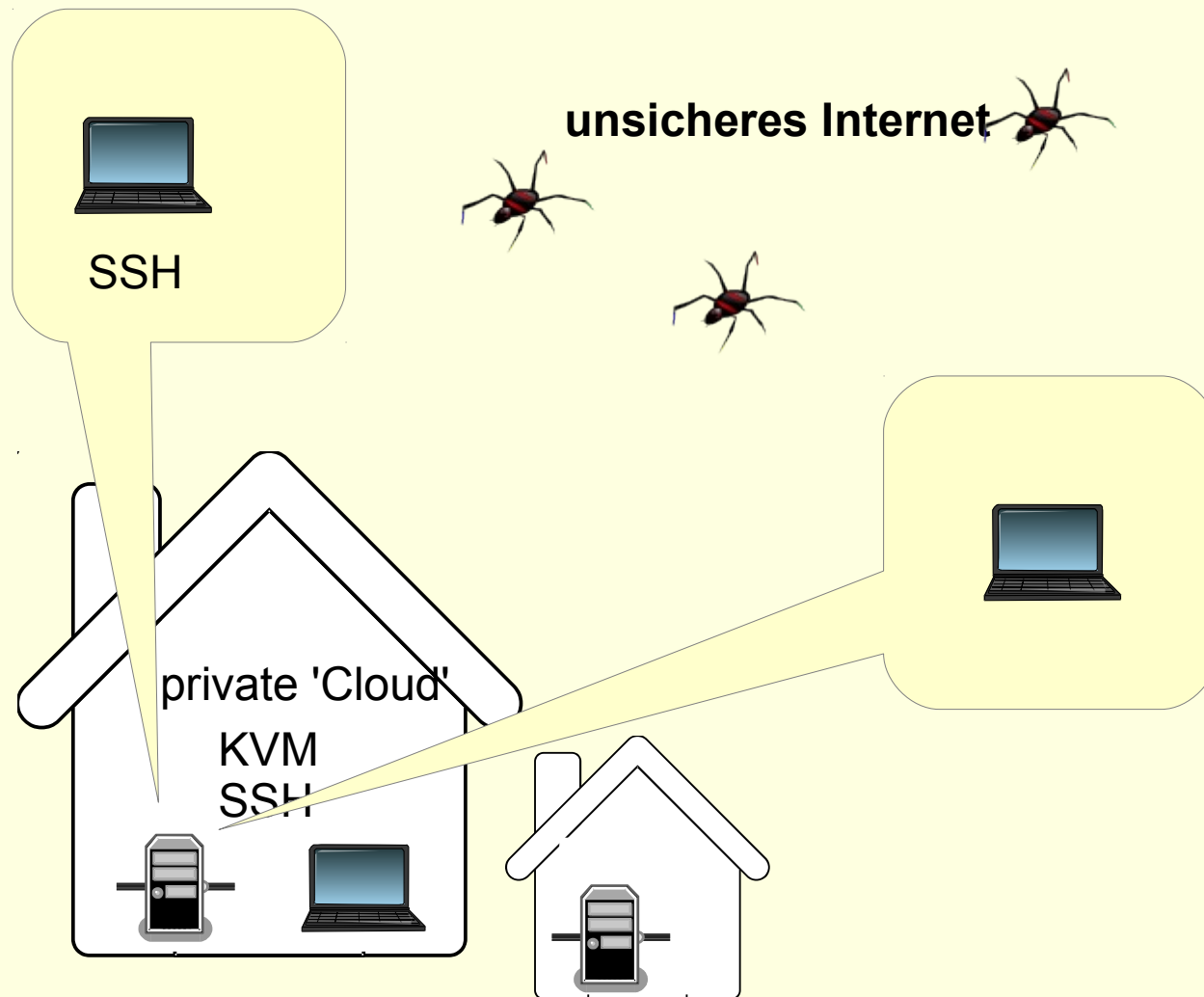
• Links

- <http://lug-ottobrunn.de>
- <http://www.lug-ottobrunn.de/wiki/Kategorie:Linuxeinsteiger>

GNU/Linux/Ubuntu im sicheren Netz



privates sicheres Netz, Sie haben die Kontrolle und die Sicherheit



sicheres Netz für die Familie

• Warum?

- Überwachung des Datenstroms nimmt zu
- 'Deep Paket Inspection' ist sehr wahrscheinlich
- „Das Arsenal der digitalen Überwachung“, 19.11.2011
 - <http://netzpolitik.org/2011/das-arsenal-der-digitalen-uberwachung/>
- Inhalte können vom Provider im Auftrag kontrolliert werden
- Sendung „Die Tücken der Überwachungstechnik“
ARD FAKT , 25.10.2011 21:45 Uhr
<http://www.mdr.de/fakt/ueberwachungssoftware100.html>

• SSH

- universelle sichere Verbindung (verschlüsselt)
- Peer to Peer

• Was kann ich damit tun?

- einfache Terminal Verbindung
- Ausgabe von grafischen Programmen umleiten
- Filemanager verteilt verwenden
- Ausgabe beliebiger Programme sicher durch das Netz bringen (Tunnel)

• 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
- stromsparender Server (z.B. invis)

Sicherheit von SSH

- SSH installieren (auf allen beteiligten PCs)

- # apt-get install **ssh**
- 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)

- Passwort Login sperren

- **Server absichern**
- **/etc/ssh/sshd_config editieren**
- Passwort-Login für alle Benutzer sperren

PermitRootLogin no
PasswordAuthentication no

- Router freischalten, nach dem Sperren des Logins

- Port 22 muss zum Server-PC weitergeleitet werden
- Firewall im Router abschalten, bzw. den SSH Port freischalten
in Doku des Routers nachlesen

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

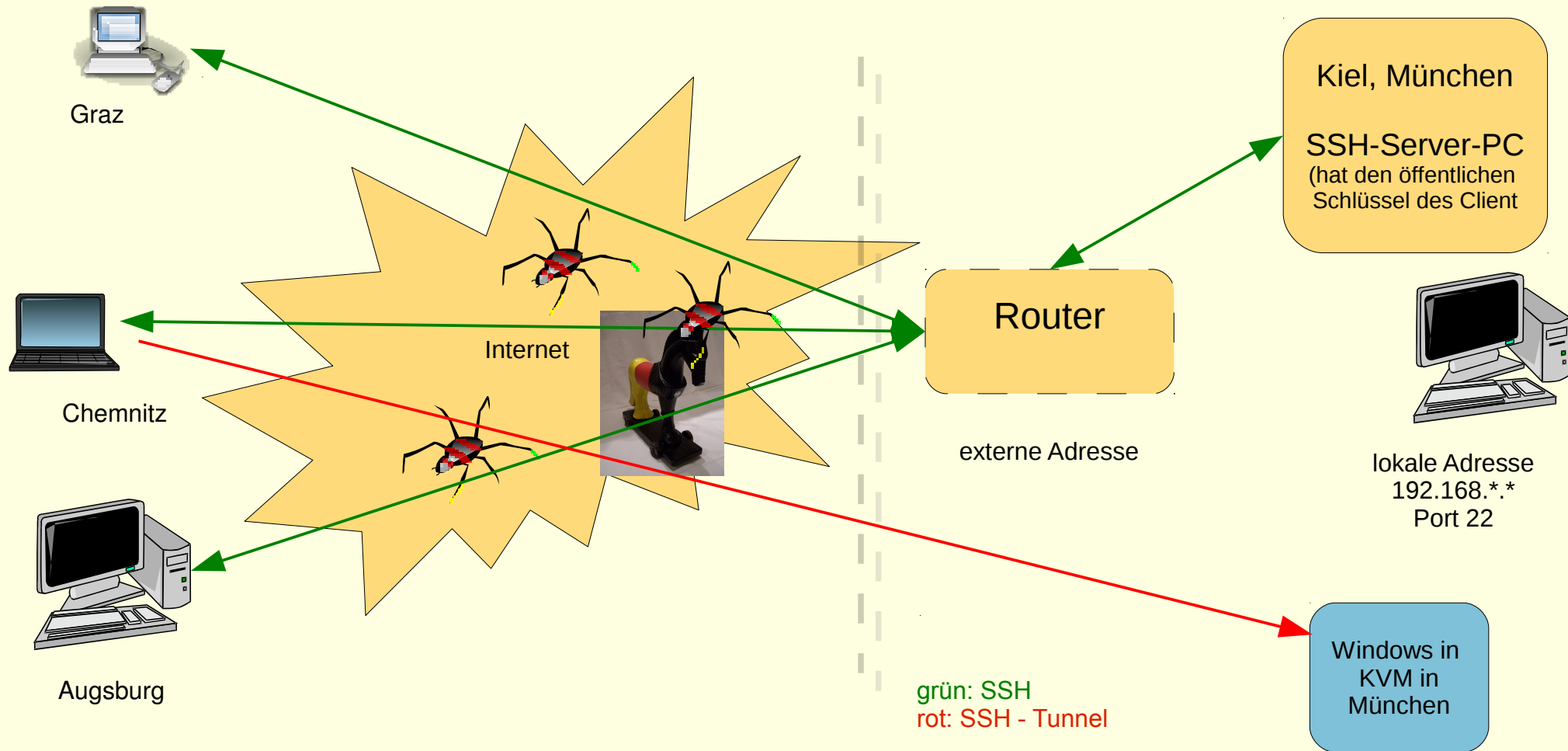
- Wer → Wohin ?

- Client initiiert Verbindung zu einem Benutzer auf dem Server
- ***ssh -X -C 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

- Links bei der LUG-Ottobrunn

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

so sieht es aus



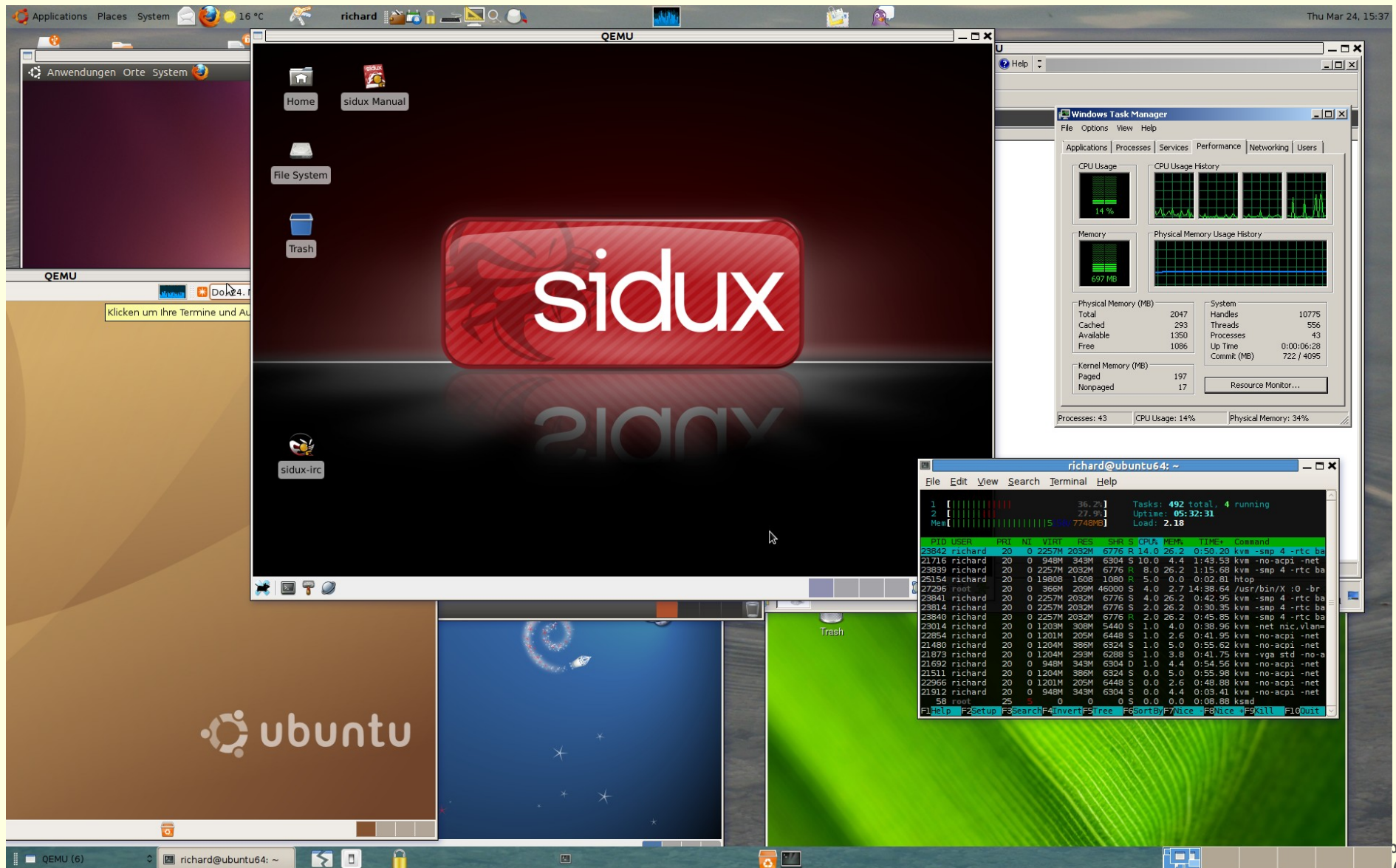
SSH Anwendungen

- **Terminal**
 - `ssh -X -C richard@kiel.ath.cx`
- **Filemanager**
 - `ssh://richard@kiel.ath.cx/home/richard`
- **X Forward**
 - in Kiel, `cd boids, ./boids`
- **X2GO**
 - Remote Desktop nach Kiel, bzw. nach München

Virtualisierung mit KVM

- Kernel Based Virtual Machine
 - von Ubuntu favorisiert
 - KVM Buch: <http://qemu-buch.de/de/index.php/Hauptseite>
 - 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.
- Warum?
 - PC Altlasten weiter betreiben
 - http://lug-ottobrunn.de/wiki/Umzug_eines_PC_nach_KVM
 - z.B. Finanzbuchhaltung, Steuererklärung
 - Testen von Linux Umgebungen
 - Mini-Server
 -
- Performance
 - fast so schnell, wie der Host PC
 - Tests
 - http://www.phoronix.com/scan.php?page=article&item=ubuntu_1110_xenkvm&num=1

Virtualisierung mit KVM



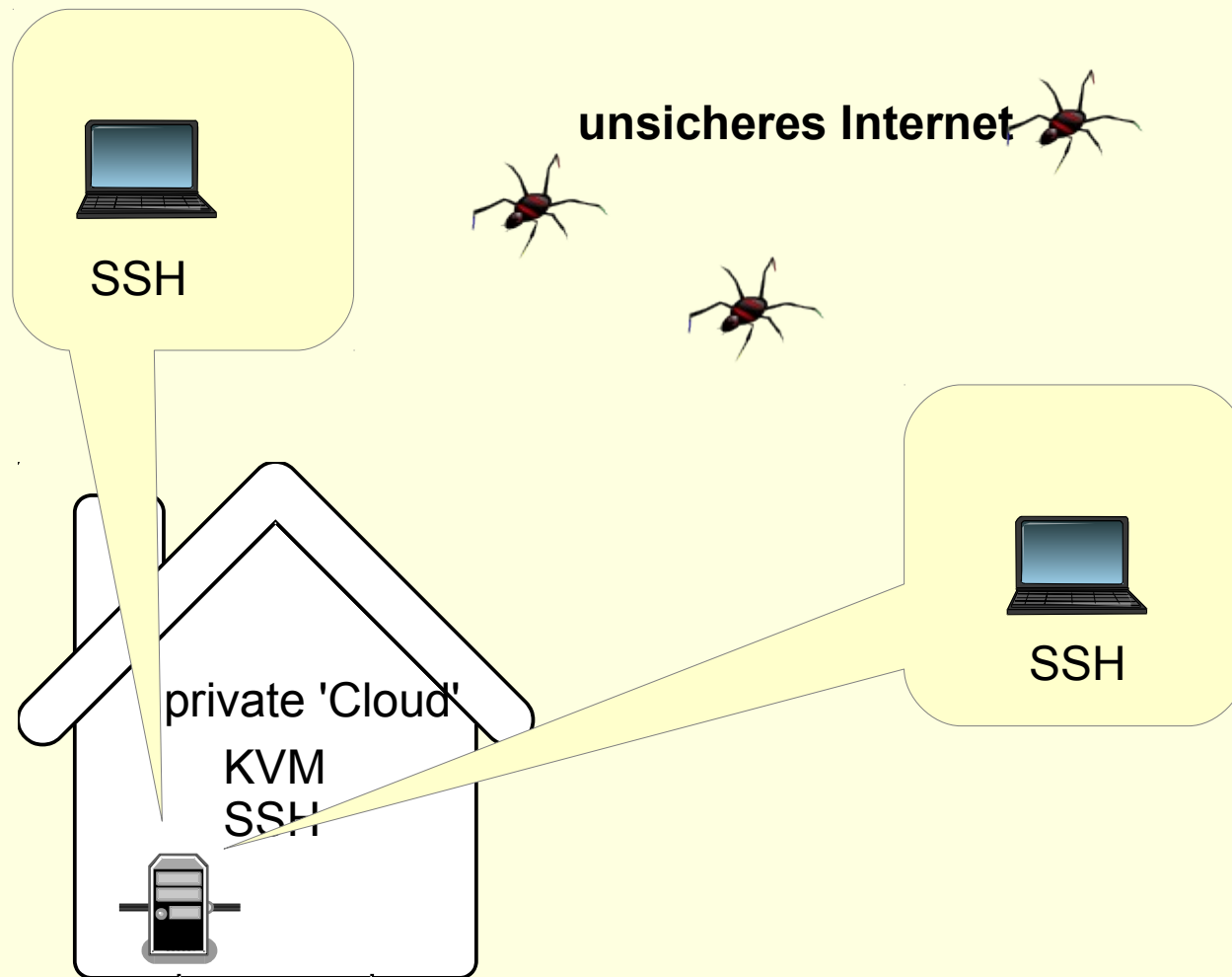
Installation von KVM unter Ubuntu

- Siehe Webseiten von 'ubuntuusers.de' und 'ubuntu.com'
 - <http://wiki.ubuntuusers.de/KVM>
 - <http://wiki.ubuntuusers.de/QEMU>
 - <https://help.ubuntu.com/community/KVM>
 - http://www.linux-kvm.org/page/Management_Tools
- Install **qemu-kvm** und testen
 - `# apt-get install kvm`
 - `$ kvm-ok`
 - INFO: Your CPU supports KVM extensions
 - INFO: /dev/kvm exists
 - KVM acceleration can be used
- http://lug-ottobrunn.de/wiki/Virtualisierung_mit_KVM

Einbinden in das lokale Netz

- *bridge utils* für Einbindung in das lokale Netz (192.168.*.*)
 - default ist 10.2.0.2, d.h. die VM ist 'unsichtbar'
 - <https://help.ubuntu.com/community/KVM/Networking>
 - nicht ganz einfach, aber gut dokumentiert
 - http://lug-ottobrunn.de/wiki/Virtualisierung_mit_KVM
- **Demos**
 - Windows 2008 Server, in KVM im lokalen Netz zu Hause
 - Zugriff mit Remote Desktop
 - Windows kann kein SSH, Ubuntu schon
 - **ssh -L 10022:vwin2008:3389 lugdemo@meinPC.dyndns.org**
 - Zugriff mit Remote-Desktop, localhost
 - **rdesktop -x l -g 1100x720 -a 16 -k de -u Administrator -p xxxxxxxx localhost:10022**
 - Demo 2: Windows 7 lokal
 - **kvm win7fibu.ovl -m 2048 -smp 2 -net nic -net user,hostfwd=tcp::3389-:3389**
 - Zugriff zum Remote-Desktop mit localhost
 - **rdesktop -x l -g 1200x720 -a 16 -k de -u rleo localhost**

privates sicheres Netz, Sie haben die Kontrolle



Ende des Vortrages, kein Ende mit Linux ;-))

- 'to go the Ubuntu/Linux Way'
 - ist der Weg zu einem sicheren, einfachen und stabilen System
- Lernprozess
 - bessere Kenntnisse im Umgang mit dem Computer
 - bessere Sicherheit des eigenen PC
- Ergebnis
 - **Sie** werden staunen, was **Sie** alles im Umgang mit Linux gelernt haben
- sicheres privates Netz
 - einfach, transparent, sicher
- KVM
 - alter PC lebt virtuell weiter
 - jedem sein PC, egal, wo man sich aufhält
 - besonders gesicherter PC in einer VM

*Vielen Dank für Ihre Aufmerksamkeit
und einen schönen Linuxtag in Chemnitz*

THE HIGHWAY TO FREEDOM IS NOW OPEN FOR EVERYONE



it's your turn to go ...