

# Sicherer Fernzugriff dank Linux - selbst auf ein uraltes Windows



TÜBIX 2024  
22. Juni 2024

# Vorstellung Stefan Baur



- BAUR-ITCS UG (haftungsbeschränkt):
  - Gesellschafter-Geschäftsführer
- freier Autor:
  - Heise Online
  - c't
  - Make:
  - Südwest Presse

# Vorstellung Stefan Baur



- Open Remote Computing Association – orca e.V.
- 1. Vorsitzender
- Projekt X2Go
  - Projektkoordinator
  - Eventplaner
  - Lead Evangelist
- Erfinder des Grannophones

# Vorstellung Stefan Baur



- Der Typ, der dem TÜBIX ein Infozelt neben die Zufahrt stellt, wenn er mit seinem Projekt keinen Stand auf dem Gelände bekommt ;-)
- 2023 offiziell mit Genehmigung der Stadt Tübingen erfolgt (öffentlicher Grund)
- 2024 sind wir aber wieder regulär dabei und drinnen zu finden → Aufzug ins Erdgeschoss nehmen, dann 90° links

# Niemand muss mitschreiben!

- Es gibt zwar keine Aufzeichnung, aber meine Slides werden im Nachgang zum Download angeboten
- Hoffentlich auf der TÜBIX-Seite
- Mindestens aber auf der X2Go-Wiki-Events-Seite  
<https://wiki.x2go.org/doku.php/events:start>  
(siehe auch QR-Code)
- QR-Code kommt auch gegen Ende nochmal
- Aufpassen: Nächstes Jahr bekommt die Seite einen neuen Inhalt → am Seitenende auf 2024 klicken, um ins Archiv zu wechseln



Event-Wikiseite

# Warum haben wir das Problem?

- Ransomware-Angreifer verlegen sich von Mails mit dubiosen Anhängen auf schlecht gesicherte Remote-Zugänge → shodan.io, Portscans, ...
- Worst Case: Portforwarding 5900 (VNC)/3389 (RDP) von öffentlicher IP auf Zielsystem – aber auch ältere kommerzielle Firewalls/Secure-Mobile-Access-Systeme mit ungepatchten Lücken (End of Life, EOL)
- Gründe fürs Schlampern: kein Geld/keine Zeit/keine Lust/keine Ahnung
- älteres Zielsystem, welches nicht upgegradet werden kann → kein aktuelles TLS/SSL, keine Network Level Authentication (NLA)
- „Wir sind doch kein lohnendes Ziel“
- Lottospiel – oder doch eher Russisches Roulette (mit mehreren Kugeln)?

# Einfachster Softwareansatz: SSH+2FA

- SSH
  - Unterstützt aktuelle, sichere Verschlüsselungstechniken
  - Unterstützt Pluggable Authentication Modules (PAM)
    - Dadurch Zwei-Faktor-Authentisierung sehr einfach möglich
    - Anbindung an LDAP oder AD zwecks Benutzerauthentisierung ebenfalls möglich (ob für diesen Zweck sinnvoll, sei dahingestellt)
- 2FA über mehrere PAMs möglich (u.a. libpam-oath, -otpw, -yubico, ...)
- Google-Modul libpam-google-authenticator ist ziemlich komfortabel (Recovery-Codes, telefoniert nicht nach Hause, Open Source)

# Netzwerk: Mittendrin oder nur dabei?

- Das System, auf dem unser SSH-Daemon laufen soll, kann entweder direkt im LAN hängen, wie das zu schützende System/die zu schützenden Systeme, oder wie eine Firewall mit separatem Ethernet-Port nur diese Systeme anbinden
- Wer im eHealth-Bereich tätig ist, fühlt sich vielleicht gerade an das Thema TI-Konnektoren erinnert ... auch bei denen war das eine wichtige Grundsatzentscheidung.
- Vor- und Nachteile müssen individuell abgewogen werden, man kann keine pauschale Empfehlung geben, welcher Ansatz der sinnvollere ist.

# Netzwerk: Mittendrin oder nur dabei?



# Netzwerk: Welcher Paranoialevel?



# Hardware: So gut wie egal

- Raspberry Pi (gegebenenfalls mit USB-Ethernet-Adapter für zweiten LAN-Port) → siehe Demo an unserem Stand
- Irgendwelche Custom-Embedded-Hardware (so lange von der Distribution noch unterstützt, auch 32-Bit-Hardware „recyclebar“)
- Älterer PC, den man gegebenenfalls noch mit ein, zwei Netzwerkkarten aufrüstet (Kostenpunkt aber: Stromverbrauch im Vergleich zu Pi und Embedded-Systemen)
- Wenn eh schon Virtualisierung im Einsatz ist, natürlich auch per VM möglich (aber auch hier wieder: Sicherheitsrisiko, VM-Ausbruch-Exploits, Heartbleed, Spectre, etc. → besser auf „echtem Blech“)

# Netzwerk: Konfiguration „nur dabei“

- Nur ein Interface
- IP-Adresse/DNS:
  - entweder statisch auf dem System selbst eintragen in /etc/network/interfaces /etc/resolv.conf
  - oder per DHCP zuteilen lassen und auf dem Router die MAC und IP fest zueinander zuordnen

```
root@alix1:/# cat /etc/network/interfaces
# interfaces(5) file used by ifup(8) and ifdown(8)
# Include files from /etc/network/interfaces.d:
source-directory /etc/network/interfaces.d
auto lo
iface lo inet loopback

allow-hotplug eth0
iface eth0 inet static
        address 192.168.178.45
        netmask 255.255.255.0
        gateway 192.168.178.1
root@alix1:/# cat /etc/resolv.conf
domain fritz.box
search fritz.box
nameserver 192.168.178.1
```

```
# Include files from /etc/network/interfaces.d:
source-directory /etc/network/interfaces.d
auto lo
iface lo inet loopback

allow-hotplug eth0
iface eth0 inet dhcp
```

# Netzwerk: Konfiguration „mittendrin“

- Zwei Interfaces
- LAN IP-Adresse/DNS:
  - Konfiguration wie vorhin
- Separates Netzwerk:
  - entweder Client und Server mit statischen IP-Adressen konfigurieren (siehe Screenshot)
  - oder DHCP z.B. mit DNSmasq einrichten
    - kein Gateway eintragen, da kein Routing und kein NAT erwünscht
  - Wer da Hilfe braucht → Folie bezüglich kommerz. Support am Ende

```
# interfaces(5) file used by ifup(8) and ifdown(8)
# Include files from /etc/network/interfaces.d:
source-directory /etc/network/interfaces.d
auto lo
iface lo inet loopback

allow-hotplug eth0
iface eth0 inet dhcp

allow-hotplug eth1
iface eth1 inet static
    address 192.168.123.1
    netmask 255.255.255.0
~
~
~
~
9,0-1 All
```

# Einrichtung SSH+2FA (Teil 1)

- Annahmen:
  - Basissystem ist Debian 12 / Devuan 5 / Raspberry Pi OS 12
  - root ist per SSH-Public-Keyfile oder an der lokalen Konsole eingeloggt (Wichtig, sonst sperrt man sich aus!)
- Als root:  
`apt update`  
`apt install openssh-server ntp libpam-google-authenticator`
- Optional als root:  
`apt install sudo molly-guard`
- Als root an das Ende der Datei `/etc/pam.d/sshd` diese Zeile anhängen:  
`auth required pam_google_authenticator.so`

# Einrichtung SSH+2FA (Teil 2)

- Als root den normalen Benutzer anlegen:  
adduser userle #oder wie der User auch immer heißen soll
- Als root die Datei /etc/ssh/sshd\_config öffnen und diese Parameter setzen/prüfen (es darf kein „#“ davorstehen):  
PermitRootLogin prohibit-password #oder no, aber kein yes  
KbdInteractiveAuthentication yes  
UsePAM yes
- Als root den sshd neu starten (dabei fliegt man *nicht* raus, keine Sorge):  
service sshd restart

# Einrichtung SSH+2FA (Teil 3)

- Entweder an der lokalen Konsole (per SSH geht es jetzt nicht mehr) als Benutzer `user1e` einloggen
- Oder als `root` mittels `su user1e` in den Benutzer wechseln
- Als Benutzer `user1e` dann die Google-Authenticator-Konfiguration starten: `google-authenticator`

# Einrichtung SSH+2FA (Teil 4)

- Die Fragen des Google-Authenticator-Konfiguration wie folgt beantworten:
  - `Do you want authentication tokens to be time-based (y/n) y`
  - Danach erscheint ein QR-Code auf der Konsole
  - Diesen mit einer OTP-App wie FreeOTP+ oder Google Authenticator einlesen
  - `Enter code from app (-1 to skip):`
    - Entweder einen Code aus der App zum Test eingeben
    - oder mittels `-1` den Test überspringen

# Einrichtung SSH+2FA (Teil 5)

- Die Scratch Codes sollte man sich nun ausdrucken und z.B. in den Tresor oder die Geldbörse packen.
- Danach geht es mit folgenden Fragen und Antworten weiter:
  - Do you want me to update your  
"/home/userle/.google\_authenticator" file? (y/n) y
  - Do you want to disallow multiple uses of the same authentication token? This restricts you to one login about every 30s, but it increases your chances to notice or even prevent man-in-the-middle attacks (y/n) y

# Einrichtung SSH+2FA (Teil 6)

- Danach geht es mit dieser Frage weiter – ich empfehle „y“, außer man ist völlig paranoid:

- By default, a new token is generated every 30 seconds by the mobile app.

In order to compensate for possible time-skew between the client and the server, we allow an extra token before and after the current time. This allows for a time skew of up to 30 seconds between authentication server and client. If you experience problems with poor time synchronization, you can increase the window from its default size of 3 permitted codes (one previous code, the current code, the next code) to 17 permitted codes (the 8 previous codes, the current code, and the 8 next codes). This will permit for a time skew of up to 4 minutes between client and server.

Do you want to do so? (y/n) y

# Einrichtung SSH+2FA (Teil 7)

- Und zuletzt noch:
  - If the computer that you are logging into isn't hardened against brute-force login attempts, you can enable rate-limiting for the authentication module.  
By default, this limits attackers to no more than 3 login attempts every 30s.  
Do you want to enable rate-limiting? (y/n) y

# Test SSH+2FA

- Siehe da, es klappt:

```
user@hpwendy:~$ ssh userle@alix1
Password:
Verification code:
Linux alix1 6.1.0-21-686 #1 SMP PREEMPT_DYNAMIC Debian 6.1.90-1 (2024-05-03) i586

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Jun 20 13:05:51 2024 from 192.168.0.14
userle@alix1:~$
```

# Readonly-Resilienz

- Eine Möglichkeit, so ein System gegen Angriffe und Abstürze resilienter zu machen, ist, ein Readonly-/Overlay-Dateisystem zu verwenden.
- Vorteile:
  - Schadcode überlebt (hoffentlich) den nächsten Neustart nicht
  - /-Dateisystem ist beim Start immer in einem saubereren Zustand
- Nachteile:
  - Vor Updates muss auf read-write geschaltet werden, danach zurück
  - /home braucht Spezialbehandlung (separater Mountpoint, Mountoptionen `rw`, `sync`, `noexec`)

# Was ist das? Was macht das?

- Nein, kein blaues Licht, sondern ein minimaler SSH-Server mit 2FA.
- Vorteile:
  - Braucht nur wenig Speicherplatz/RAM/CPU
  - Geringe Angriffsfläche – nur ein einziger exponierter Dienst
    - Wartungsarm und sicher, denn was nicht installiert ist ...
      - kann nicht gehackt werden
      - braucht nicht ständig irgendwelche Patches
  - Leicht zu auditieren

# Für Experten und Terminalfans

- SSH bietet erst mal nur eine Textkonsole, von der aus man Dinge tun kann → für Linux-Kenner OK, für Otto Normaluser eher nicht hilfreich
- Ports tunneln statt forwarden → Ja, geht, für Otto Normaluser aber immer noch etwas fummelig, als Admin sollte man da geeignete Start- und Stopskripte für die User bereitstellen
- Randnotiz: VPN statt SSH soll heute nicht Thema sein, auch das ist je nach Konstellation „fummelig“ und bei Bring-Your-Own-Device (BYOD) auch noch ein Sicherheitsrisiko (Client kann bereits gehackt sein und kommt dann ins Firmennetz). Zu „SSH als VPN“ → 16:00, Raum V2, Vortrag „SSH für/vs. Security Engineers?“ von Oleksandr Shcherbakov

# X2Go – und die Welt wird bunt

- Wenn man hauptsächlich Linux in seinem LAN nutzt, macht die Installation von X2Go auf den dort vorhandenen Linuxsystemen für den Remotezugriff definitiv Sinn.
- Damit bekommt man wahlweise komplette Remote Desktops oder einzelne Anwendungen, die im Firmennetz laufen, auf dem eigenen Rechner dargestellt.
- Der Clou dabei: X2GoClient unterstützt von Haus aus den Zugang über einen vorgeschalteten SSH-Server, so wie wir ihn gerade besprochen haben!
- Und natürlich gibt es X2GoClient auch für Windows, so dass Otto Normaluser es auch nutzen kann, und nicht zwingend Linux benötigt.

# Was ist X2Go

- X2Go ist eine freie Remote-Desktop-/Remote-Application-Lösung  
→ kostenlos nutzbar, auch in Firmen, eigene Anpassungen erlaubt
- X2GoClient gibt es für Linux, Windows und macOS
  - Er kann auch als grafisches Frontend für RDP- (Windows Remote Desktop)/XDMCP-Logins dienen → das schauen wir uns nachher an!
  - Der Linux-X2GoClient eignet sich auch zum Direktzugriff auf RDP und XDMCP – ohne X2GoServer
- X2GoServer gibt es aktuell nur für Linux → ist für den heutigen Vortrag aber nicht wirklich relevant

# Installation X2GoServer

- Annahme wiederum:
  - Basissystem ist Debian 12 / Devuan 5 / Raspberry Pi OS 12
- Als root:  
`apt update`  
`apt install x2goserver x2goserver-xsession`
- Optional *vorher* das X2Go-Stable-Repository einbinden (Anleitung, wie das geht: <https://wiki.x2go.org/doku.php/wiki:repositories:debian>)
- Zusätzlich als root, wenn das Verbindungsziel ein Windows-System mit RDP oder VNC ist:  
`apt install rdesktop freerdp2-x11 remmina`

# Konfiguration X2GoClient - SSH-Proxy

- Host: Die *interne* IP-Adresse des X2Go-Servers
- Häkchen „Proxy-Server für SSH-Verbindung verwenden“ ankreuzen → Weitere Optionen klappen aus
- Typ: SSH
- Host: Die *öffentliche* IP-Adresse des Routers (auf diesem muss ein Portforwarding eingerichtet werden)
- Login: user1e (SSH-Server-Account)

The screenshot shows the X2GoClient configuration window with the following settings:

- Sitzung:** X2GoServer-Firma
- Symbol ändern:** A button to change the session icon.
- Pfad:** /
- Server:**
  - Host: 192.168.178.123
  - Login: meinx2goserverbenutzername
  - SSH-Port: 22
  - RSA-/DSA-Schlüssel verwenden (ssh): [empty]
  - Anmeldung über voreingestellten SSH-Schlüssel oder ssh-agent
  - Kerberos5 (GSSAPI) Authentifizierung
  - Übertragung der GSSAPI-Legitimation auf den Server
  - Proxy-Server für SSH-Verbindung verwenden
- Proxy-Server:**
  - Typ:  SSH
  - Gleiche Anmeldung wie für X2Go-Server
  - Login: user1e
  - HTTP
  - Gleiches Kennwort wie für X2Go-Server
  - Host: öffentliche.ip.hier
  - RSA-/DSA-Schlüssel: [empty]
  - Port: 22
  - SSH-Agent oder SSH-Standardschlüssel
  - Kerberos5 (GSSAPI) Authentifizierung
- Sitzungsart:**
  - In X2GoKDrive starten (experimentell)
  - XFCE
  - Befehl: [empty]

Buttons at the bottom: OK, Abbrechen, Voreinstellungen

SSH-Proxy <@kdrive-server>

Anwendungen: doc.newtox2go [X2G... xclock keyes

2024-06-20 19:11 Ben Utzer

doc.newtox2go [X2Go - everywhere@home] - Pale Moon

File Edit View History Bookmarks Tools Help

x2go.org <https://wiki.x2go.org/doku.php/doc.newtox2go> DuckDuckGo

Most Visited: Pale Moon, Pale Moon forum, F.A.Q., Release notes

doc.newtox2go [X2Go - every x

Announcements / News

- Documentation
  - New to X2Go? Start here!
  - Success Stories
  - Installing X2Go
  - Using X2Go
  - Desktop Environment
  - Compatibility
  - Windows-Specific Release Notes
  - Participate in X2Go
  - Who is who in X2Go
  - Professional Support
  - Development Sponsoring
  - Frequently Asked Questions
  - HowTos

Download

### New to X2Go? Start here!

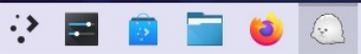
#### Overview

X2Go enables you to access a *graphical desktop* of a computer over a *low bandwidth* (or high bandwidth) connection.

X2Go is a *Remote Desktop* solution, which some vendors vaguely call *Remote Control*. This is not to be confused with Microsoft Remote Desktop Connection, which is a competing Remote Desktop solution and protocol.

- New to X2Go? Start here!
- Overview
- Terminology compared to standard X11
- Installation and Use
- Screenshots

X2Go per Spende unterstützen?  
Spendenlinks auf <https://wiki.x2go.org>  
oder via QR-Code hier:



```
~: bash — Konsole
Datei Bearbeiten Ansicht Lesezeichen Module Einstellungen Hilfe
Neues Unterfenster Split View Kopieren Einfügen
tuebix2024@hpwendy:~$ x2golistsessions
tuebix2024@hpwendy:~$
```

```
~: xclock — Konsole <@kdrive-server>
Datei Bearbeiten Ansicht Lesezeichen Module Einstellungen Hilfe
Neues Unterfenster Ansicht teilen Kopieren Einfügen Suchen
user1@kdrive-server:~$ x2golistsessions
320679|user1-50-1718903626_strPUBLISHED_dp24|50|kdrive-server|R|2024-06-20T19:13:46|e9cd222b4286d6b3020bcf6275
2d9e90|192.168.133.100|54841|54842|2024-06-20T19:13:47|user1|354|54843|-1|-1
user1@kdrive-server:~$ xclock
```



doc:newtox2go [X2Go - everywhere@home] - Pale Moon <@kdrive-server>

File Edit View History Bookmarks Tools Help

x2go.org <https://wiki.x2go.org/doku.php/doc:newto:> DuckDuckGo

Most Visited Pale Moon Pale Moon forum F.A.Q. Release notes

### doc:newtox2go [X2Go - ever] +

- Announcements / News
- Documentation
  - New to X2Go? Start here!
  - Success Stories
  - Installing X2Go
  - Using X2Go
  - Desktop Environment Compatibility
  - Windows-Specific Release Notes
  - Participate in X2Go
  - Who is who in X2Go
  - Professional Support
  - Development Sponsoring
  - Frequently Asked Questions
  - HowTos
- Download

## New to X2Go? Start here!

### Overview

X2Go enables you to access a *graphical desktop* of a computer over a *low bandwidth* (or high bandwidth) connection.

X2Go is a *Remote Desktop* solution, which some vendors vaguely call *Remote Control*. This is not to be confused with Microsoft Remote Desktop Connection, which is a competing Remote Desktop solution and protocol.



# Und nun, das Wett... äh, Windows

- X2Go unterstützt die alten, unsicheren Windows-Versionen (ohne Network Level Authentication) direkt.
- Dazu muss nur, wie zuvor auf dem Slide „Installation X2GoServer“ beschrieben, rdesktop auf dem X2Go-Server installiert werden.  
(X2GoServer = die Software; X2Go-Server = das Linuxsystem, auf dem die X2GoServer-Software installiert ist)
- Wir packen jetzt einfach X2GoServer und rdesktop auf den bisherigen SSH-Server mit drauf!

# Konfiguration X2GoClient - rdesktop

- Host: Die öffentliche IP-Adresse des Routers (auf diesem muss ein Portforwarding eingerichtet werden)
- Login: user1e (der SSH-Server-Account)
- Häkchen „Proxy-Server für SSH-Verbindung verwenden“ *nicht* ankreuzen
- Sitzungstyp:  
Verbindung mit Windows-Terminalserver herstellen/IP des Windows-PCs

The screenshot shows the X2GoClient configuration window with the following settings:

- Tab: Sitzung
- Sitzungsname: JumpHost-Firma
- Symbol: A small cartoon animal icon with the text "<< Symbol ändern".
- Pfad: /
- Server section:
  - Host: öffentliche.ip.hier
  - Login: user1e
  - SSH-Port: 22
  - RSA-/DSA-Schlüssel verwenden (ssh):
  - Anmeldung über voreingestellten SSH-Schlüssel oder ssh-agent
  - Kerberos5 (GSSAPI) Authentifizierung
  - Übertragung der GSSAPI-Legitimation auf den Server
  - Proxy-Server für SSH-Verbindung verwenden
- Sitzungsart section:
  - In X2GoKDrive starten (experimentell)
  - Verbindung mit Windows Terminalserver herstellen (selected) | Server: 192.168.178.23 | Erweiterte Einstellungen...
  - Direkte RDP-Verbindung

Buttons at the bottom: OK, Abbrechen, Voreinstellungen.

rdesktop - 192.168.123.2 <@alix1>

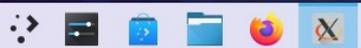
**Windows-Anmeldung**

Microsoft  
**Windows<sup>XP</sup>**  
Tablet PC Edition  
Copyright © 1985-2001  
Microsoft Corporation

Benutzername:

Kennwort:

Esc	~ `	! 1	@ 2	# 3	\$ 4	% 5	^ 6	& 7	* 8	( 9	) 0	- _	+ =	Bksp	Home	PgUp
Tab	q	w	e	r	t	y	u	i	o	p	{ [	} ]	\		End	PgDn
Caps	a	s	d	f	g	h	j	k	l	;	;	"	'	←	Del	PrtScn
Shift	z	x	c	v	b	n	m	<	,	>	.	?	/	Shift	Insert	Pause
Ctrl	⊞	Alt							@	↓	↑	←	→	Func	ScrLk	



DE 19:59  
20.06.24

X2GoClient

Sitzung Einstellungen Hilfe

**Sitzungs-ID:** userle-50-1718906182\_stRRDP\_dp24  
**Server:** 192.168.133.1  
**Login:** userle  
**Display:** 50  
**Startzeit:** Do, Juni 20 19:57:28 2024  
**Status:** aktiv

Info: using zlib stream compression 4/4.  
Info: No suitable cache file found.  
Info: Forwarding X11 connections to display ':0'.  
Info: Forwarding auxiliary X11 connections to display ':0'.  
Session: Session started at 'Thu Jun 20 19:57:28 2024'.  
Info: Established X server connection.  
Info: Using shared memory parameters 0/0K.

Zeige Details

rdesktop - 192.168.123.2 <@alix1>

**Eingabeaufforderung**

```
C:\Dokumente und Einstellungen\Pepe Paradigma>ipconfig

Windows-IP-Konfiguration

Ethernetadapter Drahtlose Netzwerkverbindung:

    Medienstatus. . . . . : Es besteht keine Verbindung

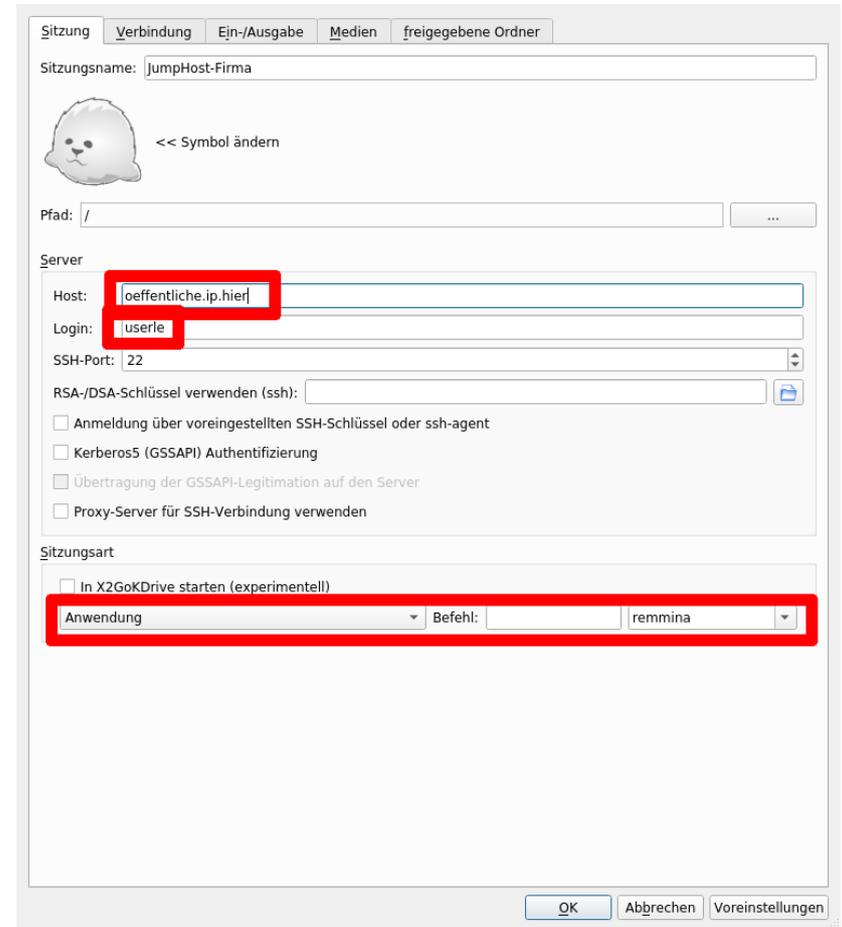
Ethernetadapter LAN-Verbindung:

    Verbindungsspezifisches DNS-Suffix:
    IP-Adresse (Autokonfig.) . . . . . : 192.168.123.2
    Subnetzmaske . . . . . : 255.255.255.0
    Standardgateway . . . . . :

C:\Dokumente und Einstellungen\Pepe Paradigma>
```

# Konfiguration X2GoClient - remmina

- Host: Die öffentliche IP-Adresse des Routers (auf diesem muss ein Portforwarding eingerichtet werden)
- Login: `user1e` (der SSH-Server-Account)
- Sitzungstyp:  
Anwendung
- Befehl:
  - erstes Feld leer lassen
  - Im Dropdown-Menü *tippen*: `remmina`



The screenshot shows the X2GoClient configuration window with the following settings:

- Tab: Verbindung
- Sitzungsname: JumpHost-Firma
- Symbol: A small animal icon with the text "<< Symbol ändern"
- Pfad: /
- Server section:
  - Host: öffentliche.ip.hierf (highlighted with a red box)
  - Login: user1e (highlighted with a red box)
  - SSH-Port: 22
  - RSA-/DSA-Schlüssel verwenden (ssh): [empty field]
  - Anmeldung über voreingestellten SSH-Schlüssel oder ssh-agent
  - Kerberos5 (GSSAPI) Authentifizierung
  - Übertragung der GSSAPI-Legitimation auf den Server
  - Proxy-Server für SSH-Verbindung verwenden
- Sitzungsart section:
  - In X2GoKDrive starten (experimentell)
  - Anwendung: [empty dropdown]
  - Befehl: [empty field]
  - remmina (highlighted with a red box)

Buttons at the bottom: OK, Abbrechen, Voreinstellungen

X2GoClient

Sitzung Einstellungen Hilfe

Sitzungs-ID: userle-50-1718969159\_stRremmina\_dp24

Server:

Login:

Display:

Startzeit:

Status:

Info: Using ZL

Info: Using ZL

Info: No suita

Info: Forward

Info: Forward

display ':0'.

Session: Sessi

2024'.

Info: Establish

Info: Using sh

Zeige Detai

OSUOSL Deb11 Stable

Remmina Remote Desktop Client <@jarvis-pi3>

Remmina Remote Desktop Client

RDP

Name	Group	Labels	Server	Plugin	Last used
WinXP			192.168.123.2	RDP	2009-10-16 - 09:04:46

Total 1 item.

X2GoClient

Sitzung Einstellungen Hilfe

Sitzungs-ID: userle-50-1718969159\_stRremmina

Server:

Login:

Display:

Startzeit:

Status:

Info: Using ZL

Info: Using ZL

Info: No suita

Info: Forward

Info: Forward

Info: Forward

display ':0'.

Session: Sessi

2024'.

Info: Establish

Info: Using sh

Zeige Detai

WinXP

RDP

Name	Group	Labels
WinXP		

Total 1 item.

WinXP <@jarvis-pi3>

### Windows-Anmeldung

Microsoft  
**Windows xp**  
Tablet PC Edition  
Microsoft

Copyright © 1985-2001  
Microsoft Corporation

Benutzername:

Kennwort:

Esc	°	^	1	"	3	4	%	&	7	(	)	=	0	?	~	Rück	Pos1	Bild auf
Tab	q	w	e	r	t	z	u	i	o	p	ü	*				←	Ende	Bild ab
Feststell	a	s	d	f	g	h	j	k	l	ö	ä	#				→	Entf	Druck
Umsch	>	u	y	h	b	n	m	,	.	;	'	#				↵	EinFa	Pause

DE 13:32 21.06.24

X2GoClient

Sitzung Einstellungen Hilfe

Sitzungs-ID: userle-50-1718969159\_stRremmina\_dp

Server: Re

Login:

Display:

Startzeit:

Status:

Info: Using ZL

Info: No suita

Info: Forward

Info: Forward

Info: Forward

display ':0'.

Session: Sessi

2024'.

Info: Establish

Info: Using sh

Zeige Detai

RDP

Name	Group	Labels
WinXP		

Total 1 item.

WinXP <@jarvis-pi3>

Papierkorb

Bluetooth-Umgebung

Mozilla Firefox

Eingabeaufforderung

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Dokumente und Einstellungen\Pepe Paradigma>ipconfig

Windows-IP-Konfiguration

Ethernetadapter Drahtlose Netzwerkverbindung:

    Medienstatus. . . . . : Es besteht keine Verbindung

Ethernetadapter LAN-Verbindung:

    Verbindungsspezifisches DNS-Suffix:
    IP-Adresse (Autokonfig.) . . . . . : 192.168.123.2
    Subnetzmaske. . . . . : 255.255.255.0
    Standardgateway . . . . . :

C:\Dokumente und Einstellungen\Pepe Paradigma>
```

Start | Eingabeaufforderung | 13:34

DE | 13:34 | 21.06.24



Info über Windows



Microsoft Windows  
Version 22H2 (Build 19045.2673)  
© Microsoft Corporation. Alle Rechte vorbehalten.

Das Betriebssystem Windows 10 Home und die zugehörige Benutzeroberfläche sind durch Marken- und andere rechtsabhängige bzw. bestehende gewerbliche Schutz- und Urheberrechte in den Vereinigten Staaten und anderen Ländern geschützt.

Dieses Produkt ist unter den [Microsoft-Softwarelizenzbedingungen](#) lizenziert für:  
Benutzername  
Unternehmensname

OK

```

C:\Users\userle> ipconfig

Konfiguration

Adapter Ethernet:

    Status . . . . . : Medium getrennt
    Subnetzspezifisches DNS-Suffix: stefanbaur.home

N-Adapter LAN-Verbindung* 1:

    Status . . . . . : Medium getrennt
    Subnetzspezifisches DNS-Suffix:

N-Adapter LAN-Verbindung* 2:

    Status . . . . . : Medium getrennt
    Subnetzspezifisches DNS-Suffix:

N-Adapter WLAN:

    Subnetzspezifisches DNS-Suffix: stefanbaur.home
    Subnetzlokale IPv6-Adresse . . : fe80::26dc:c2bc:eb48:43b%4
    Subnetzlokale IPv4-Adresse . . : 192.168.0.3
    Subnetzmaske . . . . . : 255.255.255.0
    Standardgateway . . . . . : 192.168.0.1
  
```

# Vorteil remmina

- Eine Anmeldung, mehrere Verbindungen – auch gleichzeitig
- Kann nicht nur RDP, sondern auch VNC sprechen
- VNC lässt sich auch auf Windows Home oder macOS nutzen, aber:
  - VNC ist
    - Meistens nicht verschlüsselt → SSH ändert das auf der WAN-Strecke
    - Deutlich träger als X2Go → X2Go ändert das auf der WAN-Strecke
- Dank X2Go muss Remmina nicht auf dem Client zur Verfügung stehen

# X2GoClient auf Stick

- Doppelinstallation möglich:
  - vom Stick bootfähige X2GoThinClientEdition
  - Windows-X2GoClient als Portable Application
  - Kernel, Initrd, Squashfs und Syslinux in FAT-Dateisystem
- Kann ich, wenn ich mit meinen Slides durch bin, und noch Zeit ist, noch schnell vorführen
- Ansonsten bitte unten am Stand vorbeischaun, dort können wir Live-Demos machen

# Nächste X2Go-Events

- Kommendes Wochenende (28.06.-30.06.):  
X2Go: The Gathering, Linuxhotel Essen
- Vermutlich:
- 19.09.-21.09. Kielux (nur Onlinevortrag)
- 28.09. LinuxDay.AT, Dornbirn
- 02.11. Tux-Tage (nur Onlinevortrag)
- Bestätigt: 07.11. IT-Kongress, Hochschule Neu-Ulm
- Wiki: <https://wiki.x2go.org/doku.php/events:start>



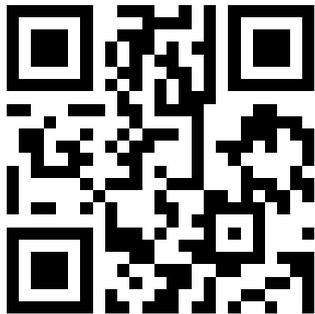
Event-Wikiseite

# X2Go lebt vom Mitmachen

- Helfer gesucht!
- X2Go kann immer zwei Dinge von euch brauchen:
  - Zeit/KnowHow – auch von Nicht-Programmierern!
  - Geld/Hardware/Dienstleistung: Man kann ...
    - über den orca e.V. (gemeinnützig) eine zweckgebundene Spende an X2Go leisten
    - eine der Firmen im Projekt mit einer konkreten Aufgabe (Bugfix, Feature Request) beauftragen

# Spenden/Aufträge

- Für Spenden haben wir mehrere WirWunder/Betterplace-Seiten (Events, Infrastrukturkosten, ...) direkt auf der Wiki-Startseite: <https://wiki.x2go.org>
- Firmen, die für Aufträge zur Verfügung stehen: <https://wiki.x2go.org/doku.php/0spnn5> (null-spnn-fünf)



Spendenlink



Liste der Supportfirmen



**Vielen Dank für das Interesse!**