Ein Client – ~~drei~~ viele Systeme



HNU IT-Kongress 2026

Stefan Baur, X2Go Lead Evangelist

Vorstellung Stefan Baur







Vorstellung WLB

- Die Württembergische Landesbibliothek (gegründet 1765 in Ludwigsburg als *Herzogliche Öffentliche Bibliothek*) ist heute
  - eine dem Ministerium für Wissenschaft, Forschung und Kunst Baden-Württemberg untergeordnete Behörde,
  - eine wissenschaftliche Universalbibliothek, und
  - eine der beiden Regionalbibliotheken Baden-Württembergs, zuständig für die Regierungsbezirke Stuttgart und Tübingen, sowie
  - zusammen mit der Badischen Landesbibliothek eine Archivbibliothek für Baden-Württemberg.
- Sie hat
  - über 6,4 Millionen Medieneinheiten im Bestand (Pflichtexemplare und zugekaufte/gestiftete Medien),
  - ca. 30.000 – 40.000 Leser/Benutzer, und
  - ca. 200 Mitarbeiter, davon grob 10 in der IT.

www.x2go.org

WLB-IT-Prinzipien

- „Open Source First“: Wenn es eine Open-Source-Lösung für ein IT-Problem gibt, wird diese bevorzugt, nicht nur aus Kostengründen, sondern auch zwecks Digitaler Souveränität.
- „Self-Hosting First“: Mit der selben Argumentation werden interne (Domäne, Fileservices, ...) wie externe Services (Internetauftritt, Lernplattform, Reservierungssystem) auch bevorzugt selbst gehostet. Eine Abschaltung/Sperre von Microsoft Entra (ehemals Azure AD) aufgrund irgendwelcher Sanktionen durch US-Behörden hätte also keine Auswirkung auf die Arbeitsfähigkeit der WLB-Mitarbeiter.
- „Public Money, Public Code“: Als Behörde wird die WLB größtenteils aus Steuergeldern finanziert, entsprechend fließen Eigenentwicklungen und Weiterentwicklungen an Open Source Software auch – wo immer möglich – an die Allgemeinheit zurück.

WLB-IT-Situation

- Die Serverlandschaft in der WLB ist so gut wie Microsoft-frei.
- Die IT-Abteilung arbeitet fast ausschließlich mit Linux-Clients.
- Die PCs für Bibliotheks-Benutzer sind ebenfalls fast ausschließlich Linux-Clients.
- Mitarbeiter-PCs sind dagegen momentan noch mit Microsoft Windows versehen:
  - Grund: Die aktuelle Kernanwendung sowie viele Fachanwendungen, die aktuell nur für Windows verfügbar sind (Der Wechsel der Kernanwendung auf eine webbasierte Lösung ist in Planung, wird sich aber über mehrere Jahre hinziehen).
  - Auch auf Windows sind aber die üblichen Open-Source-Anwendungen installiert, statt blind die Microsoft-Standardanwendungen zu verwenden (Firefox statt Edge, Thunderbird statt Outlook, etc.).
- Die Windows-Domäne wird über die Open-Source-Lösung „Samba“ realisiert.

Die verschleppte Migration

- Die Ablösung der Windows-7-Clients wurde mehrfach verschoben
- Ursprünglich war Windows 10 das Ziel, später dann Windows 11
- Windows 11 soll in komplett neue Domäne, um keine „Altlasten“ aus der W7-Welt mitzuschleppen → saubere Trennung, aber eben auch keine Vertrauensstellung o.ä.
- Viele Unsicherheiten beim Vorgehen führten zu realen oder befürchteten „Deadlocks“, so dass man die Umstellung nicht starten wollte, ohne eine Lösung für alle möglichen Varianten zu haben
- Ein bis kurz vor Schluss offener Punkt war, ob die Umstellung an einem Tag/Wochenende stattfinden kann, oder besser pro Abteilung/Gruppe erfolgt
  - Gefahr des Totalausfalls am nächsten Betriebstag

    vs.

  - Komplexität in der Übergangsphase (Wer kann welche PCs nutzen, Office-Versionskonflikte, ...)

Meetingräume/Wechselbüros

In Meetingräumen und Wechselbüros muss in einer Phase, in der sowohl Windows-7- als auch Windows-11-Nutzer dort arbeiten wollen, das „passende“ Windows bereitstehen.

- Eine Dual-Boot-Lösung wurde aber abgelehnt:
  - zu kompliziert/dem Anwender nicht vermittelbar
  - Umbooten dauert zu lange
  - doppelter Patch-Aufwand
- Active-Directory-Vertrauensstellung o.ä. war ebenfalls nicht gewünscht:
  - u.a wegen vermutetem „Versionschaos“ zwischen den Office-Versionen
  - somit kein Anmelden mit Account aus der jeweils anderen Domäne möglich

Homeoffice als Rettungsanker

- Normalerweise sehen sich Clients nicht untereinander (Client Isolation) → direkte RDP-Verbindungen von Client zu Client funktionieren also nicht.
- Aber: Alle Nutzer dieser Räumlichkeiten haben eine Homeoffice-Berechtigung.
- Homeoffice funktioniert in der WLB so, dass man sich über eine Zwei-Faktor-gesicherte Verbindung und über ein Gateway per RDP auf den Arbeitsplatzrechner verbindet (der dafür automatisch geweckt wird, wenn er noch nicht an ist).
- Dieses Gateway muss natürlich alle Clients erreichen können – aber es ist auch für eingehende Verbindungen aus dem internen Netz erreichbar!
  → Das wurde unsere Hintertür!

X2Go-ThinClientEdition

- zum Einsatz kam X2Go-ThinClientEdition in der Ausprägung „OpenboxMicroDesktop“ (OMD), also mit:
  - lokalem Desktop und
  - lokalem Browser (hier Firefox – aber Chrome oder Edge für Linux wären auch verfügbar gewesen)
- die X2Go-ThinClientEdition ist OpenSource
  - man kann und darf also Anpassungen daran vornehmen
  - das wurde hier weidlich ausgenutzt ;-)

Anpassung: Konfiguration/Theming

Theming und Konfiguration lassen sich ohne Eingriff ins Image, rein per Bootparameter und über Konfigurationsdateien anpassen:

- WLB-Logo als Startknopf
- eigenes Hintergrundbild für Desktop (WLB-Neubau-Fassade)
- eigenes Hintergrundbild für den X2GoClient (zeigt kompakte Bedienungsanleitung an)
- angepasste Startseiten für den lokalen Firefox-Browser (Intranet und Videokonferenz-Plattform → ViKo über RDP taugt nicht)
- unterschiedliche Parameter (TLS-SEC) für Verbindungen zu W7 und W11

Besonderheit: Die Konfigurationsdatei war nicht statisch auf dem Server hinterlegt, sondern wurde dynamisch generiert, aus DHCP/DNS-Daten:

- deutlich geringerer Aufwand, als einen kompletten X2Go-Session-Broker aufzusetzen
- trotzdem flexibel – kein manueller Eingriff notwendig, wenn neue Clients hinzukamen

Anpassung: Software

Für die Anpassung, das Homeoffice-Gateway zu nutzen, muss man in den Buildprozess des Images eingreifen – das geht aber sehr einfach, indem man seine zusätzlichen Dateien/Ordner in den Unterordner „patch“ kopiert, bevor man den Build startet:

- Client für die Verbindung zum Homeoffice-Gateway mit ins Image packen
- Pfad zur lokal gespeicherten 2FA-Schlüsseldatei hinterlegen

Man kann das natürlich auch ordentlich machen, indem man sich seinen eigenen Git-Branch der X2Go-TCE anlegt, aber in den meisten Fällen wird das nicht notwendig sein.

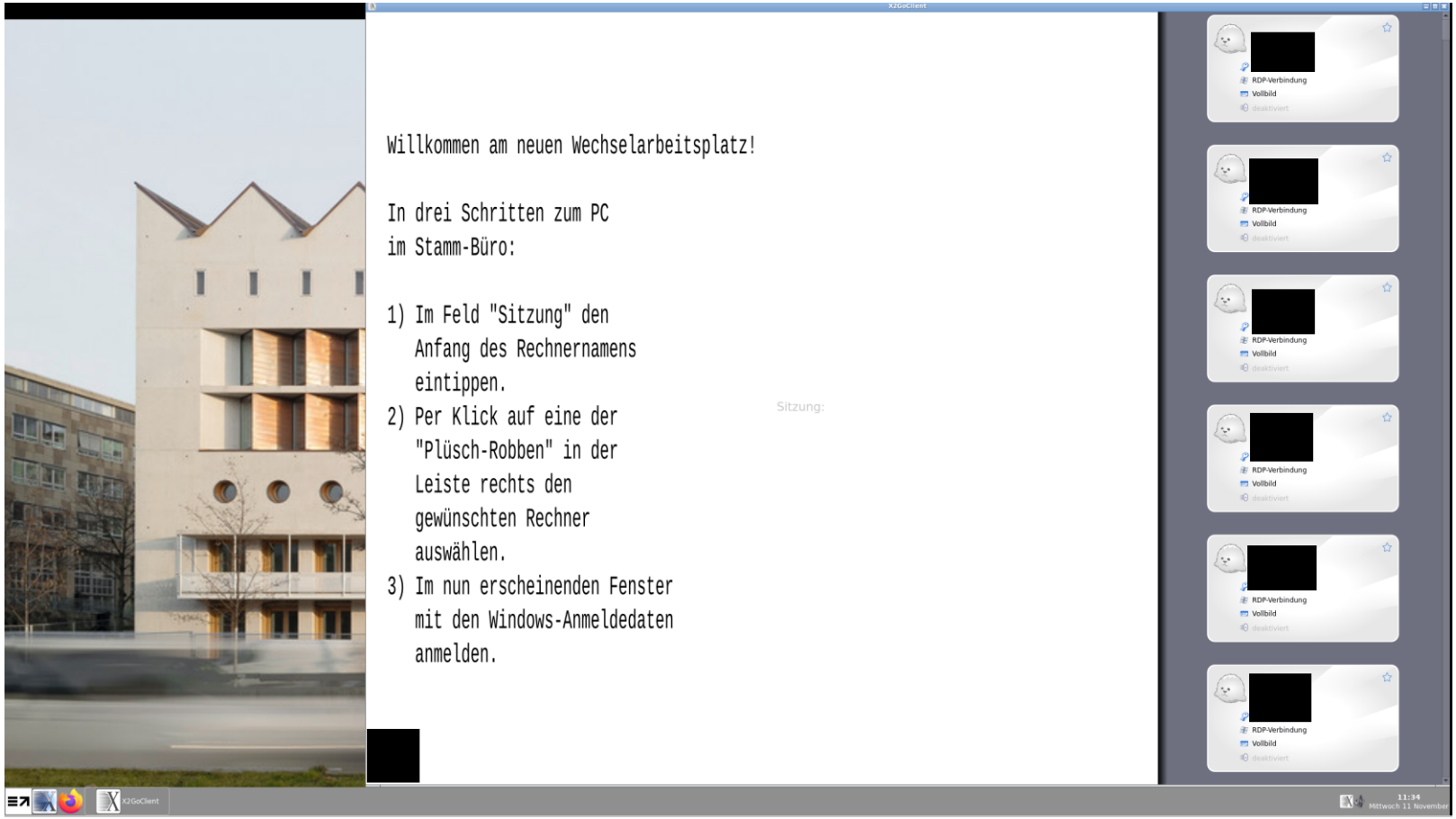
Auf dem jeweiligen Client war ebenfalls etwas Vorarbeit notwendig:

- manuell eine Partition auf der Festplatte anlegen und beim formatieren (DOS oder ext2/3/4) mit passendem Label (Partitionsname) versehen, auf den das Image beim Start matcht, wenn es seine Konfigurationsdateien sucht
- individuelle 2FA-Schlüsseldatei für diesen Client in der neuen Partition hinterlegen (wird also nicht unverschlüsselt übers Netzwerk übertragen) – individuelle Schlüsseldateien deswegen, damit man einzelne Clients auch schnell zentral stilllegen kann, wenn ein Schlüssel kompromittiert würde

Boot übers Netzwerk

- es gibt bereits einen DHCP-Server im Netz, der auch PXE-Netzwerkboot unterstützt
- in dessen Konfiguration klinken wir uns ein
- Erkennung der Clients anhand der MAC-Adresse → nur die Clients in der Liste starten übers Netz die X2Go-TCE
- die 2FA-Schlüsseldatei muss natürlich lokal auf dem Client gespeichert sein
- durch den Netzwerkboot vermeiden wir den Aufwand, immer wieder Updates auf die Clients ausrollen zu müssen – ein Image-Update auf dem Server schlägt beim nächsten Neustart auf alle X2Go-TCE-Instanzen durch

Screenshot X2Go-TCE @ WLB



Das waren sie also,

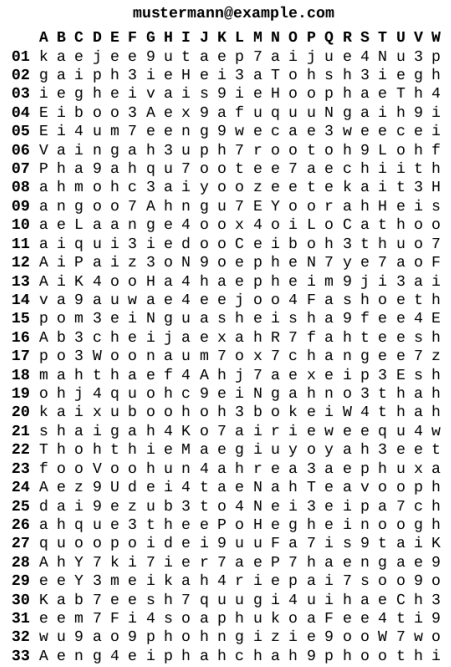


unsere drei ~~Probleme~~ Systeme ...

Passwortübernahme

- Nächstes Risiko: Was, wenn die automatisierte Passwortübernahme aus der alten in die neue Domäne nicht möglich ist/nicht funktioniert?
- Man müsste grob 200 Mitarbeitenden auf einen Schlag neue Passworte zukommen lassen
  - Wie?
    - Per Anruf von bekannter Rufnummer?
      → zu wenig IT-Mitarbeiter, zu unsicher (Mehr-Personen-Büros)
    - Per Brief vorab?
      → zu wenig Vorlauf, zu verwirrend für nicht-IT-affine Mitarbeitende
    - Per Ausdruck auf Netzwerkdrucker?
      → zu unsicher, selbst mit „Zahlenmeer“, zu zeitaufwendig

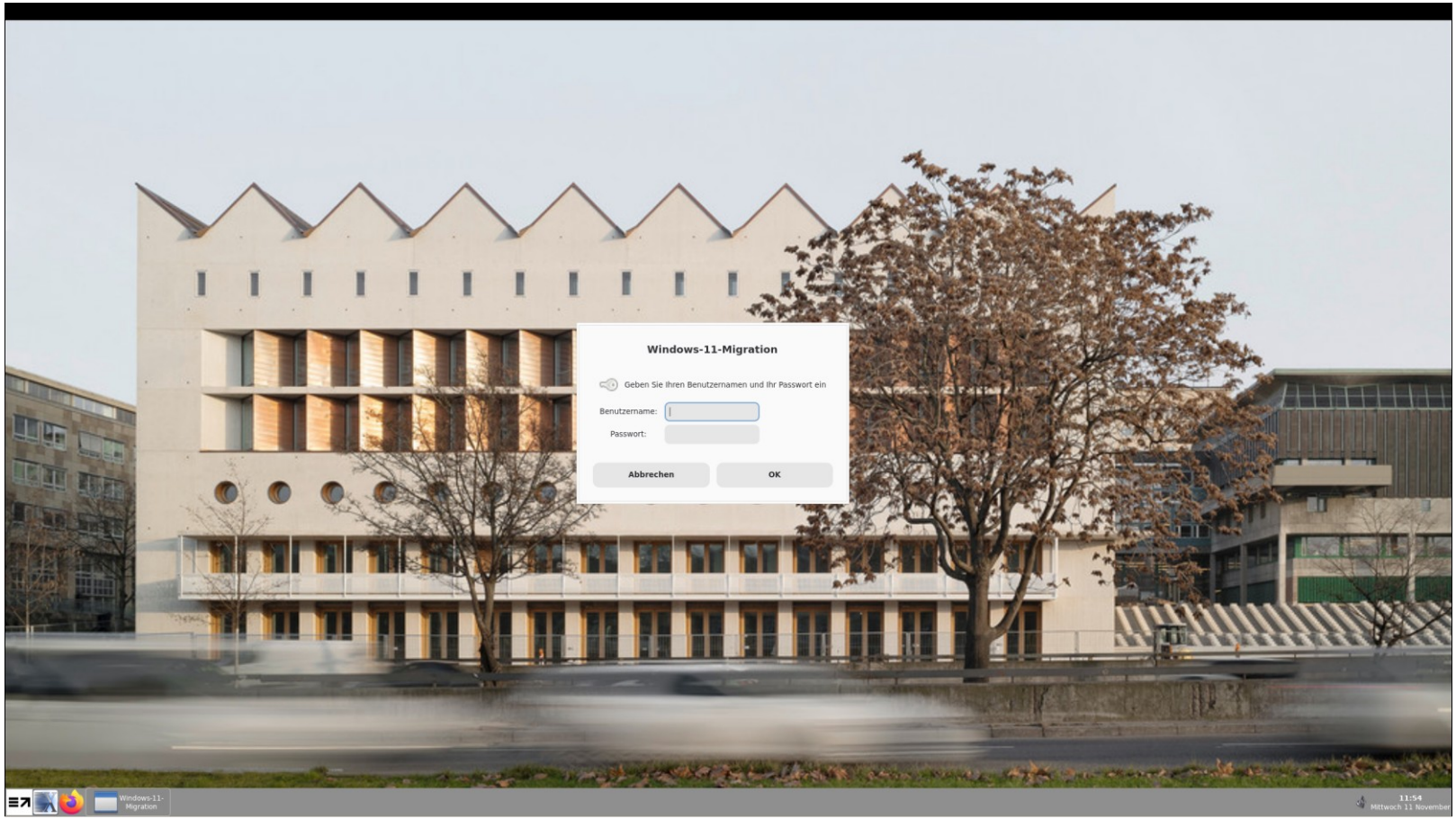
    → alles nicht umsetzbar
- Stattdessen Fallback mit angepasster X2Go-ThinClientEdition
  - X2GoClient wird nicht gestartet
  - an seiner Stelle startet ein WLB-intern entwickeltes Tool, welches die aktuellen Anmeldedaten abfragt



Passwortübernahme – Ablauf

- System wird per Wake on LAN geweckt
- Clients sind so eingestellt, dass sie bei WOL vom Netzwerk, statt von der SSD booten
- X2Go-TCE-Desktop startet, zeigt aber nicht X2GoClient, sondern unser selbstgeschriebenes Tool
- Mitarbeiter tippt Benutzername und Passwort in die Eingabemaske unseres Tools ein, beides wird im RAM gespeichert
- Im Hintergrund (ohne weitere Benutzer-Interaktion) passiert folgendes:
  - Mit den gespeicherten Daten wird versucht, eine Verbindung zur alten Windows-7-Domäne aufzubauen. → Wenn das funktioniert, war es das richtige Passwort.
  - Dann wird von einem Netzwerkpfad das Initialpasswort für die Windows-11-Domäne aus einer Datei gelesen, die anschließend gelöscht wird.
  - Die Verbindung zur Windows-7-Domäne wird getrennt.
  - Nun folgt die automatische Anmeldung an der Windows-11-Domäne mit Benutzername (identisch in W7 und W11) und Initialpasswort.
  - Die Aufforderung zum Passwortwechsel seitens des ADs wird vom Tool mit dem Initialpasswort und anschließender zweimaliger Übergabe des gespeicherten Passworts aus der Windows-7-Domäne beantwortet.
  - Anschließend erfolgt ein Shutdown des PCs, um das Passwort nicht länger als nötig im RAM zu halten.
- Der nächste, manuelle Start (per Knopfdruck durch den Mitarbeiter) startet das lokal installierte Windows 11.

Screenshot Passwortübernahme



Migration erfolgreich!

- im Endeffekt wurde es ein relativ harter Cut, aber es gab Ausnahmen:
  - es gab einige Pilotuser in einzelnen Abteilungen/Gruppen
  - der größte Teil wurde an einem Wochenende umgestellt:
    - grob zweieinhalb Tage Aufwand, beginnend an einem Freitagnachmittag
    - Arbeiten gingen gut voran, für Montag vorgesehene Tätigkeiten wurden bereits am Sonntag erledigt
  - einzelne Mitarbeiter/Gruppen mussten länger auf W7 ausharren, u.a. aufgrund von Abhängigkeiten zu externen Dienstleistern bei spezieller Hardware
- das Passwort-Übernahme-Tool wurde nicht benötigt
- die Lösung für den Meetingraum fand Anklang und ist bis heute im Einsatz
  - war eigentlich nur als Übergangslösung geplant
  - Mitarbeiter empfinden es aber als Vorteil, sich nicht erst am Arbeitsplatz abmelden zu müssen, sondern ihren Desktop ins Meeting „mitnehmen“ zu können
  - nach dem selben Prinzip funktionieren nun auch zwei Plätze innerhalb der IT-Abteilung, allerdings mit lokal gespeichertem Image, nicht per Netzwerkboot → verwenden Auto-Update-Mechanismus der Disk-basierten TCE

Migrationsbeschwerden?



Da gibt’s doch was von …

... Ratiopharm? Nein, aber von X2Go!



Dann kam der Sommer ...

Die Hitzewelle 2026 sorgte dafür, dass die Temperaturen in den Gebäuden, die nicht über eine Klimatisierung verfügen, massiv anstiegen, vor allem in den oberen Stockwerken.

- Mitarbeiter wurden teilweise ins Homeoffice geschickt
- komplette IT-Abteilung sitzt in nicht klimatisiertem Gebäude, im 3. Stock → Idee:
  - in untere, kühlere Stockwerke ausweichen lassen
  - auf normale Mitarbeiter-Plätze, die gerade frei sind (Urlaub, Teilzeit, etc.)
  - dort X2Go-TCE booten und die „Hintertür“ über das Homeoffice-Gateway nutzen

Damit sind wir beim vierten System – dem Zugriff auf Linux-Desktops in der IT.

Erschwerte Bedingungen

- für den Zugriff ins IT-Netz gelten höhere Sicherheitsanforderungen
- deswegen sind die IT-PCs auch nicht in der Auswahlliste enthalten, die am normalen X2Go-ThinClient für die Mitarbeiter angezeigt wird
- auch die 2FA-Schlüsseldatei kann aus Sicherheitsgründen nicht auf dem Client gespeichert werden (wenn das Windows „gekapert“ würde, hätte der Angreifer Zugriff auf die Schlüsseldatei, könnte also ins IT-Netz eindringen und größeren Schaden anrichten)
- daher anderes 2FA-Verfahren, plus individueller Konfigurationsdatei auf USB-Stick – und zwar nur der Konfiguration für den jeweiligen IT-Mitarbeiter, nicht für alle IT-PCs
- getestet, funktioniert → und kommt vielleicht nächsten Sommer zum Einsatz
- Der Umzug ins renovierte, klimatisierte Gebäude verschiebt sich nämlich um mindestens ein Jahr. :‘(

Neue Zeiterfassung

Es soll ein neues, webbasiertes Zeiterfassungssystem ausgerollt werden

- Ziel: weg vom Papier – auch bei Aushilfskräften
- Aushilfskräfte haben in einigen Fällen gar keinen Account an einem PC, weil sie für ihre Tätigkeit keinen PC brauchen
- man kann für alle Aushilfen zukünftig AD-Accounts anlegen (oder einen Gruppenaccount anlegen, aber das ist aufgrund des geteilten Passworts „Pfui“)
  → dann muss aber auch irgendwo ein neuer, W11-tauglicher PC hin
- oder man gibt Ihnen irgendwo Zugang zu einem System, das ohne Anmeldung einen Browser starten kann (die Anmeldung am Zeiterfassungssystem erfolgt über einen separaten Account, nicht per SSO)
  → durch die W11-Umstellung haben wir so einige alte PC-Hardware übrig, wir brauchen also keinen neuen PC „verschwenden“, wenn wir nur Linux starten müssen
- X2Go-TCE-OMD kann natürlich auch einfach nur einen Browser mit voreingestellter Startseite laden, statt des X2GoClients, wenn man das will …

Und damit sind wir bei System fünf.

Wo geht die Reise hin?

Weitere mögliche Einsatzszenarien in der WLB:

- Die Benutzerplätze sind momentan Linux-Fat-Clients; beim nächsten größeren Update könnte man eine Umstellung auf X2Go-TCE und einen X2Go-Terminalserver (oder zumindest auf ein Live-Linux) ins Auge fassen, um Update-Aufwände zu reduzieren und die vorhandene Hardware länger und damit nachhaltiger nutzen zu können.
- Analog des für die Zeiterfassungs-Terminals evaluierten Systems einen Browser im Fullscreen-/Kiosk-Modus anzeigen und für webbasierte Self-Service-Kiosk-Lösungen und Infoscreens verwenden; Mit angeschlossenen Lautsprechern könnte man sogar Durchsagen per Livestream-Audio machen.
- Vielleicht, irgendwann in ferner Zukunft, die Mitarbeiter-Plätze ebenfalls damit statt mit Windows betreiben – wenn sich die letzten paar unvermeidbaren Windows-Anwendungen per Windows-/Citrix-Terminalserver bereitstellen lassen.

Nächste X2Go-Events

Leider abgesagt:

- 13.11.2026 – 14.11.2026 Tux-Tage Online
  (Es wird aber Videos „aus der Konserve“ geben)

Noch nicht angemeldet/noch keine Zusage:

- 28.03.2027 – 29.03.2027 Chemnitzer LinuxTage
- 02.04.2027 – 03.04.2027 Grazer LinuxTage

Termin/Ort noch offen:

- „X2Go: The Gathering/The Spread 2026“
- orca e.V. Jahreshauptversammlung 2026

Wiki: https://wiki.x2go.org/doku.php/events:start

Event-
Wikiseite

X2Go lebt vom Mitmachen

- Helfer gesucht!
- X2Go kann immer zwei Dinge von Ihnen 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!
Mehr Infos und Q&A am Stand!

Spendenlink

Liste der Supportfirmen