



Vorstellung

Stefan Baur

- Vormalig: über 10 Jahre bei einem Geldinstitut
 - Schwerpunkttätigkeit dort:
 - IT-Security
 - Virenschutz
- Aktuell: *Der Mann mit den 4 Hüten*
 - X2Go-Projektmanager
 - X2Go Lead Evangelist
 - X2Go Event Planner
 - Firmenchef, BAUR-ITCS UG (haftungsbeschränkt)

Events!



X2Go: The Gathering 2016 in Essen – Anmeldeschluss 11.07.16 – 1 Monat noch!



Vor 3 Jahren



05.06.2013



Snowden

Die Snowden-Enthüllungen

TOP SECRET//SI//ORCON//NOFORN

Special Source Operations

PRISM/Over

The SIGAD Used M

Over

Ap

TOP SECRET//SI//ORCON//NOFORN

Special Source Operations

(TS//SI//NF) Int

U.S. as World's Telec

- Much of the world's communications flow through the U.S.
- A target's phone call, e-mail or chat will take the **cheapest** path, **not the physically most direct** path – you can't always predict the path.
- Your target's communications could easily be flowing into and through the U.S.

International Internet Regional Bandwidth Capacity in 2011
Source: Teleography Research

TOP SECRET//SI//ORCON//NOFORN

TOP SECRET//SI//ORCON//NOFORN

Collection Details

PRISM

What Will You Receive in Collection Surveillance and Stored Comms)?
It varies by provider. In general:

il
– video, voice
as
ns
d data

ransfers
o Conferencing
ications of target activity – logins, etc.
ie Social Networking details

cial Requests

eb page:

TOP SECRET//SI//ORCON//NOFORN

Google! Skype paltalk.com YouTube AOL mail &

PRISM Collection Provider

Apple (added Oct 2012)
AOL 3/31/11
Skype 2/6/11
YouTube 10

PRISM Program Cost: ~ \$20M per year

2007 2008 2009 2010 2011 2012 2013

TOP SECRET//SI//ORCON//NOFORN

Edward Snowden (Bildlizenz: CC-BY 3.0, Laura Poitras/Praxis Films)



Und alle so:

AAAAAaaaaaaah!

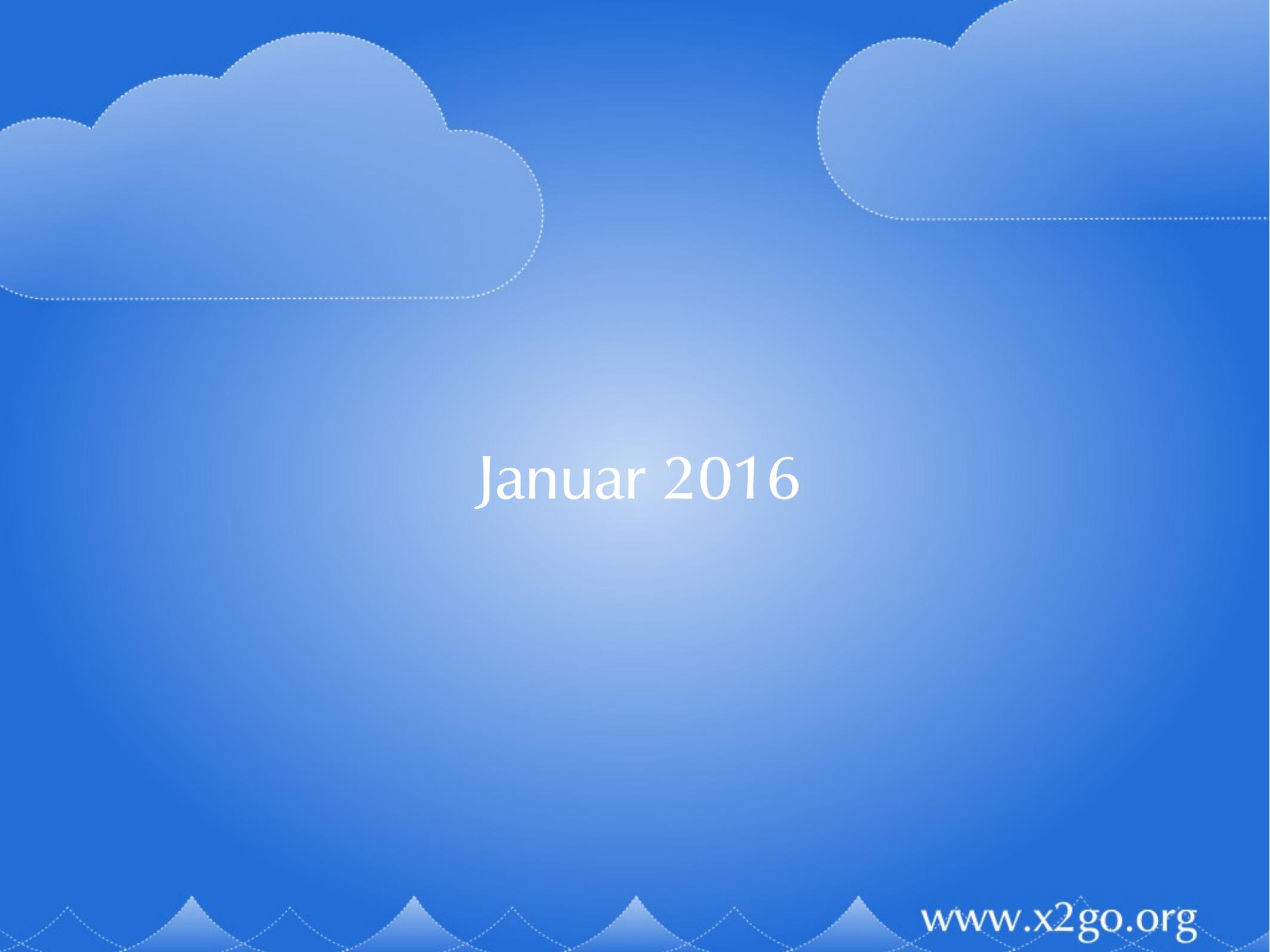




Ein Weckruf

Und alle hatten Angst.

- *Der Datenklau geht um.*
 - Aber nur Angst, ausgespäht zu werden
 - Ja, wenn die privaten Nacktbilder plötzlich nicht mehr so privat sind, ist das ärgerlich und peinlich.
 - Konstruktionspläne, Firmeninterna, Patientendaten, da wird's dann aber auch noch teuer.
 - Angst vor *Datengeiselnahme* damals: Fehlanzeige



Januar 2016



Ransomware



In The Wild

Neue Situation

- *Aus kopieren* wird nun wirklich *stehlen*
- Benutzer hat keinen Zugriff mehr
- Lösegeld zahlen hilft auch nicht immer
 - Teilweise schlampig programmierte Trojaner
 - Teilweise nicht mehr erreichbarer Erpresser
- Infektionswege:
 - Drive-By-Downloads/Zero-Day-Exploits
 - E-Mail-Anhänge (Fake-Rechnungen etc.)



ReCoBS

ReCoBS steht für ...

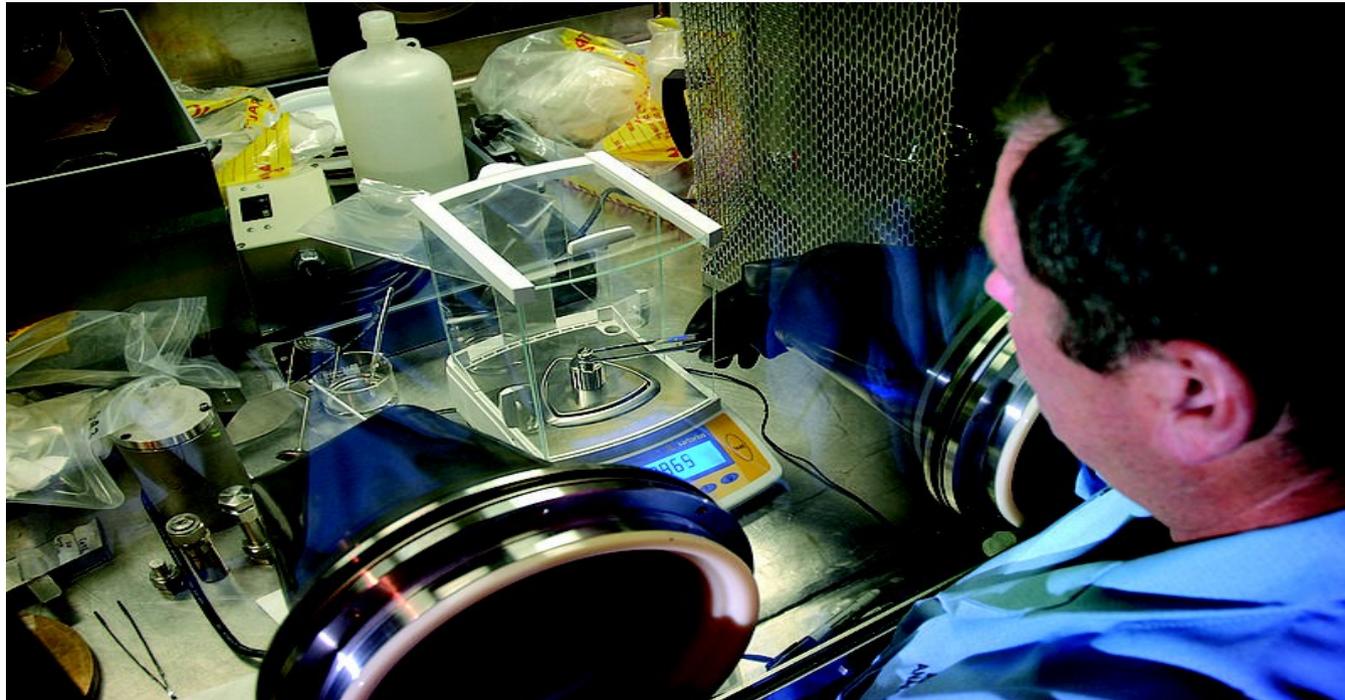
- Remote
- Controlled
- Browsers
- System

ReCoBS vs. UTM/Firewall/Antivirus

- Was macht ein ReCoBS anders als eine (Consumer-)Firewall, ein Virens Scanner, eine UTM-Appliance?
 - Nicht nur „Du kommst hier nicht rein“, sondern auch „Du kommst hier nicht raus“
 - *kein Scan, keine Signaturen, keine Heuristik*
 - Keine *diagnostische Lücke*, keine Chance für Zero-Days
 - Keine Fehlalarme
 - Internet nur per *Guckkasten*
 - Alle aktiven Inhalte werden in der DMZ ausgeführt

Das ReCoBS-Prinzip

Guckkasten, Manipulatorkiste = GloveBox



Bildlizenz: CC-by-2.0; Autor: Idaho National Laboratory



History ...

LINUX GRAPHICAL WALL

- 30. August 1999
- Früheste mir bekannte Erwähnung der Idee als
 - *Graphical Firewall* oder
 - *LINUX GRAPHICAL WALL*
- im *Firewall Handbuch für LINUX 2.0 und 2.2* von Guido Stepken

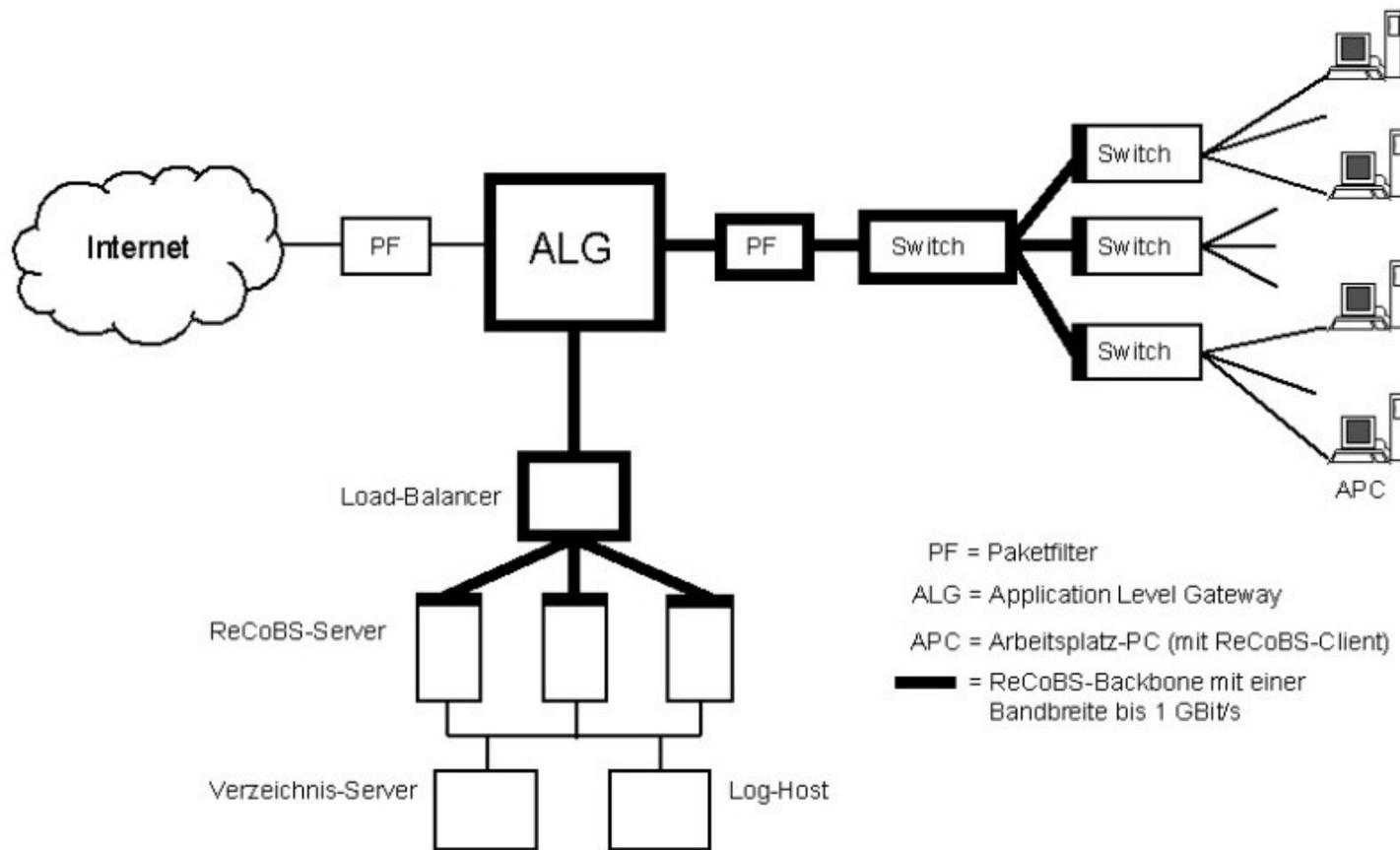
Weitere-ReCoBS-Vorläufer

- Oktober/November 2001 – ehemaliger Arbeitgeber installiert NT4 WTS+Citrix (im selben Netz wie alle Clients – die noch unter OS/2 liefen)
- Jahreswechsel 2005/2006 – ehemaliger Arbeitgeber *rüstet auf*:
 - Redundanz und Virtualisierung
 - Wechsel zu W2K3/Citrix und eigener Domäne (AD)
 - Firewall/DMZ
 - Proxy mit Virens Scanner (unter Linux)

2006 – ReCoBS is born

- 3-teilige Artikelreihe *Aktive Inhalte* in der <kes> (Zeitschrift für Informations-Sicherheit des BSI)
 - Teil 1 in 2005#5
 - Teil 2 in 2005#6 – enthielt schon ReCoBS-Andeutungen
 - Teil 3 in 2006#1 – *Remote-Controlled Browsers System – Sichere und bequeme Nutzung von aktiven Inhalten*
- BSI-Grundschrift-Handbuch, M 4.365 Nutzung eines Terminalservers als grafische Firewall

ReCoBS



ReCoBS-Skizze aus <kes> 2006#1

Geldinstitut != IT-Firma

- Ein Geldinstitut kein IT-Dienstleister und wird so ein System nicht vermarkten.
- Das Konzept ist kein Geschäftsgeheimnis mehr.
- Ein Klein-Anwender (Arzt, Rechtsanwalt, Notar, Steuerberater, ...) wird kein Geld für einen Windows-TerminalServer mit Citrix ausgeben.
- Linux ist sowieso der sicherere Ansatz.
 - Eigenbau in klein, sicher, günstig.
 - Vermarktung/Probelauf im Nebenerwerb

25.01.2007

- erster Mailversand vom Prototyp der *elektronischen GloveBox*
- damals noch namenlos („Surf-Server“)
- Remote Applications → Seamless Mode
 - einzelne Apps integrieren sich in Windows-Desktop
 - über NoMachine NX (2-User-Free-as-in-Beer-Lizenz)
 - Nur einzeln startbar (neue Anmeldung pro App), oder über Starter, der als Host-Anwendung läuft (Xdialog/Kdialog → Support-Albtraum bei Upgrade)

Lessons learned (2007-2009)

- Als VM-Gast mit VMware Server auf einem W2K3-Host, der viel CPU und RAM für die Praxissoftware-Datenbank und -Anwendung braucht, nicht sonderlich performant
- An zusätzliche Firewall-VM nicht zu denken (Performance geht noch mehr in den Keller)
- Hickhack mit den IT-Dienstleistern für die Praxissoftware

Folgerungen

- Eigene Server-Hardware ist Pflicht – und muss zuverlässig sein (möglichst ohne bewegliche Komponenten → Lüfterlos, heute auch SSD)
- Dort kann man virtualisieren, wie man lustig ist
- Auch eine Firewall-VM geht dann
- Nie, nie, nie als Vor-Ort-Dienstleister auftreten:
 - immer den vorhandenen einbinden
 - one face to the customer
 - kein „der andere ist schuld, dass \$FOO nicht geht“

Dezember 2009

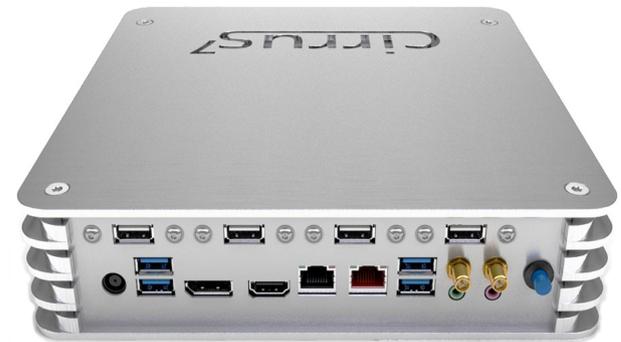
- Neue Generation, nun auf dedizierter Hardware
- Wechsel zu FreeNX für höhere Userzahl
- Namensfindung: *elektronische GloveBox*
- 3 OS-Partitionen auf Host (von IBM inspiriert):
Wartung, Produktion, Fallback
- Anlaufschwierigkeiten
 - Erster Blick: „Ah, Firewall.“ → „Hab’ ich schon.“
 - Sehr beratungsintensives Produkt

X2Go

- Juli 2010 – März 2011
 - FreeNX wird immer mehr zum Dead-End
 - Pakete offiziell nur noch für Ubuntu
 - Neuere Releases nur noch schleppend bis gar nicht
 - „schleichend“ beginnendes X2Go-Interesse
- Februar 2012 – April 2012:
 - kommerzielles Sponsoring der X2Go-Entwicklung
 - Ergebnis: X2Go-Published-Application-Feature
 - X2Go nun analog Citrix nutzbar

elektronische GloveBox

- heutige Version: Hardware aus Esslingen
- es wird nur noch *gemalt*
 - Ausführung passiert zentral
 - PC weiß nicht, was er da malt
 - Damit sicheres Internet, selbst mit Windows XP
- zwischen DSL-/Kabel-Router und LAN einstecken (DSL-/Kabel-Router ist die 1. Firewall aus dem ReCoBS-Bild), Clients einrichten, fertig



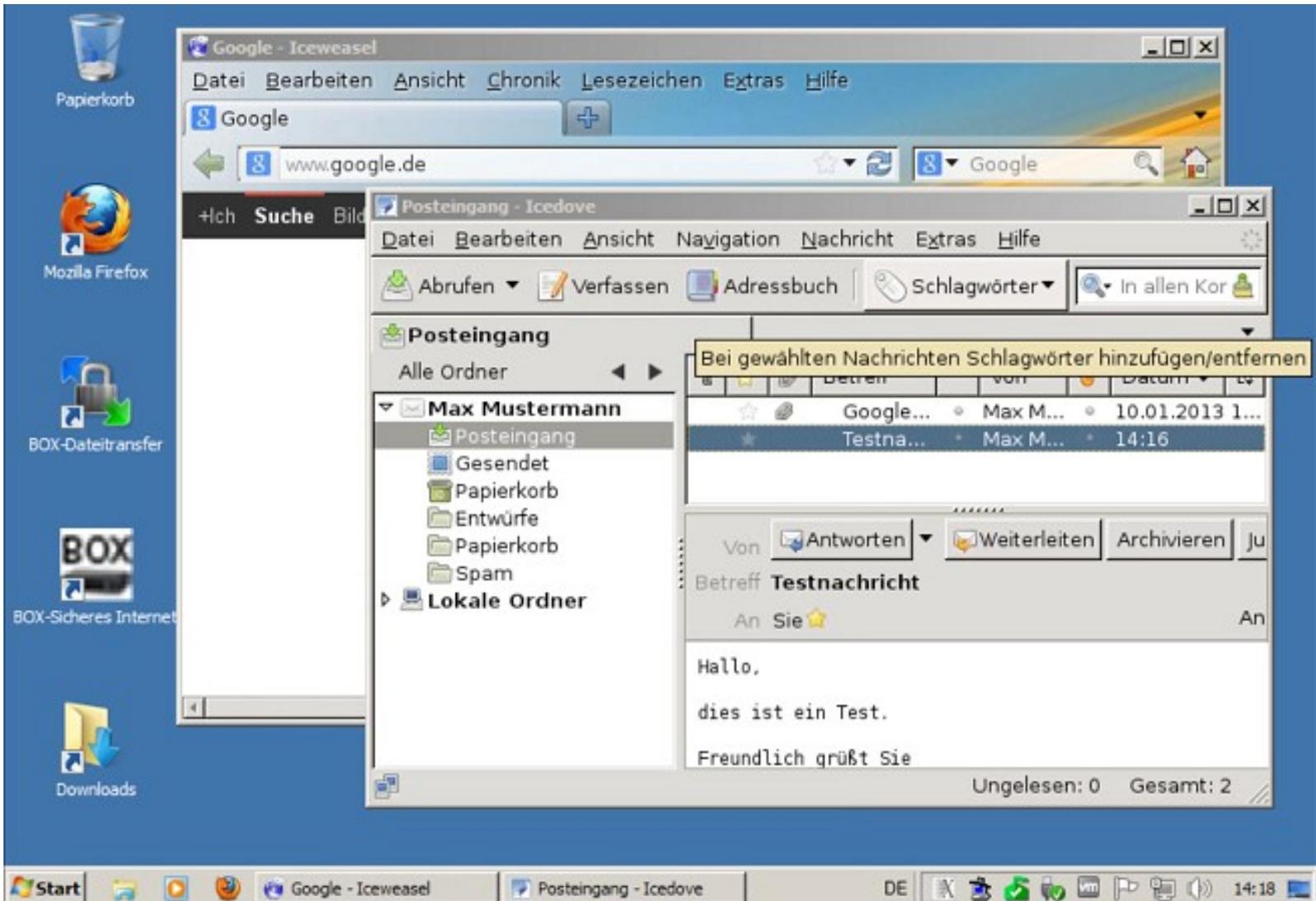


Screenshots

elektronische GloveBox

The screenshot displays a Windows 7 desktop environment. The primary focus is a web browser window titled 'Funktionsweise - BAUR-ITCS UG (haftungsbeschränkt) - Iceweasel'. The browser's address bar shows the URL 'www.baur-itcs.de/10-elektronischeglovebox/20-funktionsweise'. The page content includes the header 'BAUR-ITCS UG - Ihr Spezialist für sicheren Datenverkehr.' and a navigation menu with items like 'Elektronische GloveBox', 'Servermodelle', 'Downloads', 'Demos', 'Über uns', and 'Kontakt'. The main content area features a diagram titled 'Wie funktioniert die elektronische GloveBox?' with the subtitle 'Die Box surft stellvertretend für Ihren PC:'. The diagram illustrates the data flow: a PC sends input to a 'GloveBox', which then connects to a 'Router' and the 'Internet'. Two numbered steps are provided: '1. Ihr PC leitet Tastatur- und Mauseingaben an die GloveBox weiter.' and '2. Als Antwort erhält er ein Abbild der Internetseite.' The desktop also shows a 'Downloads' folder icon, a 'viernull' folder, and a taskbar with various application icons. A file explorer window is open, showing the contents of the 'Downloads' folder, including files like '.x2go', '.x2goclient', and 'Desktop'.

elektronische GloveBox





Live-Demo GloveBox



User- Feedback

Benutzerwünsche 1

- Router mit Auto-Disconnect trotz Flatrate
- Netzscan – wer ist im LAN online
- Anbindung an FritzBox für Faxversand/-empfang
- GDI-Drucker-Support
 - Er muss nur am Windows-PC angeschlossen sein.
 - Ja, das geht generisch und ohne Samba-Freigabe.
- Zeitsteuerung (Feiertage!)
- Windows-VM/zentrale Windows-Updates

Benutzerwünsche 2

- selektiver Proxy-Bypass, weil eine Labordaten-Web-Anwendung so beschungeschickt hingefrickelt ist, dass sie nicht proxyfähig ist
- Text-Chat, damit man den Techniker auch erreicht, wenn er in der Besenkammer (*hust* Serverraum) oder im Keller im Funkloch steht
- Nutzungsmöglichkeit für halb defekte Hardware
- Watchdog für Host und Router
→ schaltbare Steckdosenleiste mit Timer

Benutzerwünsche 3

- VPN (OpenVPN)
 - Site-to-Site
 - Roadwarrior
- VPN-Router-Uplink zu KV-SafeNet
- Anbindung von Mobilgeräten
 - Eigentlich nicht sinnvoll möglich
 - Es fehlt an
 - X2GoClient für Android/iOS
 - Linux-Apps, die für kleine Touchscreens tauglich sind

Erfolg!

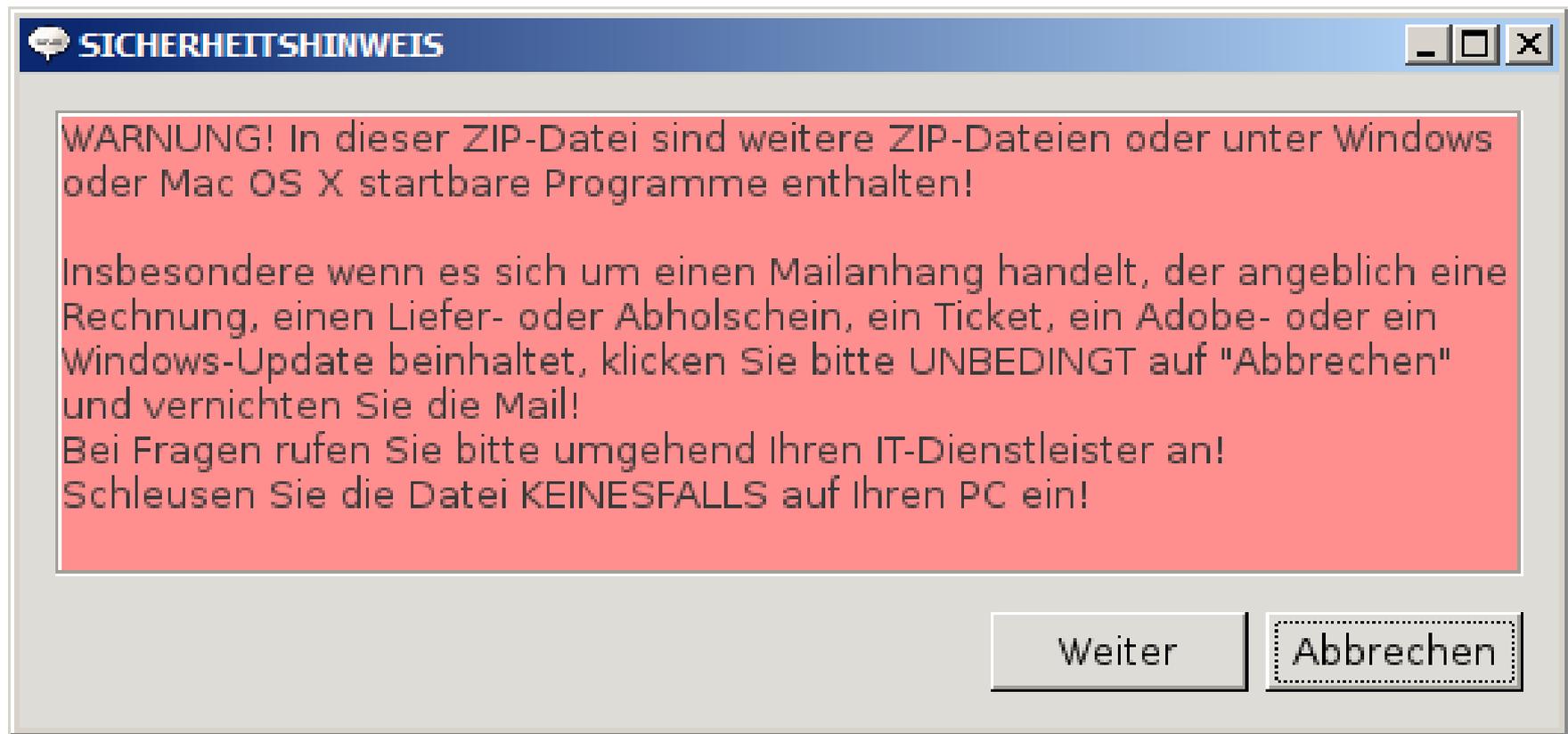
- Genau zwei Infektionen nach schwerem Benutzerfehlverhalten („set brain=off“)
 - in über 6 Jahren
 - bei grob 50 Installationen
 - mit im Schnitt 4-5 Usern pro Installation
- Erfolgreiche Schadenseindämmung
 - Nur jeweils betroffener PC neu zu installieren
 - Kein Datenverlust
 - Kein Datenabfluss

Was war passiert?

- Mailanhang à la rechnung.pdf.exe.zip
- Geht nach entpacken natürlich nicht auf, da kein WINE installiert
- Benutzer schleust ins LAN ein, anstatt zu sagen „Oh, kaputt!“ und den Support anzurufen
- Malware-Loader läuft lokal los - kann aber seinen Schadcode nicht per HTTP nachladen
- Ausbruch gestoppt!

Neue Schutzmaßnahme

- Popup bei gepackten Mailanhängen mit ausführbarem Inhalt





Live-Demo Installation



X2Go- Projekt

Freiwillige gesucht!

- Frauen besonders willkommen!
- Bei uns geht es *nicht* zu wie auf der Linux-Kernel-MailingListe!
- Trotzdem bisher kaum weibliche Beiträge aufgefallen → Schade!
- Einer der wenigen weiblichen Beiträge kam dafür gleich von der NASA. ;-)

Uns fehlen ...

- Übersetzer
 - Vor allem für *exotischere* Sprachen abseits von
 - Englisch
 - Französisch
 - Italienisch
- Wikiadmins
- Mailinglistenadmins
- Bugtracker-Admins
- Programmierer

Man hilft uns auch mit ...

- Kommerziellen Aufträgen
 - Feature Requests/Feature Enhancements
 - Wartungs- und Supportverträge
- Sponsoring
 - Finanziell
 - *Naturalien* (Hardware)
- Goodiekauf
 - Erhaltene Werbegeschenke, die wir zugunsten des Projekts verkaufen



Vielen Dank!