Windows-Systeme vor Ransomware schützen – mit Linux und X2Go

Vorstellung

Stefan Baur

- Vormals: 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-Planer
  - Firmenchef, BAUR-ITCS UG (haftungsbeschränkt)

Events!

X2GoHackTrain / X2Go: The Gathering

„Polymorphe Präsentation“

- Dieser Vortrag *mutiert* ;-)
- Gleicher Vortragstitel schon bei:
  - TÜBIX 2016
  - IT-Kongress 2016
  - LinuxDay.AT 2016 (Video verfügbar)
  - Chemnitzer LinuxTage 2017 (Video verfügbar)
- Aber immer leicht abweichende Folien und aktuelle Ergänzungen
- Trotzdem heute das letzte Mal!

Vor grob
4 Jahren ...

05.06.2013

Snowden

Die Snowden-Enthüllungen

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

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

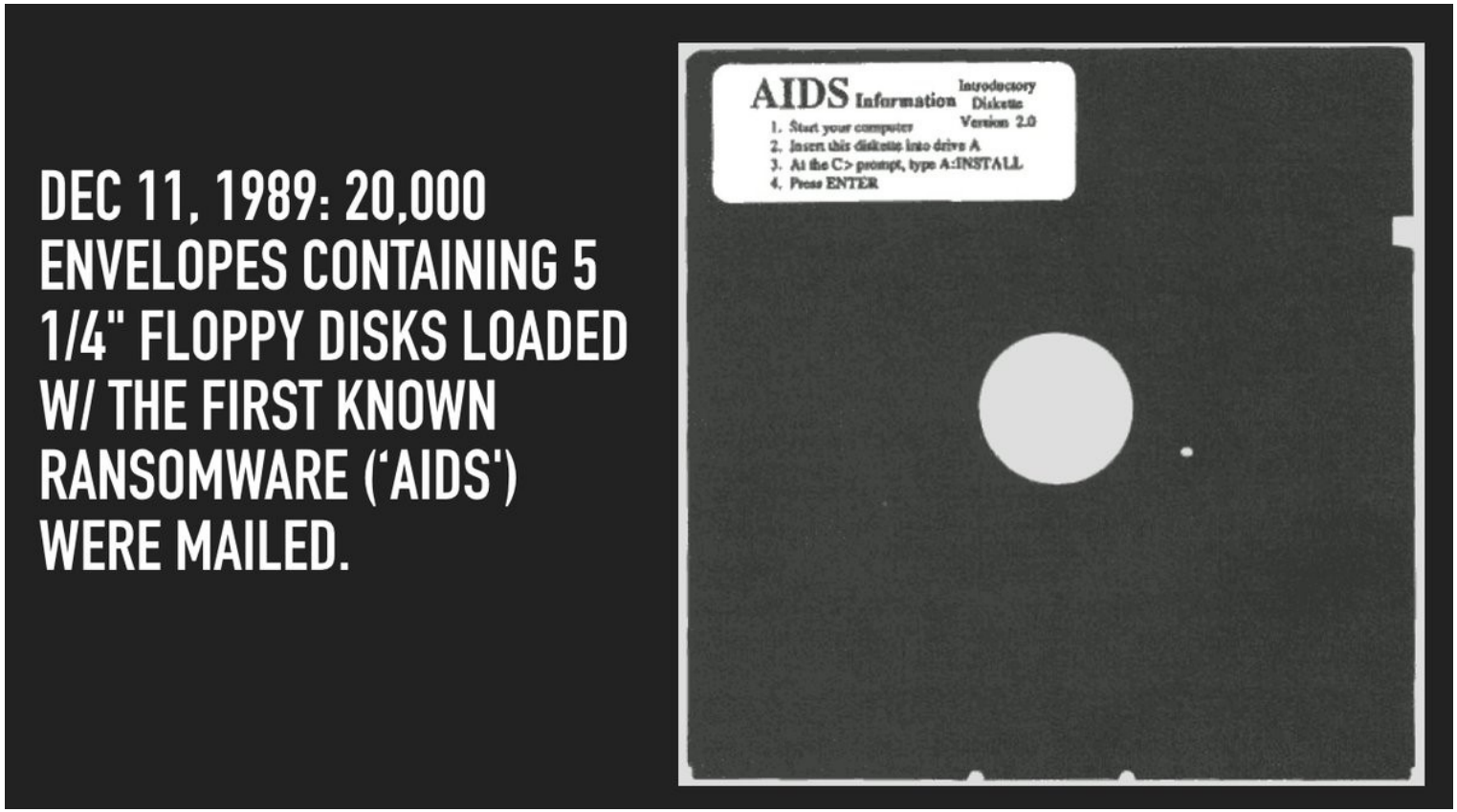
In The Wild

Ransomware

- 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.)

Geschichte der Ransomware

- Erste Ransomware: AIDS/PC Cyborg, 1989, DOS



(Bildquelle: https://twitter.com/jeremiahg/status/849655690243088384)

Geschichte der Ransomware

- Erste Ransomware: AIDS/PC Cyborg, 1989, DOS
- 1996: Veröffentlichung des Papers „ Cryptovirology: Extortion-Based Security Threats and Countermeasures“ (Young und Yung)
- ca. 2006-2010: vereinzeltes Auftreten von Ransomware, Bezahlung z.B. über
  - Western Union
  - Einkauf bei bestimmtem russischem Webshop
  - Premium-SMS-Versand

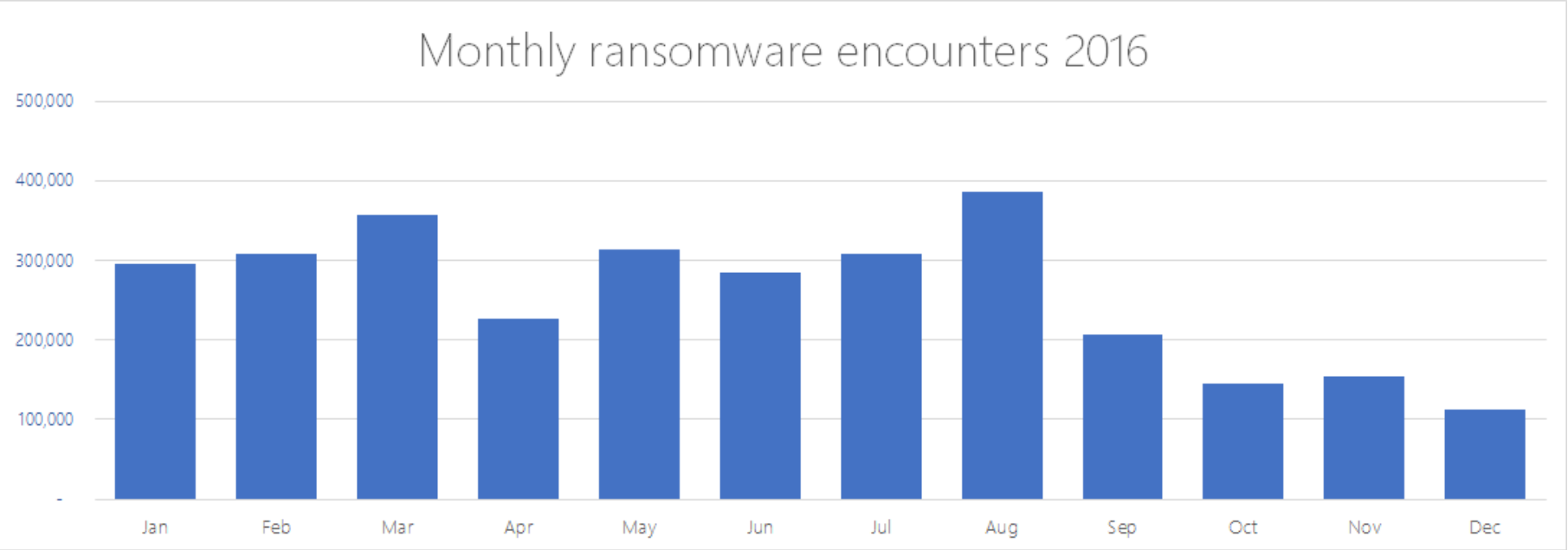
Geschichte der Ransomware

- Nächstes Puzzleteil: Bitcoin
  - 2008 erfunden
  - 2009 erste Software
  - 2011 mehrfache Erwähnung bei Heise
    → Anzeichen für steigende Verbreitung
  - 2013
    - Bitcoin ist hinreichend verbreitet, anonym/pseudonym
    - Ransomware-Entwickler springen auf den Zug auf
- 2013 verbreitete sich schon CryptoLocker

Geschichte der Ransomware

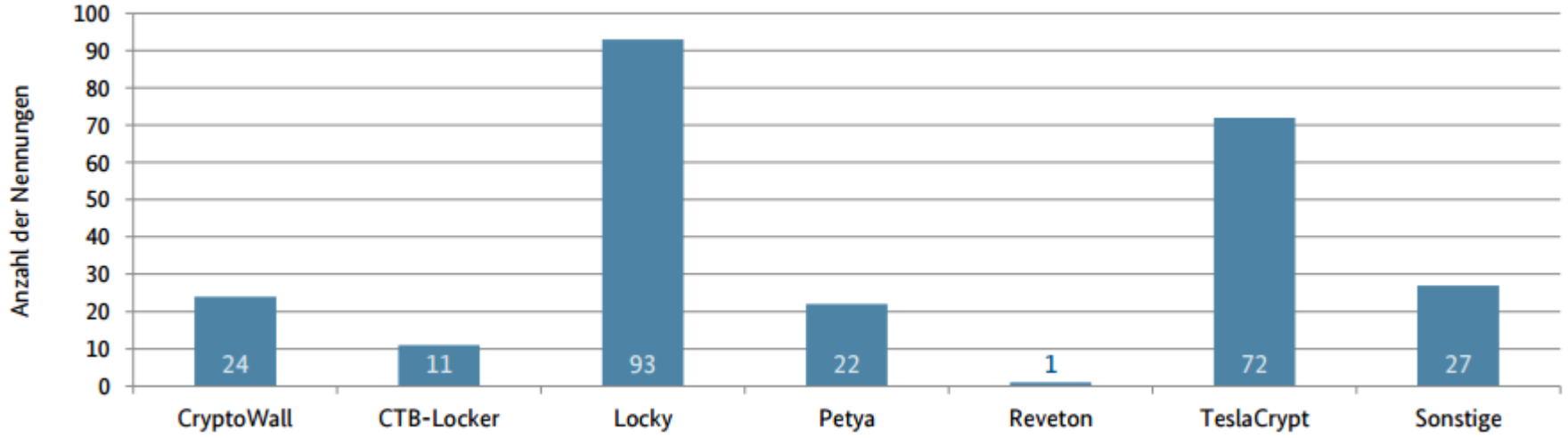
- Januar 2016: Locky
  - starke Verbreitung
  - Medienhype
  - diverse Trittbrettfahrer/Evolutionen
- Bis heute:
  - ständig neue Varianten von CryptoLocker, Locky & co.
  - teils Weiterentwicklungen, teils neuer Code
  - viel Schrott („hard encryption is hard“), aber leider auch einige erfolgreiche Varianten

Statistik: Entwicklung 2016



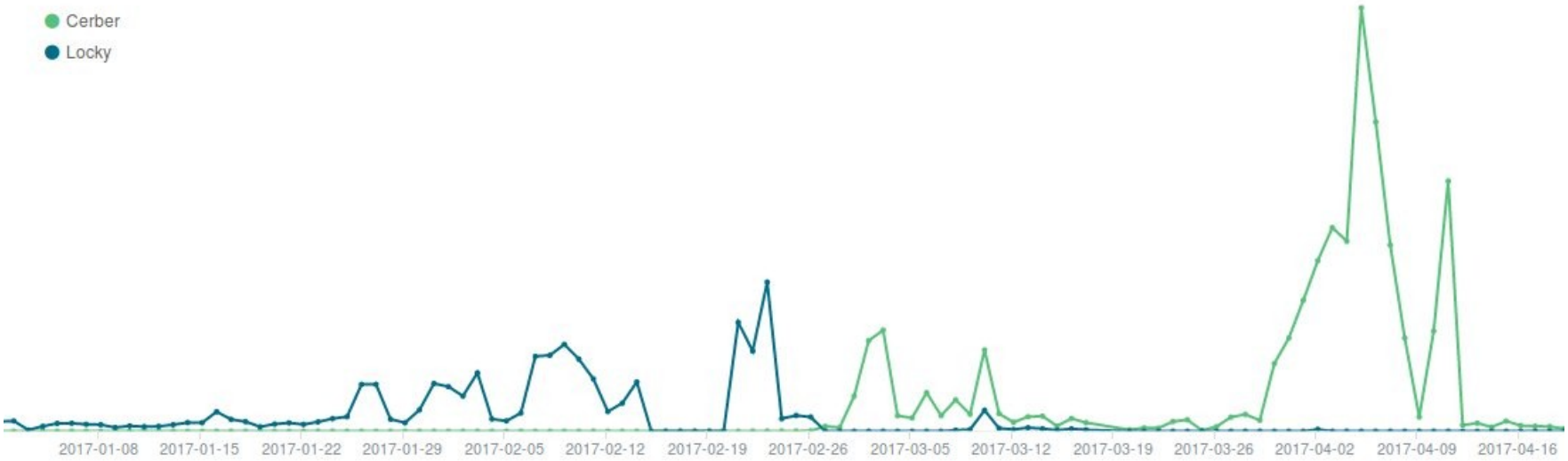
- Flaut langsam ab – ob dauerhaft, wird sich zeigen
- Quelle: Microsoft Malware Protection Center, https://blogs.technet.microsoft.com/mmpc/2017/02/14/ransomware-2016-threat-landscape-review/

Noch mehr Statistik (1 Jahr alt)



- 33% aller Firmen sind von Ransomware betroffen
  - Mit Abstand am häufigsten: Locky und TeslaCrypt
  - Bei 22 Prozent kam es zu erheblichen Ausfällen.
  - Etwas über 10 Prozent hatten ernsthaften Datenverlust.
- Quelle: BSI-Umfrage/https://heise.de/-3189776

Noch mehr Statistik (aktuell)



- Locky wurde von Cerber deutlich überholt
- Quelle: F-Secure, https://twitter.com/FSLabs/status/854688704169988096

Übersichtstabelle

Ransomware Overview

Ransomware | Unidentified | Detection | Prevention | Infographics | Download | Sources and Contributors

Name	Extensions	Extension Pattern	Ransom Note Filename(s)	Comment	Encryption Algorithm	Also known as	Date Added/Modified	Decryptor	Info 1	Info 2	Screenshots
.CryptoHasYou.	.enc		YOUR_FILES_ARE_LOCKED.txt		AES(256)				http://www.nyxb		https://www.g
777	.777	._[timestamp]_$[email]$. e.g. ._14-05-2016-11-59-	read_this_file.txt		XOR	Sevleg		https://decrypter			https://www.g
7ev3n	.R4A .R5A		FILES_BACK.txt			7ev3n-HONE$T		https://github.co https://www.yout	http://www.nyxb		https://www.g
7h9r	.7h9r		README_.TXT		AES				http://www.nyxb		https://www.g
8lock8	.8lock8		READ_IT.txt	Based on HiddenTear	AES (256)			http://www.bleep			https://www.g
AiraCrop	._AiraCropEncrypted		How to decrypt your files.txt	related to TeamXRat					https://twitter.co		https://www.g
Al-Namrood	.unavailable .disappeared		Read_Me.Txt					https://decrypter			https://www.g
Alcatraz Locker	.Alcatraz		ransomed.html						https://twitter.co		https://www.g
ALFA Ransomware	.bin		README HOW TO DECRYPT	Made by creators of Cerber					http://www.bleep		https://www.g
Alma Ransomware	random	random(x5)	Unlock_files_randomx5.html		AES(128)			https://cta-servic	https://info.phish	http://www.bleep	https://www.g
Alpha Ransomware	.encrypt		Read Me (How Decrypt) !!!!.txt		AES(256)	AlphaLocker		http://download	http://www.bleep	https://twitter.co	https://www.g
Alphabet				Doesn't encrypt any files / provides you the key					https://twitter.co		https://www.g
AMBA	.amba		ПРОЧТИ_МЕНЯ.txt READ_ME.txt	Websites only amba@riseup.net					https://twitter.co		https://www.g

https://t.co/pFRHITgglb bzw. https://docs.google.com/spreadsheets/d/1TWS238xacAto-fLKh1n5uTsdijWdCEsGIM0Y0Hvmc5g/pubhtml

Wird gepflegt von https://twitter.com/cyb3rops

Reiter „Prevention“ mit nützlichen Tipps

ReCoBS

ReCoBS steht für ...

- Remote
- Controlled
- Browsers
- System

Typische Firewall ...

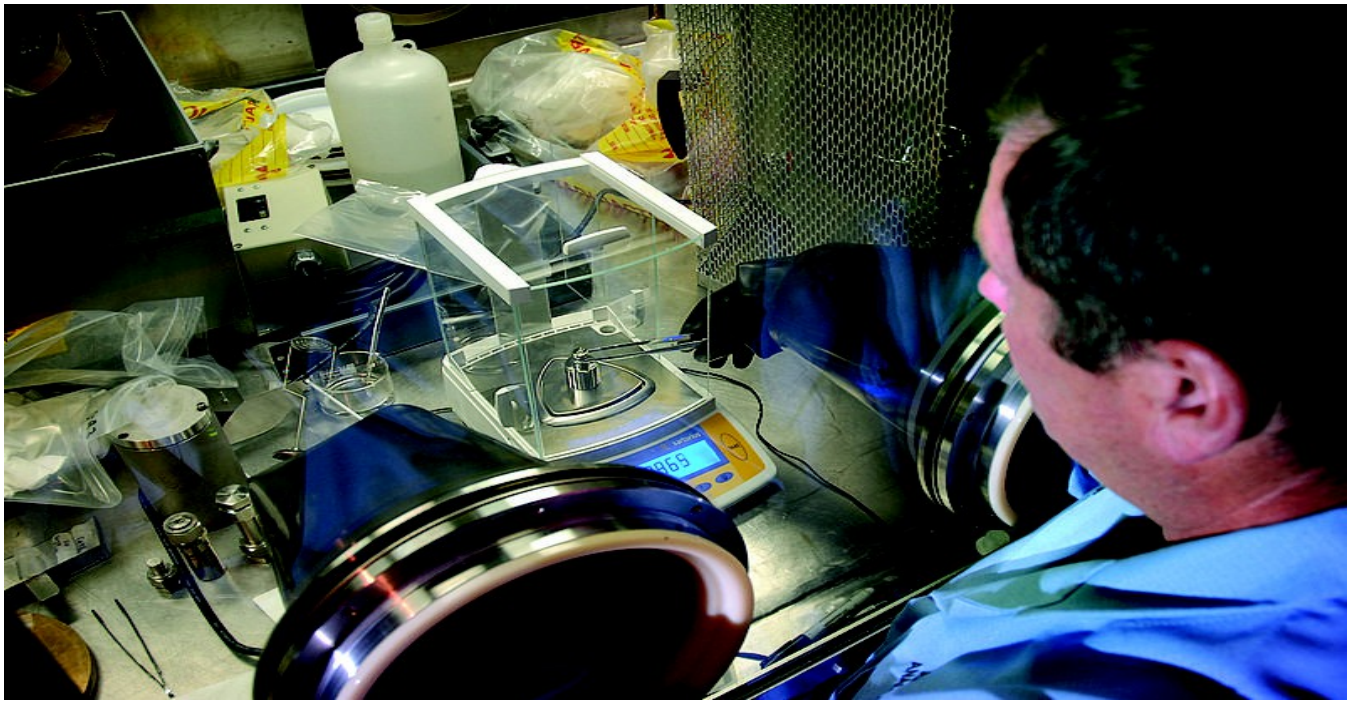
https://twitter.com/GossiTheDog/status/731973271252566017

ReCoBS vs. UTM/Firewall/Antivirus

- Was macht ein ReCoBS anders als eine (Consumer-)Firewall, ein Virenscanner, 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



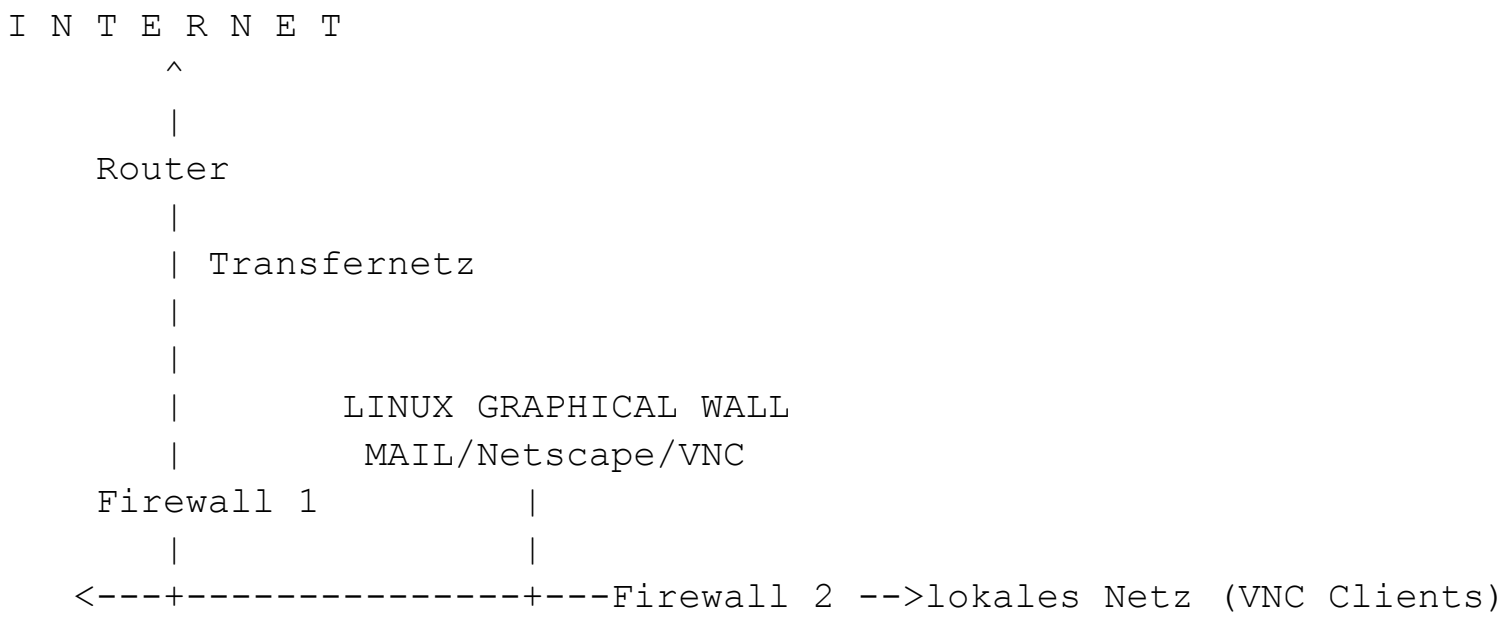
History ...

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

LINUX GRAPHICAL WALL

Original-Skizze von der damaligen Webseite:



Beispiel LINUX GRAPHICAL WALL

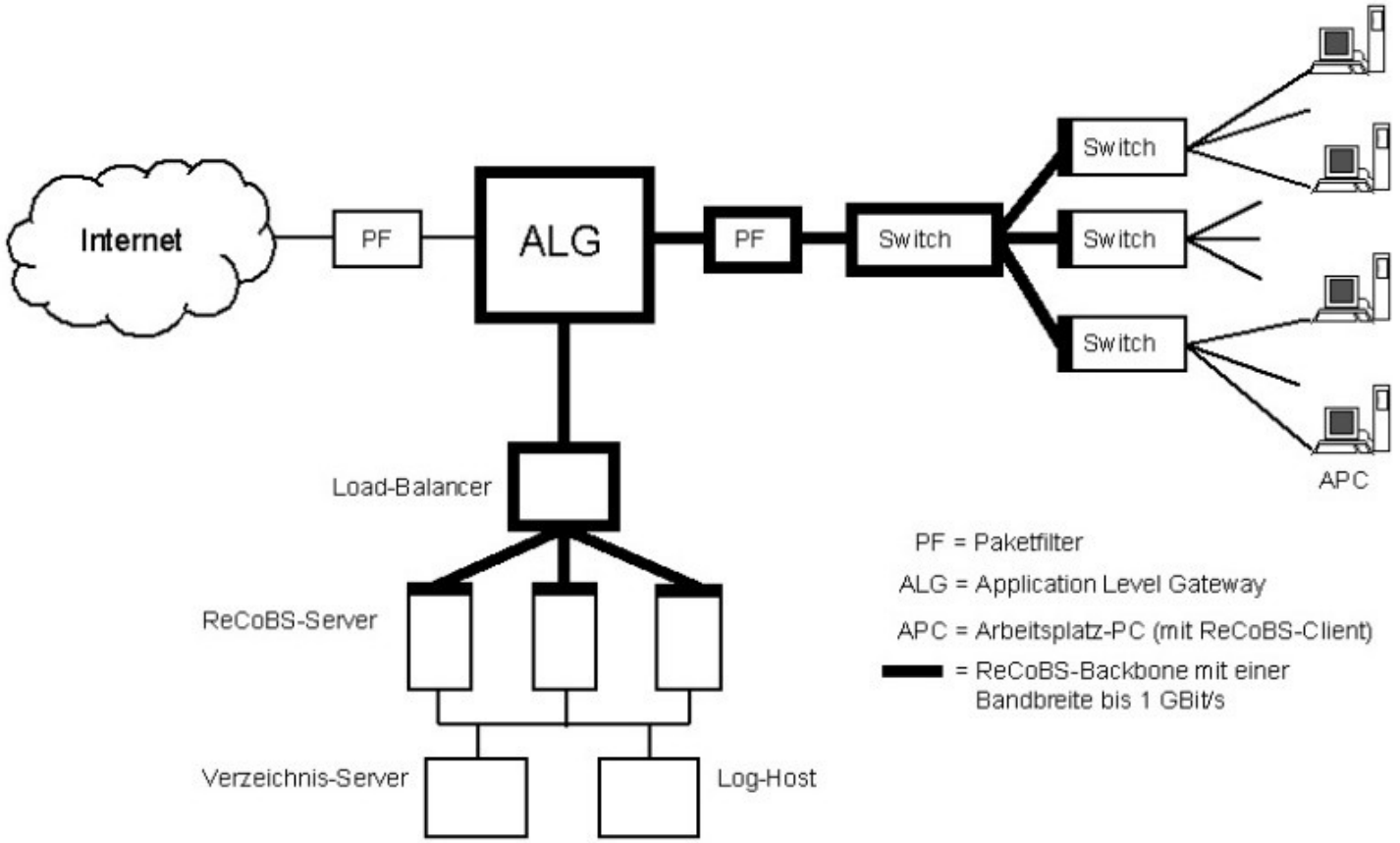
Weitere ReCoBS-Vorläufer

- 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 Virenscanner (unter Linux)

2006 – ReCoBS is born

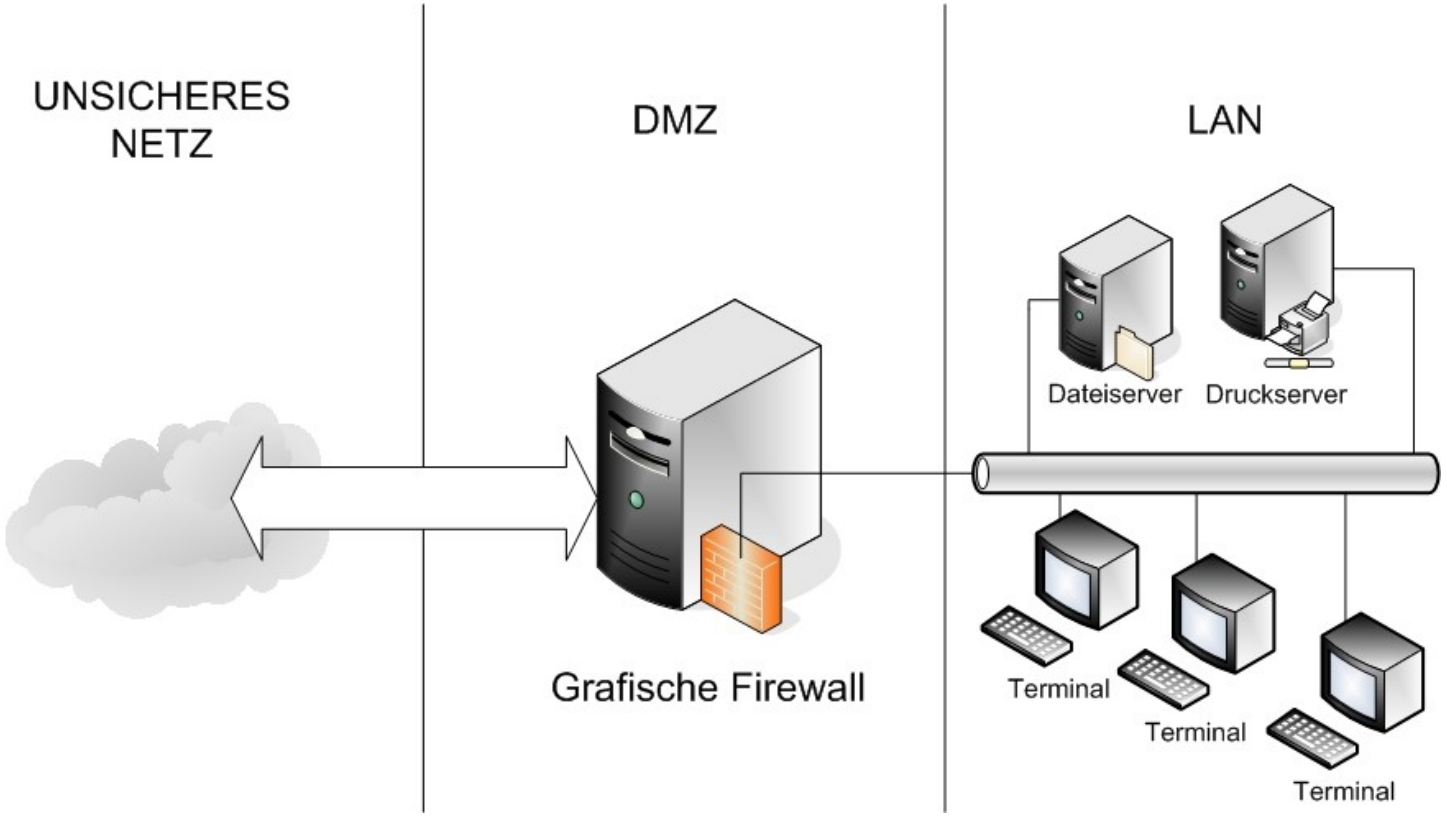
- 3-teilige Artikelreihe *Aktive Inhalte* in der <kes> (Zeitschrift für Informations-Sicherheit des BSI)
  - Teil 1 in 2005#5
  - Teil 2 in 2005#6 – enthielt schon ReCoBS-Andeutungen
  - Teil 3 in 2006#1 – *Remote-Controlled Browsers System – Sichere und bequeme Nutzung von aktiven Inhalten*
- BSI-Grundschutz-Handbuch
  - Maßnahmenkatalog, Abschnitt M 4.365: „Nutzung eines Terminalservers als grafische Firewall“
  - https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04365.html

ReCoBS



ReCoBS-Skizze aus <kes> 2006#1

ReCoBS



ReCoBS-Skizze aus BSI-Grundschutzhandbuch

Geldinstitut != IT-Firma

- Ein Geldinstitut ist 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

3 Jahre später: Dezember 2009

- Sprung in die Vollzeit-Selbstständigkeit
- Gründung als UG (haftungsbeschränkt)
- Produktnamensfindung: *elektronische GloveBox*
- Wahl fiel auf FreeNX als Serverkomponente
- Anlaufschwierigkeiten bei der Vermarktung
  - 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

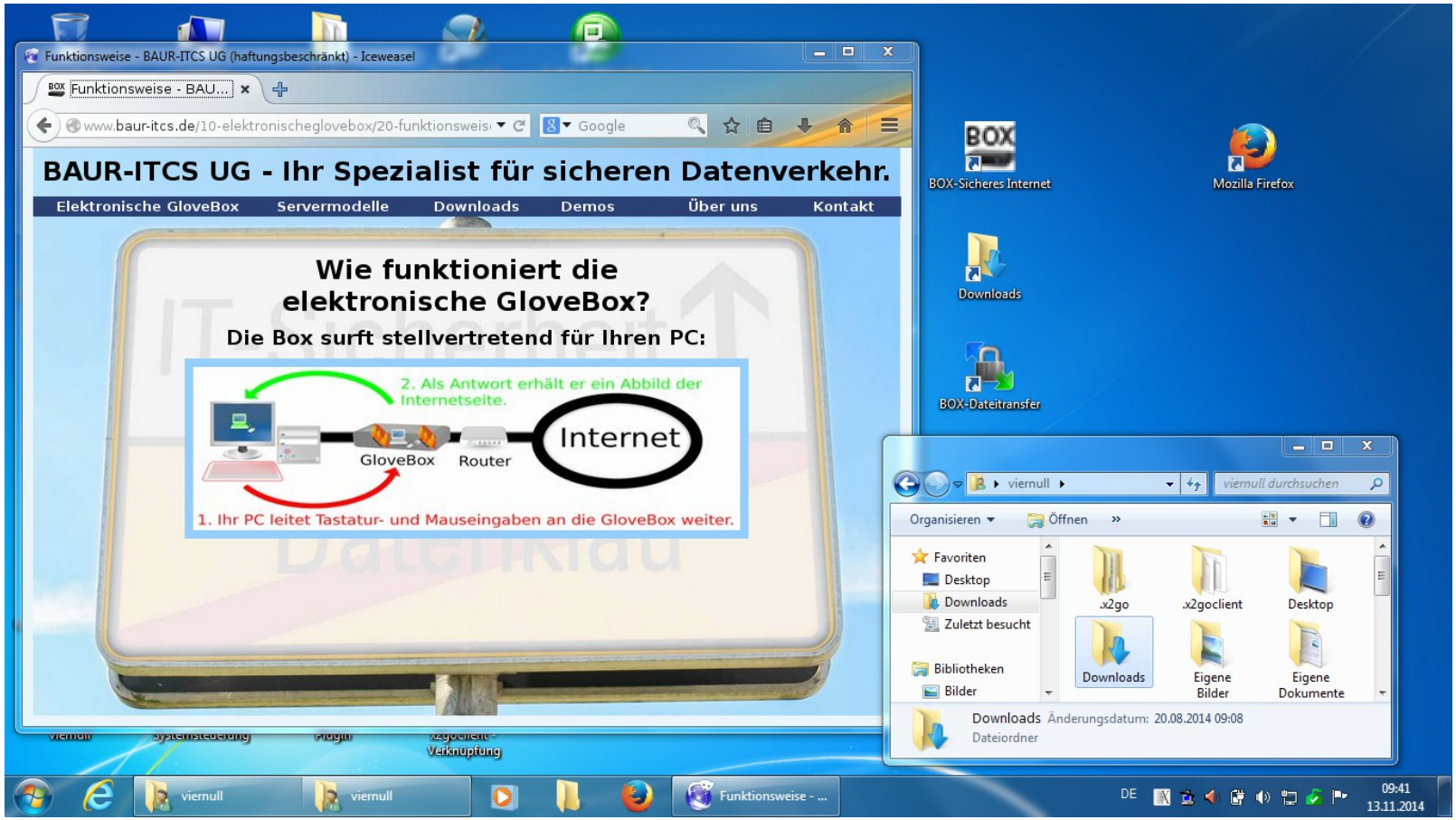
elektronische GloveBox

- 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

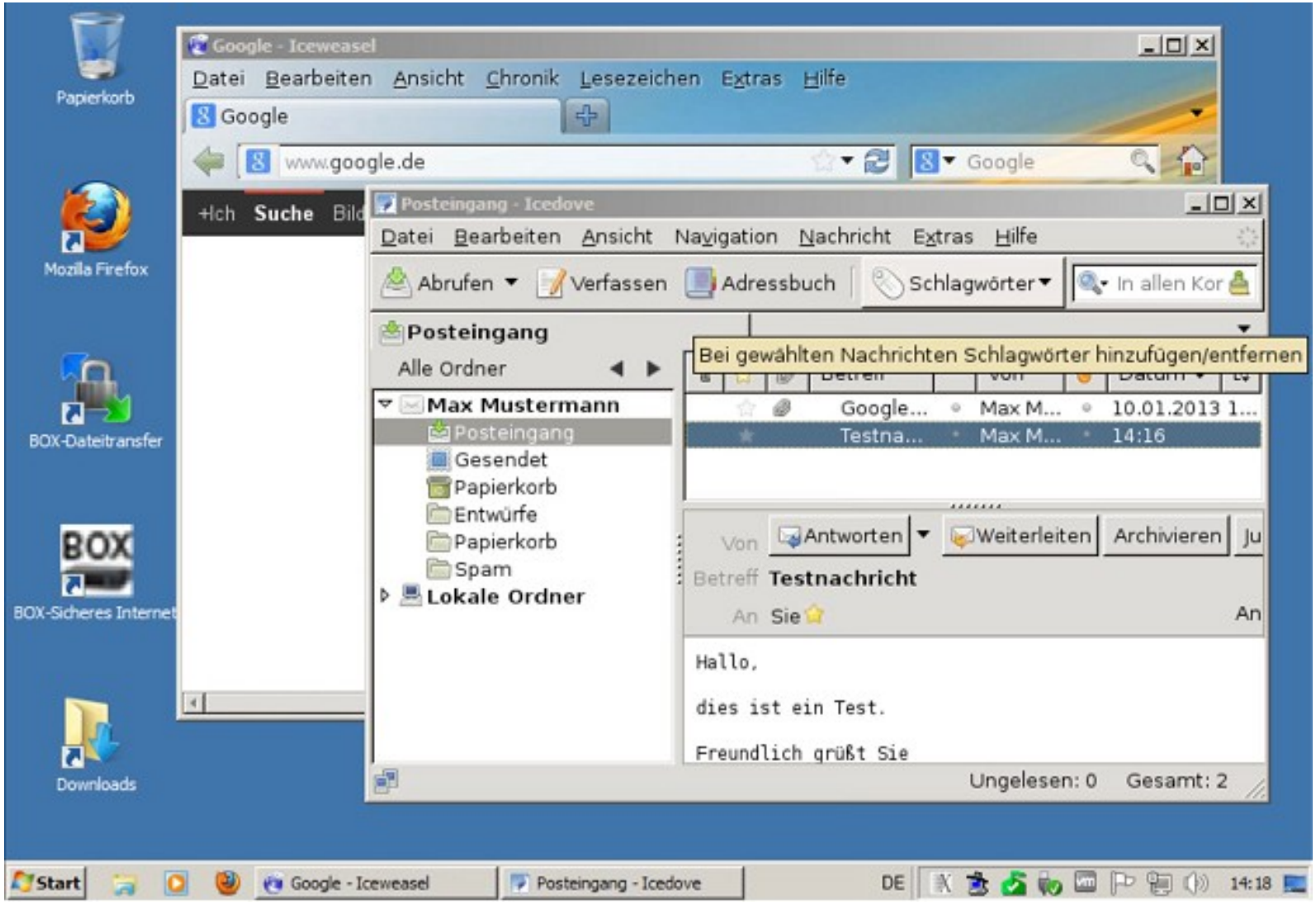
- zwischen DSL-/Kabel-Router und LAN einstecken (DSL-/Kabel-Router ist die 1. Firewall aus dem ReCoBS-Bild), Clients einrichten, fertig

Screenshots

elektronische GloveBox



elektronische GloveBox



Live-Demo GloveBox
→ am Stand

- alter hp-Tablet-PC mit XP und X2Go

Erfolg!

- Genau zwei Infektionen nach schwerem Benutzerfehlverhalten („set brain=off“)
  - in über 7 Jahren
  - bei grob 50 installierten Serversystemen (Peakwert)
  - mit im Schnitt 4-5 Usern pro Installation
- Erfolgreiche Schadenseindämmung
  - Nur jeweils betroffener PC neu zu installieren
  - Kein Datenverlust – nichts gelöscht/verschlüsselt
  - Kein Datenabfluss

Was war passiert?

- Mailanhang à la rechnung.pdf.exe.zip
- Geht nach dem 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!

Malware-Struktur

SwiftOnSecurity @SwiftOnSecurity · 8. März
The files you get in email and phishes, they're not the malware. Whac-a-mole. They're called "droppers." They download the actual stuff.
Original (Englisch) übersetzen
2 18 28

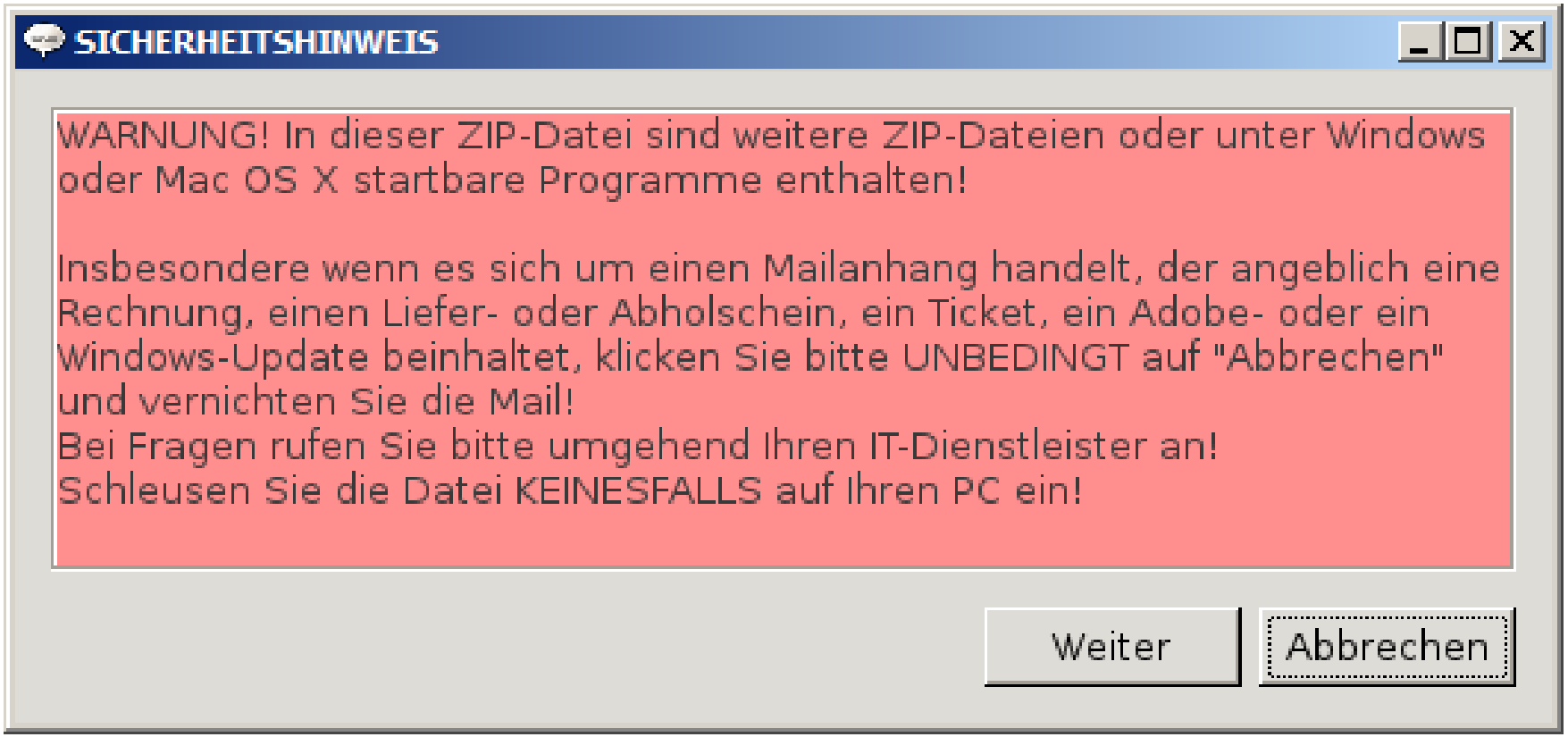
SwiftOnSecurity @SwiftOnSecurity · 8. März
Droppers are cheap to make and reformat so antivirus doesn't detect them. Small and simple and in flux so it's harder to profile them.
Original (Englisch) übersetzen
5 12 15

SwiftOnSecurity @SwiftOnSecurity · 8. März
They then pull down multiple other pieces of malware, depending on who's paying. The ecosystem is literally an entire mercenary economy.
Original (Englisch) übersetzen
3 12 17

- Quelle: https://twitter.com/SwiftOnSecurity/status/839270402601992193

Neue Schutzmaßnahme

- Popup bei gepackten Mailanhängen mit ausführbarem Inhalt



DOs and DON'Ts für ReCoBS

Thema Benutzerkennungen

- Identische Benutzerkennungen in Produktionsnetz und Surfumgebung bedeutet:
  - Wer die Surfumgebung kompromittiert, hat damit eine Liste von gültigen Benutzerkennungen des Produktionsnetzes
  - Viel zielgerichtetere Angriffe möglich
- Warum wollen es Kunden es trotzdem:
  - Weil sie Single-Sign-On wollen und meinen, dass sie „es dafür unbedingt brauchen!!!1!1!!einseinself!“
  - Dabei können wir SSO auch anders – und sicher

Thema Dateischleuse

- Wir setzen auf eine manuelle Schleuse
  - Benutzer muss selbst aktiv werden und sagen „Ja, genau diese Datei(en) jetzt durchschleusen“
- Kunden wollen gern eine automatische Schleuse (synchronisiertes Verzeichnis)
  - Aus Sicherheitsgründen abzulehnen
  - Drive-By-Download in dieses Verzeichnis → DLL-Injection und „Oh, eine dancing_bunnies.exe“-Effekt
  - Exploits dafür existieren bereits

Exkurs: Windows-DLL-Suche

- Windows-Programme – auch Installer wie eine „setup.exe“ – können externe DLLs voraussetzen
- Wird eine Funktion aus einer DLL aufgerufen, sucht Windows eine DLL mit diesem Namen ...
  - erst im Verzeichnis, in dem die setup.exe liegt
  - wenn dort keine solche DLL liegt → Systempfad
- Hack: gleicher DLL-Name, geänderte Funktion
- Anfällig ist z.B. JRSoft InnoSetup: UXTheme.dll

Optional Live-Demo
→ bei Zeitmangel am Stand

Thema Virenscanner

- Virenscanner – klingt nicht unvernünftig, aber:
  - mehr und mehr Seiten setzen auf https
  - https-Datenstrom nicht scanbar, da verschlüsselt
  - Virenscanner müsste Man-in-the-Middle spielen
    - klappt nicht immer
    - Problematik bzgl. Datenschutz/IT-Security (Integrität)
  - Bleibt Dateisystemscanner → Linux nicht Zielgruppe
- Frage der Wirtschaftlichkeit – bei z.B. 200 Usern
  - Lizenzkosten / ~1 Client-Reinstallation alle 3 Jahre

Thema MiTM-TLS/SSL-Virenscanner

- TLS/SSL → HTTPS
- Man-in-the-Middle-Scanner sind meistens irgendwie kaputt – mit fatalen Folgen
  - 12 von 13 TLS/SSL-MiTM-Scannern und 11 von 12 TLS/SSL-MiTM-Scan-Appliances verschlechterten im Test die Sicherheit der Verbindung
  - in vielen Fällen konnten die Forscher den angeblichen Schützern sogar massive Sicherheitsprobleme nachweisen

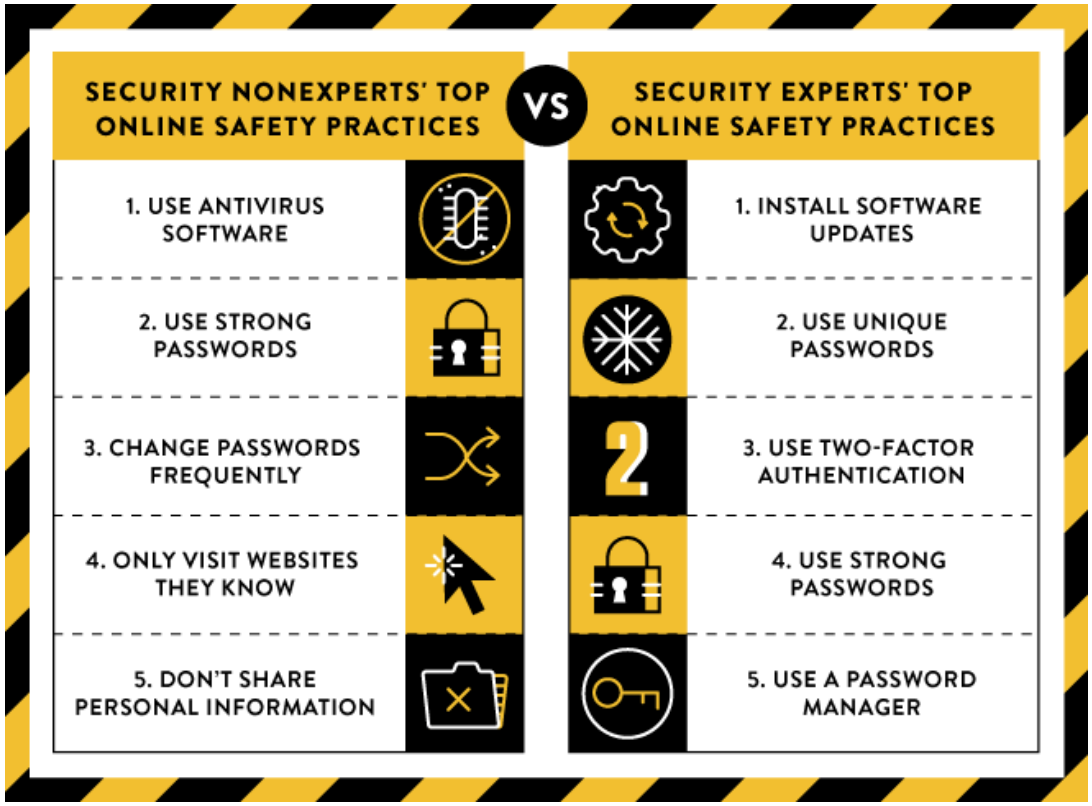
Quelle: https://heise.de/-3620159

Thema MiTM-TLS/SSL-Virenscanner

- US-CERT warnt vor HTTPS-Inspektion: HTTPS Interception Weakens TLS Security
- „Wer Software mit HTTPS-Inspektion einsetzt, müsse testen, ob die erforderliche Sicherheit damit noch gewährleistet bleibt.“
- CERT-Bund sieht das ebenfalls als Problem

  Quellen: https://heise.de/-3660610, https://www.us-cert.gov/ncas/alerts/TA17-075A

Virenscanner sind überbewertet



- Quelle: https://security.googleblog.com/2015/07/new-research-comparing-how-security.html

Virenscanner sind trotzdem sinnvoll!

- Es war von „Online Safety Practices“ die Rede.
- Andere klassische Infektionswege
  - Verseuchter USB-Stick (privat → Urlaubsbildersammlung, externer Techniker → Druckertreiber, ...)
  - Absichtliches Einschleusen ins Netzwerk durch vermeintliche Putzfrau etc. (Industriespionage)
- Ex-Firefox-Entwickler rät zur De-Installation von AV-Software (Quelle: https://heise.de/-3609009)
  → Bitte nicht!

Konsequentes Rechtekonzept

- 2016: 530 gemeldete Sicherheitsprobleme in Microsoft-Anwendungen
  - 94% davon waren nur ausnutzbar, wenn der Benutzer Admin-Rechte hatte
  - 100% der gemeldeten Sicherheitsprobleme in IE und Edge waren nur mit Admin-Rechten ausnutzbar
- Quelle: https://tech.slashdot.org/story/17/02/26/1047257/94-of-microsoft-vulnerabilities-can-be-mitigated-by-turning-off-admin-rights

Thema Netztrennung

- gern gemachter Fehler
- Netze mit unterschiedlichem Sicherheitsniveau gehören auf unterschiedliche Hardware
- Das heißt:
  - Trennung von Internet/DMZ und Produktionsnetz nur per VLAN auf selbem Switch ist tabu
  - VLANs sind Managementwerkzeug, keine Sicherheitsmaßnahme
- Switch-Betriebssysteme sind Angriffsziel

Thema Netztrennung

- „Gravierende Telnet-Lücke bedroht zahlreiche Cisco-Switches“
- 300 verschiedene Cisco-Modelle mit IOS- und IOS-XE-Betriebsystemen betroffen
- aus der Ferne und ohne Authentifizierung Schadcode ausführbar
- Somit auch Zugriff über VLAN-Grenzen möglich
- Quelle: https://heise.de/-3658915

X2Go
skaliert gut!

Skalierbarkeit X2GoServer

- auf ARM (Raspberry Pi)
  - Nicht wirklich sinnvoll, außer für Remote-Administration (noch keine Sitzungsspiegelung)
  - Fertige Pakete für Raspbian
- auf Intel/AMD
  - Pakete für die gängigen Distributionen vorhanden
  - Loadbalancer (X2Go-Broker) → Server-Farm
- auf POWER7/8, OpenPower, und bald System z
  - Scale-Up statt Scale-Out

Broker-Testumgebung

- Installationsskripte für Demo-Umgebung im Wiki: http://wiki.x2go.org/doku.php/doc:howto → Installing an X2Go Session Broker Demo Environment
  - Debian Preseed-Files für LDAP-Server, NFS-Server, Postgres-Server, Broker, 2 X2GoServer, 1 Client
  - Vollautomatische Installation
  - LDAP-Beispiel-Setup **keinesfalls** im Produktivbetrieb nutzen, auch nicht darauf aufbauen versuchen, bitte! → Wer nicht hören will: Es wird furchtbar weh tun!

Broker-Demo-System
→ am Stand

Immer noch Zeit?
→ dann Projektinfos

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 ...

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