SF Spezial
Die Computer-Knacker

Erlebnisbericht aus der Sicht der t1g3rs

GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
team@csnc.ch www.csnc.ch

- Im Rahmen der SF Spezial Woche „Alles unter Kontrolle?“ wurde ein Hacker-Contest durchgeführt

- 6 Teams kämpften gegeneinander
  - Napali (System Engineers)
  - Synttys aka Syndikal-Teletypewriters (IT-Freaks)
  - t1g3rs (Security Analysts)
  - Bit Defenders (Studenten Uni Bern)
  - X-ETH-One (Studenten ETH Zürich und Uni Zürich)
  - ENIAC (Studenten FH Bern)

GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

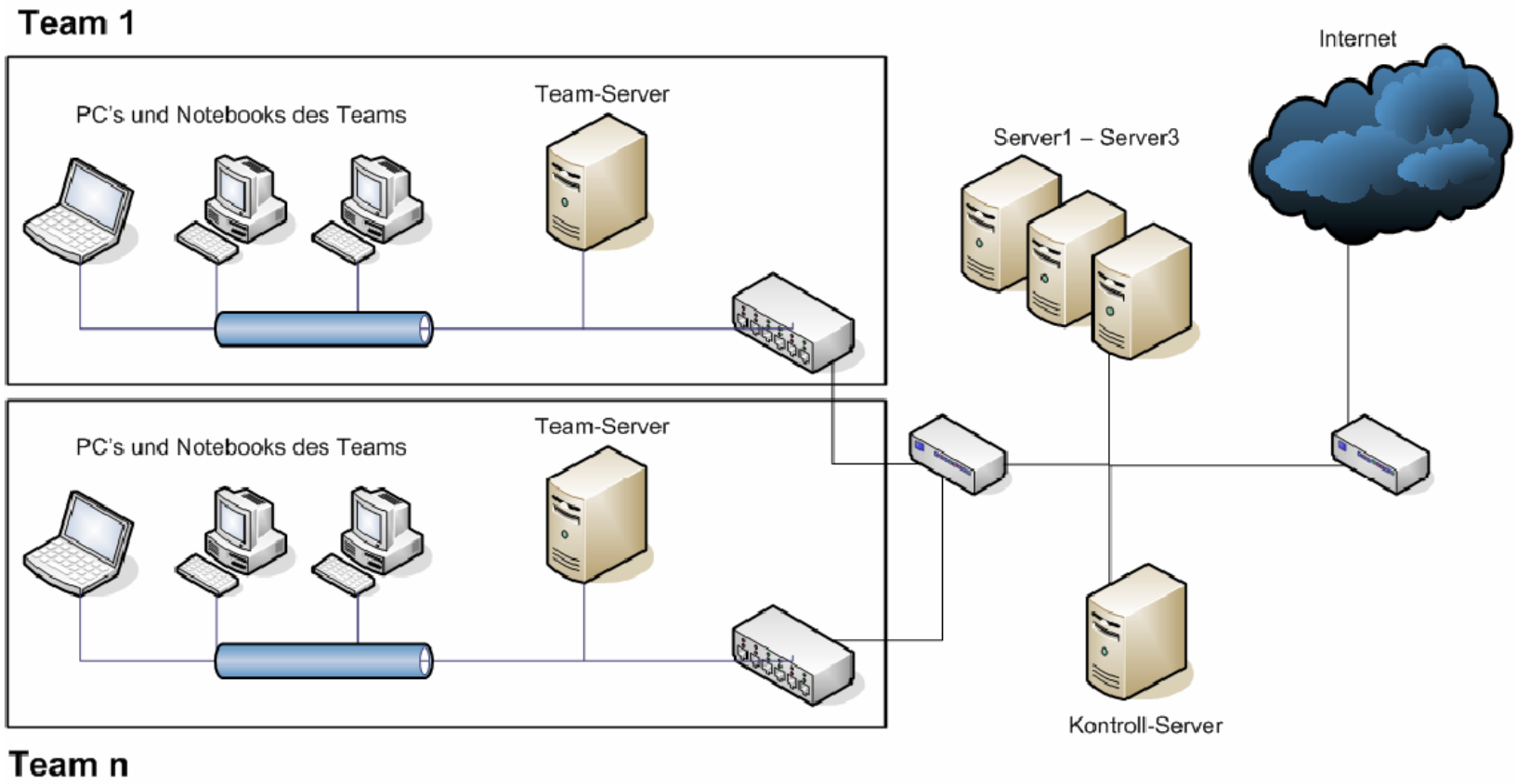
Tel.+41 55-214 41 60
Fax+41 55-214 41 61
team@csnc.ch www.csnc.ch

GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
team@csnc.ch www.csnc.ch

GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
team@csnc.ch www.csnc.ch



GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
team@csnc.ch www.csnc.ch

- Die Spielregeln und Aufgaben wurden erst 30 Minuten vor Spielbeginn mitgeteilt. Jedes Team durfte sich „blind“ vorbereiten und Software mitnehmen.

- Jedes Team musste einen Server aufsetzen mit folgenden Diensten.
  - echo
  - anonymous ftp
  - ftp upload
  - http
  - dns
  - mail (smtp/pop)

GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
team@csnc.ch www.csnc.ch

- Jedes Team musste versuchen während 21 Stunden
  - die Verfügbarkeit des gegnerischen Teams negativ zu beeinflussen
  - die Dienste des gegnerischen Teams zu übernehmen

- Erschwerend kam hinzu, dass sich die Teams nur von Junk-Food ernähren konnten: Hamburger und Pommes, Pizza, Schnitzelbrot, Sandwich und Coca-Cola!!!

GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
team@csnc.ch www.csnc.ch

- Zwischendurch wurden Zusatzaufgaben erteilt mit denen ein Team zusätzlich Punkten konnte
  - Dienste auf IPv6 bereitstellen
  - Modifizieren eines einzigen Bytes in einem Linux Binary so dass zwei Zahlen addiert statt subtrahiert werden
  - 95 Multiple-Choice-Fragen in 50 min zu Linux
  - Information Gathering bei 3 bereitgestellten Servern
    - RedHat, SuSe, Solaris
  - Übernahme von 4 bereitgestellten Servern
    - RedHat, SuSe, Solaris, Windows 2003
  - Bereitstellen einer eingeschränkten Remote-Shell ohne Login
  - Syslog-Meldung an Kontroll-Server versenden

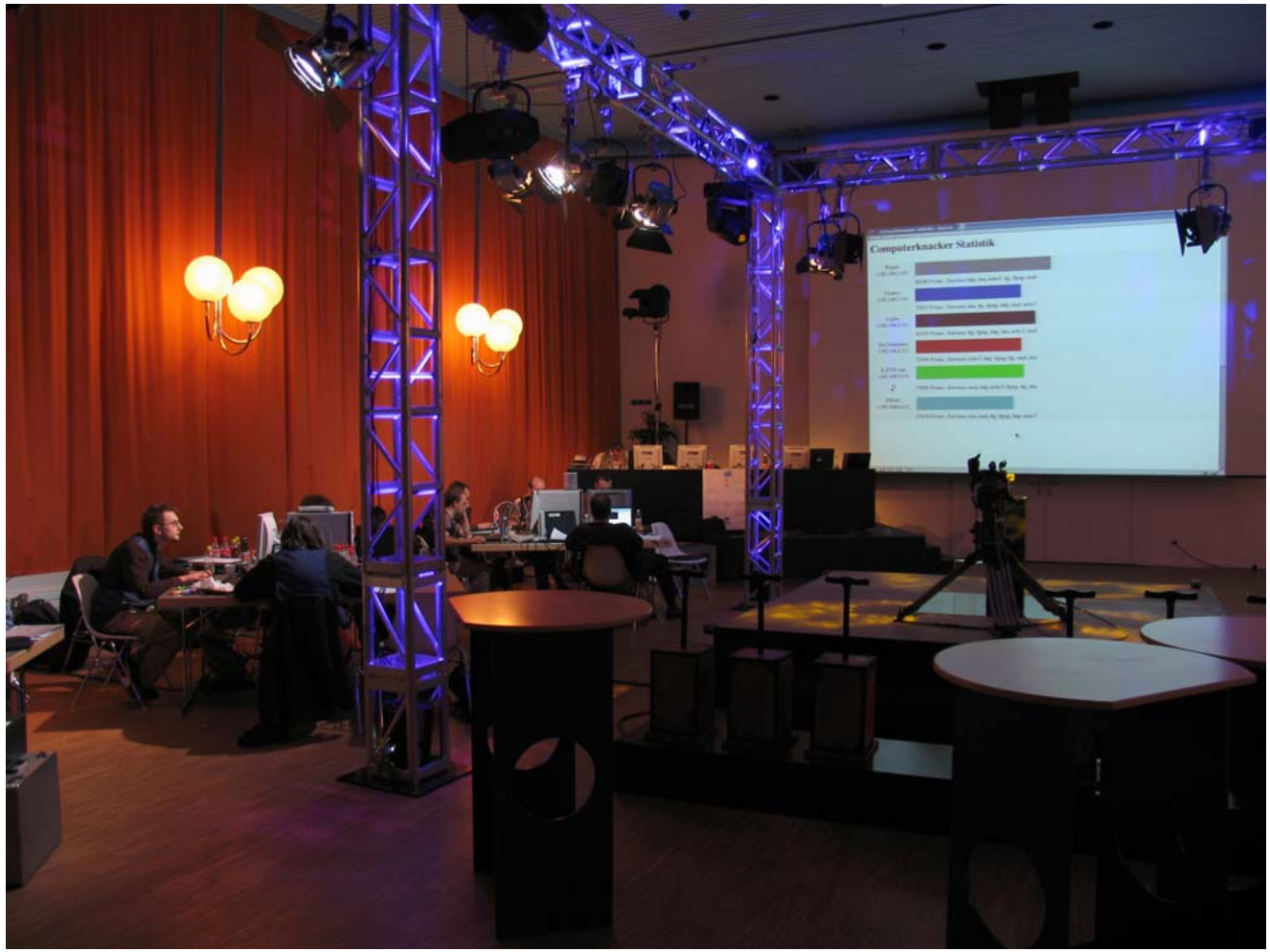
GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
team@csnc.ch www.csnc.ch

- Der Kontroll-Server prüfte alle 2 Minuten die Verfügbarkeit und Funktion der Services.
- War alles in Ordnung vergab der Kontroll-Server Punkte. Gewisse Dienste gaben mehr Punkte als andere.
- Für Zusatzaufgaben wurde jeweils bis zu 5000 zusätzliche Punkte vergeben.

GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
team@csnc.ch www.csnc.ch



GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
team@csnc.ch www.csnc.ch

- Ziel der t1g3rs
  - Server sicher aufgesetzt so dass keine Kompromittierung möglich ist
  - Erreichen des Finals
- Strategie
  - Services von Anfang an sicher konfigurieren unter Einbusse der Geschwindigkeit
  - Organisation im Team (2 Verteidiger/Überwacher, 2 Angreifer, 1 Koordinator/Joker)
  - Verfügbarkeit der Dienste garantieren
  - Andere Systeme übernehmen

GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
team@csnc.ch www.csnc.ch

- Server von t1g3rs: SuSe 9.2 out of the Box
  - Verwendete Software-Pakete für die Services
    - echo → xinetd
    - http → Apache
    - ftp → vsftp
    - smtp → Postfix
    - pop → qpopper
  - Firewall iptables
    - Obwohl ein vorbereitetes und getestetes Firewall-Script verwendet wurde, waren beim Einschalten der Firewall die Services nicht mehr erreichbar. Daher wurde entschieden auf die Software-Firewall zu verzichten.

GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
team@csnc.ch www.csnc.ch

- Hardware Clients
  - 4 DELL Notebooks
  - 1 DELL Desktop

- Betriebssysteme Clients
  - SuSe Standard Distribution
  - Auditor Security Collection
  - Knoppix STD
  - Windows 2000 SP4 (gehärtet)
  - Windows XP SP2 (gehärtet)

GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
team@csnc.ch www.csnc.ch

Team t1g3rs an der „Arbeit“

GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
team@csnc.ch www.csnc.ch

- Man-in-the-Middle-Attacke mittels ARP-Spoofing
  - Passwort sniffen
- Social-Engineering
  - Passwort abschauen beim gegnerischen Arbeitsplatz

→ Login auf gegnerischen Server mittels SSH
→ Defacing des HTTP- und FTP-Service war möglich
→ Beeinträchtigung des Mail-Service war möglich in dem das Kontroll-Mail auf dem gegnerischen Server gelöscht wurde

- Umleiten des Verkehrs anderer Teams mittels ARP-Spoofing

→ Verfügbarkeit der Dienste anderer Teams beeinträchtigt

GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
team@csnc.ch www.csnc.ch

- Vulnerable Services
  - Übernahme des Unix-Benutzers *bin* mittels remote Telnet-Exploit auf der Solaris Maschine.
  - Da X-ETH-One zuerst auf dem Solaris-Server war und sie diesen gehärtet haben, war es t1g3rs nicht mehr möglich root zu werden.
  - Ausnutzung der sadmind Schwachstelle und somit Zugriff als Root (leider deaktivierte X-ETH-One den RPC Dienst im gleichen Moment)
  - Beim Härten unterlief X-ETH-One ein Fehler, so dass sie sich aus dem System ausgesperrt haben.

- Schwach konfigurierte Services
  - Anonymous FTP erlaubte Berechtigungen der Dateien (chmod) zu ändern. Somit war eine Schreiboperation möglich.

  → Defacing des FTP-Service war möglich

GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
team@csnc.ch www.csnc.ch

- Server nur mit den benötigten Services aufgesetzt. Zugriff auf Server nur mittels SSH Public-Key möglich.
- Statische ARP-Cache Einträge, um ARP-Spoofing zu verhindern.
- Wurden wir angegriffen, so haben wir jeweils von Hand alle zu einer IP-Adresse gehörenden Child-Prozesse gestoppt.
- War ein Service nicht mehr erreichbar, so wurde dieser von Hand neu gestartet.
- Cron-Job der jede Minute die Kontroll-Webseite mit der Team-Kennung neu erstellte.
- Keine Zettel mit Passwörter offen auf dem Tisch liegen lassen ;-)

GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
team@csnc.ch www.csnc.ch

- Denial-of-Service
  - ARP-Flooding

  → Netzwerk DoS

  - SYN-Fooding

  → TCP-Service DoS

  - Versenden langen Massenemails

  → Mail-Service DoS

- X-ETH-One
  - RPC-Remote-Exploit von Solaris

GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
team@csnc.ch www.csnc.ch

- Vorbereitete Linux Installationen
  - Dadurch waren die Services von einigen Teams sehr schnell oben!
- Gute Firewall-Rules
  - Limitierung der halb-offenen TCP-Verbindungen
  - Limitierung der Anzahl Verbindungen pro IP pro Minute
  - ARP-Poisioning, welches das ARP-Poisioning der anderen neutralisierte

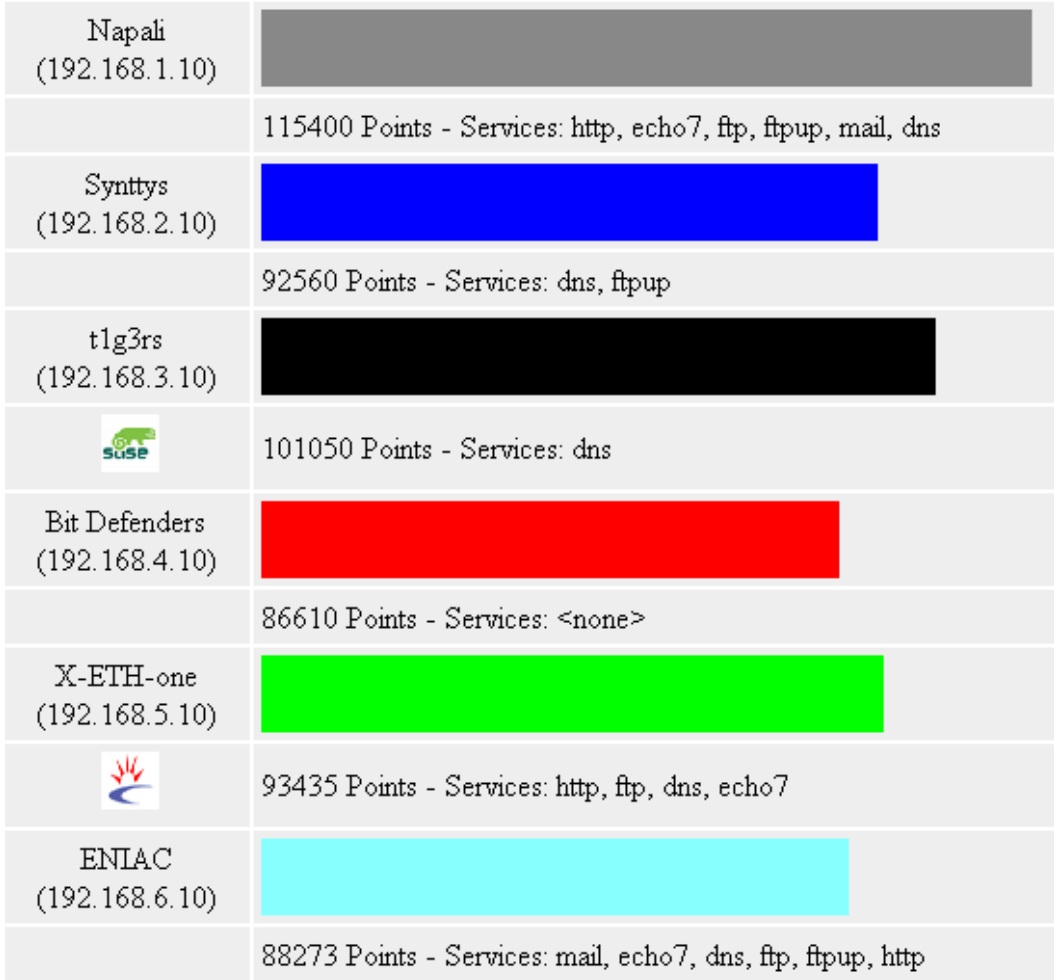
GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
team@csnc.ch www.csnc.ch

Rangliste und Punktestand bei Vorentscheidung

- Rangliste
  1. Napali
  2. t1g3rs
  3. X-ETH-One
  4. Synttys
  5. ENIAC
  6. Bit Defenders

- Finalisten
  - Napali
  - t1g3rs



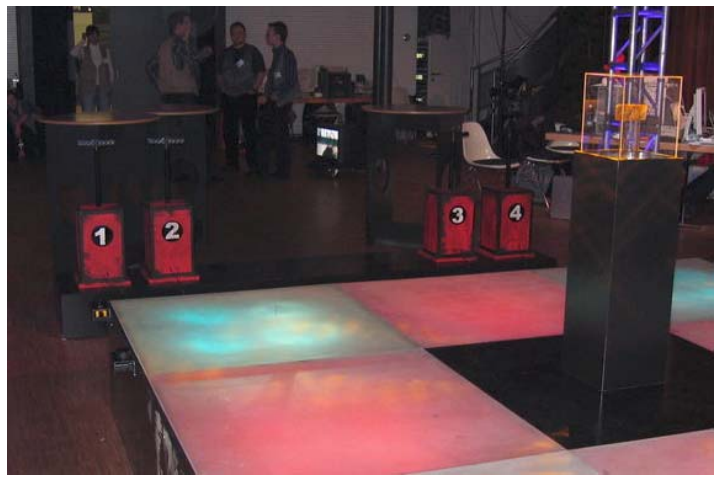
GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
team@csnc.ch www.csnc.ch

- Es mussten à la “Wer wird Millionär” Fragen beantwortet werden (1 Frage – 4 mögliche Antworten)

- Bei richtiger Beantwortung konnte das Team einen von 4 Auslösern betätigen. Wenn es knallt, dann ist das Gold gewonnen!

- Der Gewinner der Vorausscheidung war als erstes dran mit Fragen beantworten.



GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
team@csnc.ch www.csnc.ch

- 1. Frage an Team Napali
  - Frage: Welcher Hersteller hat den ersten Laptop auf den Markt gebracht?
  - Antwort Napali: Toshiba
  - Ueli Schmezer: Falsch, es war Epson!

- 2. Frage an Team t1g3rs
  - Frage: In welchem Film übernahm der Computer HAL-9000 die Kontrolle?
  - Antwort t1g3rs: 2001–A Space Odyssey
  - Ueli Schmezer: Das ist richtig!
  - Christoph Schnidrig wählt den 3. Auslöser aus

→ … Boom!!! → 1 kg Gold für die t1g3rs!!!

GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
team@csnc.ch www.csnc.ch

Die t1g3rs sind (v.l.n.r): Adrian Leuenberger, Walter Sprenger, 1kg Gold, Marco Schurtenberger, Jan P. Monsch, Christoph Schnidrig

GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
team@csnc.ch www.csnc.ch

- Alles unter Kontrolle? (inkl. Video-Streams)
  http://www.allesunterkontrolle.ch
- Statistik und Rangliste Computerknacker
  http://computerknacker.hta.fhz.ch/
- Spielanleitung
  http://kos.li/computerknacker.pdf
- Online-Fotoalbum von X-ETH-One
  http://party.kos.li/ComputerKnacker
- Quellen Fotos
  - Ulrich Frede, Luzern
  - X-ETH-One

GLÄRNISCHSTRASSE 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
team@csnc.ch www.csnc.ch