

# Compass Security AG

[The ICT-Security Experts]



Mobile Security - Angriffsszenarien auf mobile Dienste:  
Wie (un-)sicher sind iPhone, Blackberry & Co.?

Marco Di Filippo

Compass Security AG  
Glärnischstrasse 7  
Postfach 1628  
CH-8640 Rapperswil

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

# Science-Fiction von heute

[Impressionen aus der realen Welt]



Übrigens: Heute müssen Sie Ihr Telefon nicht ausschalten. Ich empfehle jedoch den Stumm-Modus ;-)



A vertical decorative strip on the left side of the slide features a close-up image of a computer keyboard with a prominent yellow padlock resting on one of the keys.

# Das Mobile Netzwerk

Compass Security AG  
Glärnischstrasse 7  
Postfach 1628  
CH-8640 Rapperswil

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

Auszug aus den aktuellen Lagebericht zur IT-Sicherheit des BSI (Bundesamt für Sicherheit in der Informationstechnik)

**„Cyberkriminelle nutzen neben Botnetzen, Spamversand und Phishing-E-Mails zunehmend Infiltration über Mobiltelefone und WLAN“**

## Mobile Geräte: kritisch und oft vergessene Kinder ...

- ✦ Mobile Geräte arbeiten oft ohne schützende Firmen-Firewall.
- ✦ Sie werden viel transportiert und sind einfach zu bewegen.
- ✦ Sie kommunizieren mit fremden Netzen über unsichere Verfahren.
- ✦ Die Benutzer haben oft Administrator-Rechte.
- ✦ Können einfach entwendet, geklaut oder zerstört werden...
- ✦ Werden im Sicherheitskonzept oft vergessen oder bewusst nicht berücksichtigt.

Übrigens: Haben Sie die Verschlüsselung Ihres BlackBerrys oder den Zugangsschutz Ihres iPhones aktiviert?



## Cap'n Crunch Hack

Dank einem mehr oder weniger exakt 2600 Hertz hohen Ton (z.B. mittels einer Pfeife aus einer Cornflakes-Packung) konnte man den Gebührenzähler beim CCITT5-Standard manuell deaktivieren, um Kosten zu sparen.



## John Draper

Er perfektionierte die Entdeckung von Joseph Engressia (16-jähriger blinder Schüler) in Form von der 1970 entwickelten BlueBox, mit der man die Gebührenzähler von AT&T überlisten konnte.



## BlueBox

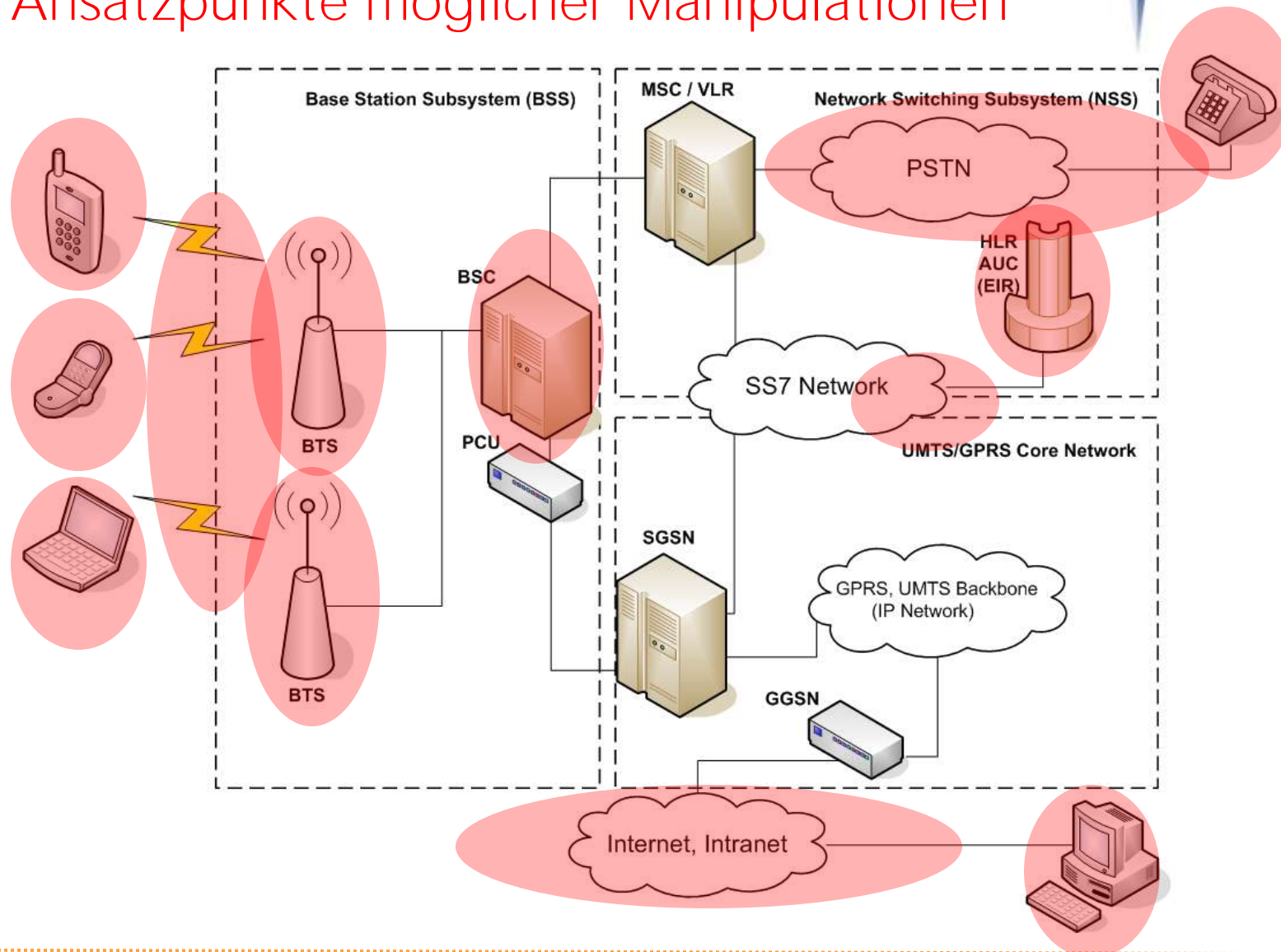
Die BlueBox produzierte einen 2.600 Hertz-Ton, welcher von CCITT v5-kompatiblen Vermittlungsstellen benutzt wurde. Beim Phreaking wurden damit illegal kostenlose Telefonate erschlichen.



## BeigeBoxing

Dienst zum illegalen Anzapfen der Telefonleitung einer anderen Person, um auf deren Kosten zu telefonieren bzw. Gespräche mitzuhören. Die BeigeBox hat ihren Namen von der beige Farbe der durch sie angezapften Verteilerkästen.

## Ansatzpunkte möglicher Manipulationen



## Was geschah am 21.04.2009 in Deutschland?

Tag der Wirtschaft und Hannover Industrie Messe

Auftaktveranstaltung 21.04.2009 um 10Uhr

[www.pressebox.de](http://www.pressebox.de)

Erstes Cloud-Betriebssystem von VMware

Das Cloud-OS vereinfacht die Datenverarbeitung

[www.silicon.de](http://www.silicon.de)

ZDF heute journal

Thema: Killerspile & Verbot

[www.youtube.de](http://www.youtube.de)

**39,1 Millionen Kunden in Deutschland ohne Handynet:**

Fast das komplette Netz von T-Mobile ist ausgefallen.

[www.spiegel.de](http://www.spiegel.de), [www.stern.de](http://www.stern.de), [www.welt.de](http://www.welt.de), etc.



Glauben Sie dass die Ortung von mobilen  
Geräten ausschließlic Sache von  
Behörden und Geheimdiensten ist?

# Wo bin ich? Ortung mittels GSM

Compass Security AG  
Glärnischstrasse 7  
Postfach 1628  
CH-8640 Rapperswil

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

Jeder, der Signale aussendet, kann prinzipiell auch geortet werden.

Im Umkehrschluss kann man sich selbst orten, indem man Signale, welche von bekannten Positionen gesendet werden, auswertet.



Welche Informationen werden zur Ortung benötigt?

Referenzpunkte:

- ✦ Eindeutige Kennung der Mobilfunkzelle, in der sich das Endgerät aufhält/befindet

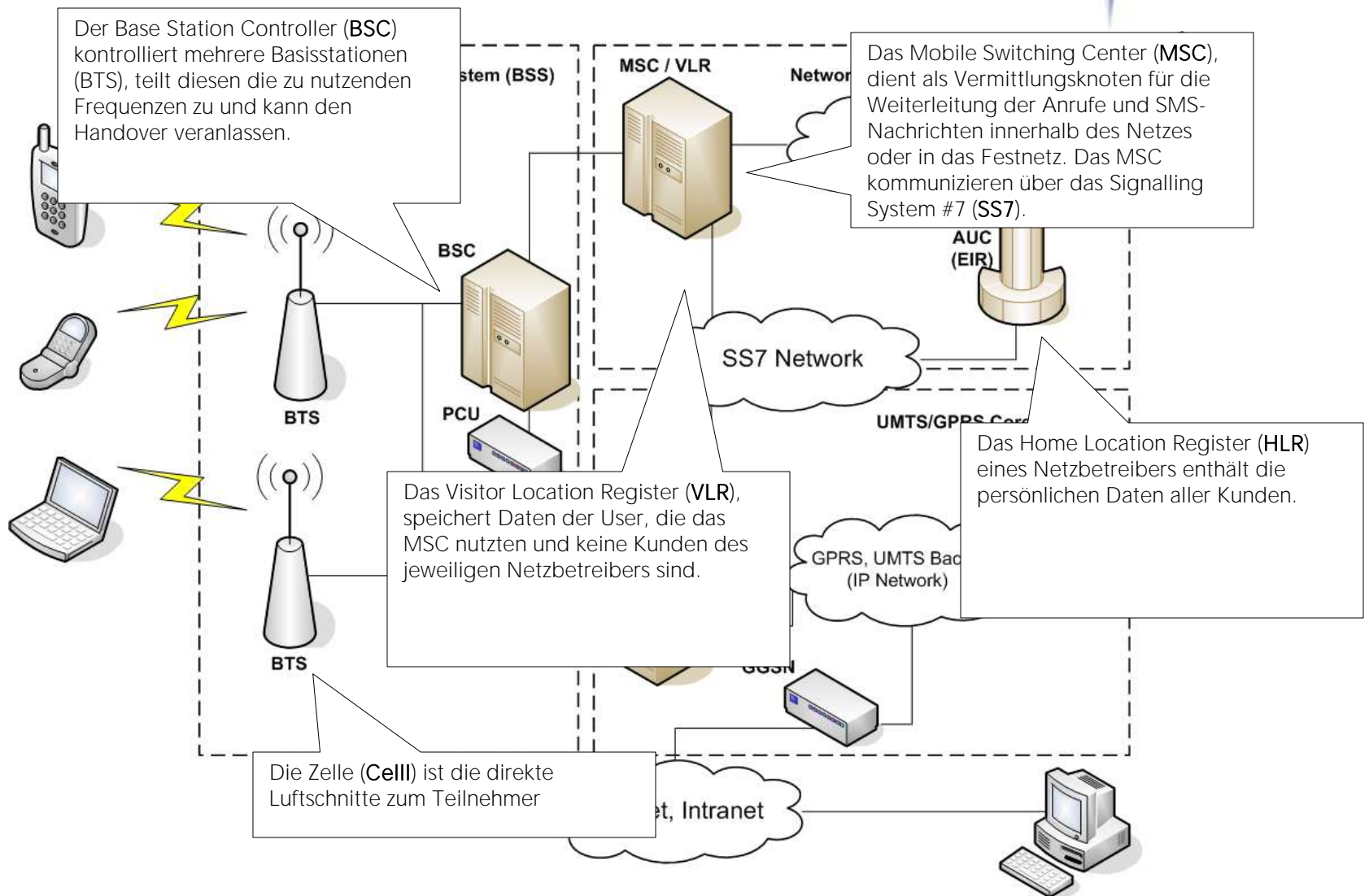
Koordinaten der Referenzpunkte:

- ✦ Datenbank mit den Senderkoordinaten (BTS/BSC)

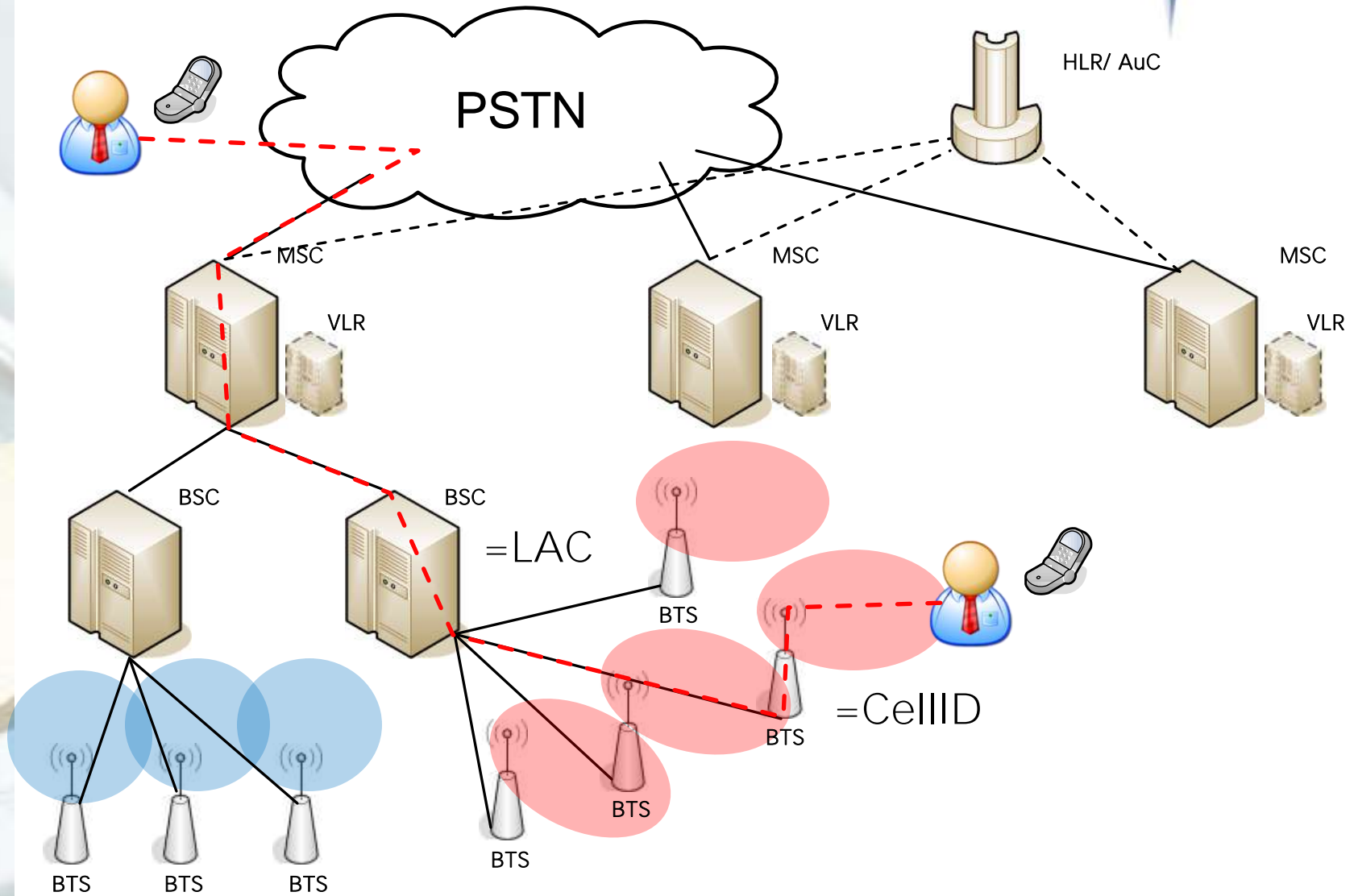
Die Ortungsmethoden lassen sich in zwei unterschiedliche Gruppen einteilen:

- ✦ Selbstortung (auch mobile centric positioning)
  - ✦ Signale von Sendern mit bekannten Positionen werden ausgewertet, um somit die eigene Position zu ermitteln. Beispiele hierfür sind Leuchttürme, Astronavigation oder GPS.
- ✦ Fremdortung (auch network centric positioning)
  - ✦ Der Netzbetreiber sammelt Positionsinformationen von mehreren seiner Basisstationen und kombiniert sie später zentral, um die Position eines Endgerätes zu berechnen.

# Referenzpunkte im Mobilnetz



# Vermittlungsweg im GSM-Netz



## Relevante Daten der momentan aktiven/befindlichen Zelle lokal auslesen (Beispiel Siemens S45 Monitormode)

**CH** Frequency Channel Number \*) **RX** RXLEV Reception Level [dBm]

**CI** Cell Identity (in Hex)

**C1** Path-loss Criterion xx Technological type SIM? (hier93)

**LAI** Location Area Identity

MCC Mobile Country Code (hier 23F4 = 324)

MNC Mobile Network Code (hier 05 = 50)

Format: c<sup>2</sup>c<sup>1</sup>Fc<sup>3</sup>n<sup>2</sup>n<sup>1</sup> kkkk

LAC Location Area Code (hier 0538)

**TXPWR** Allowed Transmit Power [dBm]

**RXAM** Reception Accetable Minimal Level [dBm]

**C2** Cell-reselection Criterion

**BSPA** BSPA multiframe is feature of the network. Describes, how often the mobile must switch on the receiver. The range is between 2 and 9. The most networks use multiframe=6. A lower figure indicates more power consumption.

**BA** BCCH Allocation

**P0, P1, P2, P3** Paging

```
CH045 RX-068
CI 10A8 C1+38 93
LAI 23F405 0538
TXPWR33 RXAM-106
C2+38 BSPA6 BA15
P0          P1
P2          P3
```

Relevante Daten der momentan aktiven/befindlichen Zelle lokal auslesen (Beispiel iPhone/SignalApp)

- ✦ Installieren der Signal.app


```
deb file  
Signal.deb - iOS4 app.
```

```
Die Datei Signal.deb in das  
Verzeichnis  
/var/root/Media/Cydia/AutoInstall  
legen und das iPhone neu starten (evtl.  
das Verzeichnis neu erstellen).
```

Hinweis: In der Version iOS 4.x wurde der Fieldtest von Appel Inc. deaktiviert.

Relevante Daten der momentan aktiven/befindlichen Zelle lokal auslesen (Beispiel iPhone/SignalApp)

- ✦ Installieren der Signal.app
- ✦ Auslesen der GSM Cell Daten

A screenshot of the Signal app interface on an iPhone. The status bar at the top shows "Telekom", signal strength, Wi-Fi, time "11:48", and battery "90%". The app title is "Signal" with a "Done" button. Below the title, it says "Current cell" and lists various GSM parameters in a table.

Parameter	Value
Radio Access Technology	GSM
Mobile Country Code	262
Mobile Network Code	1
Location Area Code	38914
Cell ID	57564
RX power level	-94 dBm
Absolute RF Channel Number	15
Base Station Identity Code	59

Relevante Daten der momentan aktiven/befindlichen Zelle lokal auslesen (Beispiel iPhone/SignalApp)

- ✦ Aktivieren des Feldtest-Modus
- ✦ Auslesen der GSM Cell Daten
  - ✦ MCC (Mobile Country Code)

A screenshot of the Signal app on an iPhone. The status bar at the top shows "Telekom", signal strength, Wi-Fi, time "11:48", and battery "90%". The app title is "Signal" with a "Done" button. The main content is titled "Current cell" and lists various GSM parameters in a table format.

Parameter	Value
Radio Access Technology	GSM
Mobile Country Code	262
Mobile Network Code	1
Location Area Code	38914
Cell ID	57564
RX power level	-94 dBm
Absolute RF Channel Number	15
Base Station Identity Code	59

## MCC (Mobile Country Code)

- ★ Anhand der ersten Ziffer kann man eine kontinentale Einordnung vornehmen:

- 0 nicht vergeben
- 1 nicht vergeben
- 2 Europa**
- 3 Nordamerika und Karibik
- 4 Asien, Indien, naher Osten
- 5 Australien und Ozeanien
- 6 Afrika
- 7 Südamerika
- 8 nicht vergeben
- 9 Welt

Siehe auch [www.nobbi.com/wiki/doku.php/mcc](http://www.nobbi.com/wiki/doku.php/mcc)

## MCC (Mobile Country Code)

- ★ Die zweite und dritte Ziffer definiert das Land (Auswahl):

262	Germany
228	Switzerland
232	Austria
234	United Kingdom
235	United Kingdom
310	bis
316	United States of America

Siehe auch [www.nobbi.com/wiki/doku.php/mcc](http://www.nobbi.com/wiki/doku.php/mcc)

Relevante Daten der momentan aktiven/befindlichen Zelle lokal auslesen (Beispiel iPhone/SignalApp)

- ✦ Aktivieren des Feldtest-Modus
- ✦ Auslesen der GSM Cell Daten
  - ✦ MCC (Mobile Country Code)
  - ✦ MNC (Mobile Network Code)

A screenshot of the Signal app on an iPhone. The status bar at the top shows "Telekom", signal strength, Wi-Fi, time "11:48", and battery "90%". The app title is "Signal" with a "Done" button. The main content is titled "Current cell" and lists various GSM parameters in a table format. The "Mobile Network Code" value "1" is circled in red.

Current cell	
Radio Access Technology	GSM
Mobile Country Code	262
Mobile Network Code	1
Location Area Code	38914
Cell ID	57564
RX power level	-94 dBm
Absolute RF Channel Number	15
Base Station Identity Code	59

## MNC (Mobile Network Code)

- ✦ Der MNC steht für den Netzbetreiber

### Deutschland

01,06	T-Mobile
02,04,09	Vodafone
07,08,11	O <sup>2</sup>

### Schweiz

01	Swisscom Mobile
02	Sunrise
03	Orange

Relevante Daten der momentan aktiven/befindlichen Zelle lokal auslesen (Beispiel iPhone/SignalApp)

- ★ Aktivieren des Feldtest-Modus
- ★ Auslesen der GSM Cell Daten
  - ★ MCC (Mobile Country Code)
  - ★ MNC (Mobile Network Code)
  - ★ LAC (Location Area Code)  
organisatorische Zusammenfassung von Zellen

A screenshot of the Signal app on an iPhone. The status bar at the top shows "Telekom", signal strength, Wi-Fi, time "11:48", and battery "90%". The app title is "Signal" with a "Done" button. The main content is titled "Current cell" and lists various GSM parameters in a table-like format.

Current cell	
Radio Access Technology	GSM
Mobile Country Code	262
Mobile Network Code	1
Location Area Code	38914
Cell ID	57564
RX power level	-94 dBm
Absolute RF Channel Number	15
Base Station Identity Code	59

Relevante Daten der momentan aktiven/befindlichen Zelle lokal auslesen (Beispiel iPhone/SignalApp)

- ★ Aktivieren des Feldtest-Modus
- ★ Auslesen der GSM Cell Daten
  - ★ MCC (Mobile Country Code)
  - ★ MNC (Mobile Network Code)
  - ★ LAC (Location Area Code)  
organisatorische Zusammenfassung von Zellen
  - ★ Cell ID, zwei Bytes die eine Zelle innerhalb einer LAC identifizieren

A screenshot of the Signal app on an iPhone. The status bar at the top shows "Telekom", signal strength, Wi-Fi, time "11:48", and battery "90%". The app title is "Signal" with a "Done" button. The main content is titled "Current cell" and lists various GSM parameters in a table-like format.

Current cell	
Radio Access Technology	GSM
Mobile Country Code	262
Mobile Network Code	1
Location Area Code	38914
Cell ID	57564
RX power level	-94 dBm
Absolute RF Channel Number	15
Base Station Identity Code	59

# Ortung durch LBS Location Based ID



In unserem Beispiel wäre die eindeutige Location Based ID

MCC – MNC – LAC – CID

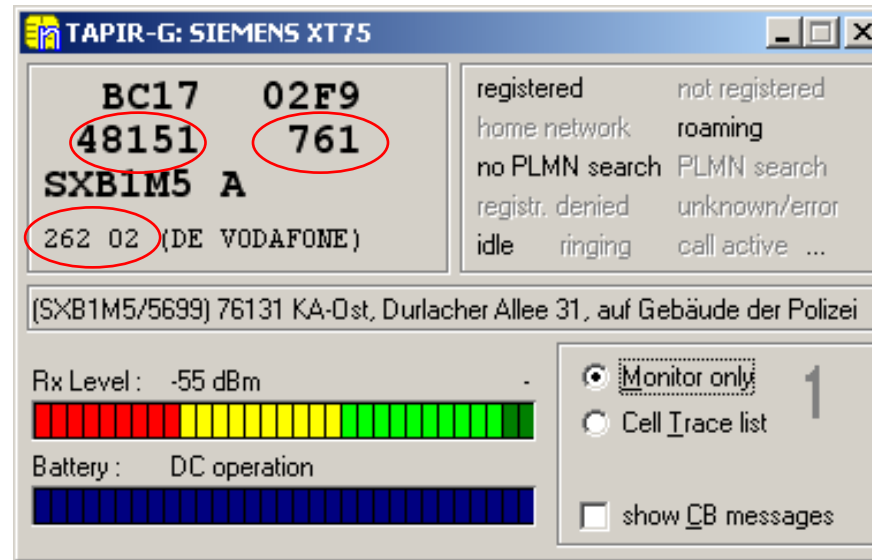
262 – 01 – 38914 – 57564

Aktuelle Position (LAI)

228 – xxx – xxx – xxx

Alternative Tools zum Ermitteln der Location Based ID

TAPIR: NetMonitor mit PC-Unterstützung



Siehe auch [www.nobbi.com/monitor/index.html](http://www.nobbi.com/monitor/index.html)

Alternative Tools zum Ermitteln der Location Based ID

GPS Tracker Peilsender TK102-2



Live Demo [+49 171 9133185]

Siehe auch [www.itakka.at/shop/](http://www.itakka.at/shop/) und [www.positionx.de](http://www.positionx.de)

A vertical decorative strip on the left side of the slide features a close-up image of a computer keyboard with a yellow padlock resting on one of the keys.

Was nun? Die Ermittlung des  
Standortes ist auch eine Frage der  
richtigen Datenbank

Compass Security AG  
Glärnischstrasse 7  
Postfach 1628  
CH-8640 Rapperswil

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

Die Ermittlung des Standortes ist eine Frage der Datenbank.  
Ziel: Cell-ID zu Koordinaten (z.B. UTM-System, Gauß-Krüger, Google etc.)

- ★ Datenbank der Netzbetreiber

**Nachteil:** Non-Public, nur den Netzbetreibern und Behörden zugänglich

- ★ Nutzung freier Datenbanken

- ★ [www.nobbi.com/btsquerydb.html](http://www.nobbi.com/btsquerydb.html)

- ★ <http://sercpos.com>

- ★ [www.opencellid.org](http://www.opencellid.org)

- ★ <http://developer.yahoo.com/yrb/zonetag/locatecell.html>

**Nachteil:** Örtlich begrenzt, unvollständig

- ★ Googledaten???

**Nachteil:** Non-Public

# Ermittlung der Referenzkoordinaten



## Mittels OpenCellID

A screenshot of the OpenCellID website. The page has a blue header with the "opencellid" logo and navigation links: "About", "Stats", "Download", "Api", "Browse cells", "Cells Map", and "Raw data". The main content area is white and contains a "Welcome to OpenCellID" section. A callout box with a black border is overlaid on the right side of the page, containing the text "cell/get" and a list of parameters and their descriptions: "key: The apikey", "mcc: mobile country code (decimal)", "mnc: mobile network code (decimal)", "lac: locale area code (decimal)", and "cellid: value of the cell id". The callout also includes a note about default behavior and an example URL.

**cell/get**

Get the position of a specific cell <http://www.opencellid.org/cell/get?key=myapikey&mnc=1&mcc=2&lac=200&cellid=234>

Where:

- key:** The [apikey](#)
- mcc:** mobile country code (decimal)
- mnc:** mobile network code (decimal)
- lac:** locale area code (decimal)
- cellid:** value of the cell id

lac can be omitted

If cellid is not present or if cellid is unknown, a default return will be based on lac information, but with a much lower accuracy. In that case, cellid return will be -1.

The position will be returned in xml format by default in the following form

Example: <http://www.opencellid.org/cell/get?mcc=250&mnc=99&cellid=29513&lac=0>

# LiveDemo [Use Google's Dataset]

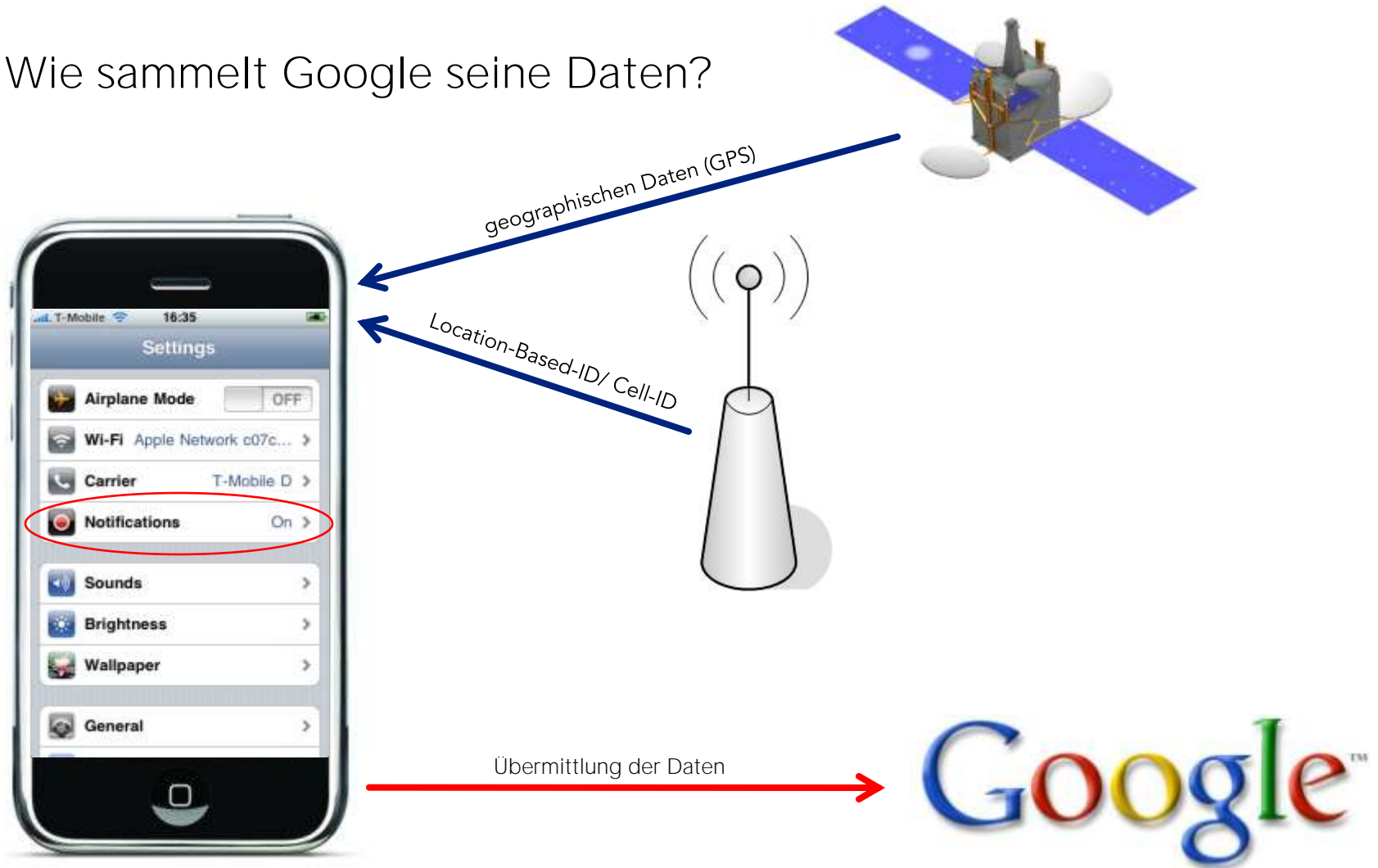
Compass Security AG  
Glärnischstrasse 7  
Postfach 1628  
CH-8640 Rapperswil

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

# Ermittlung der Referenzkoordinaten



Wie sammelt Google seine Daten?



A vertical decorative strip on the left side of the slide shows a close-up of a computer keyboard with a yellow padlock resting on one of the keys.

## Ortung mittels stiller SMS

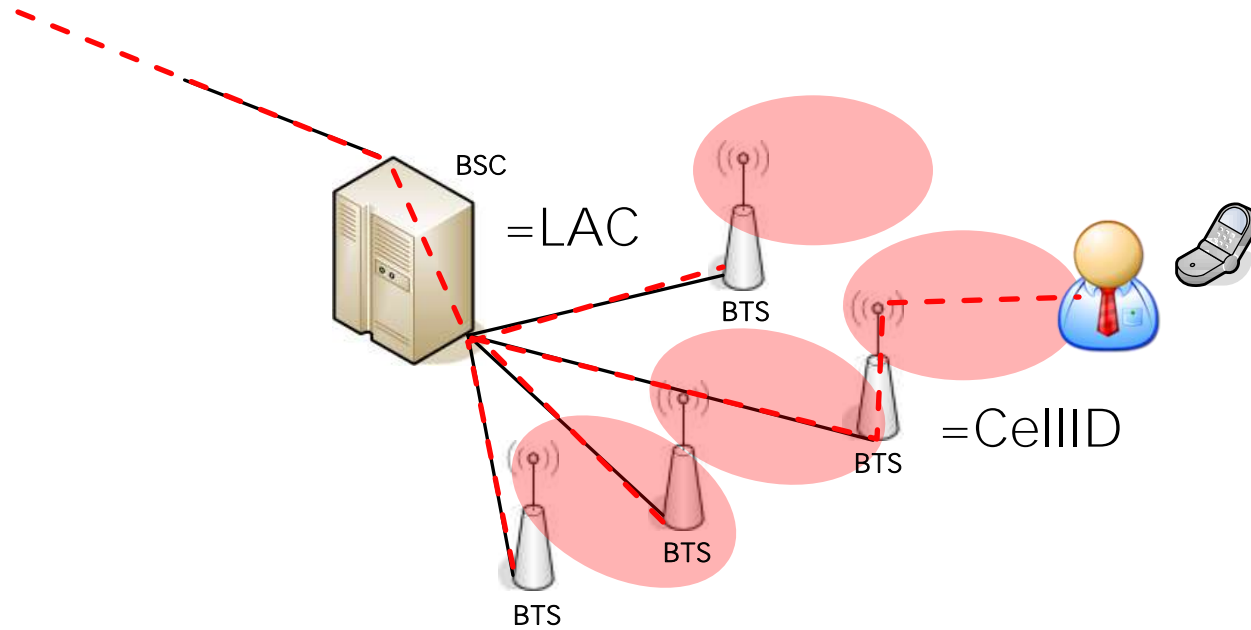
Compass Security AG  
Glärnischstrasse 7  
Postfach 1628  
CH-8640 Rapperswil

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

## Wozu benötigt man die stille SMS

- ✦ Nach Netz-Authentizierung wird nur die Location Area Identity (LAI) im Visitor Location Register (VLR) gespeichert
- ✦ Bei netzseitiger Kontaktaufnahme mit dem Mobiltelefon, rufen alle Basisstation (BTS) innerhalb des BSC nach dem Teilnehmer
- ✦ Information über die benutzten Basisstation während eines Gesprächs oder zum Zeitpunkt des Empfangs/Senden einer SMS zählen nach dem Telekommunikationsgesetz zu den zu speichernden Vorratsdaten
- ✦ Verhält sich bei der Übermittlung wie eine normale SMS, wird aber auf dem Mobiltelefon weder optisch noch akustisch angezeigt
- ✦ Zugriff auf die Datenbank des Netzbetreibers notwendig

# Ortung mittels stiller SMS





# LiveDemo [Stille SMS/PDUspy]

Compass Security AG  
Glärnischstrasse 7  
Postfach 1628  
CH-8640 Rapperswil

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

A vertical decorative image on the left side of the slide shows a close-up of a computer keyboard with a magnifying glass resting on it. A solid blue vertical bar is positioned to the left of the keyboard image.

## Ortung mittels SS7-Protokoll

Compass Security AG  
Glärnischstrasse 7  
Postfach 1628  
CH-8640 Rapperswil

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

Welche Routing-Infos werden zurück gegeben?

- ✦ die IMSI (die „echte“ Rufnummer)
- ✦ Die Kennung der genutzten MSC
- ✦ Benutzer-Fehler (z. B. "Absent Subscriber" == das Telefon ist ausgeschaltet)

# LiveDemo [Ortung mittels SS7 abfrage]

Compass Security AG  
Glärnischstrasse 7  
Postfach 1628  
CH-8640 Rapperswil

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

Auch hier ist die Nutzung der richtigen Datenbank essentiell!

## T-Mobile Germany

## Vodafone Germany

Berlin +491710360000

+491720012097

Hamburg +491710400000

+491720022097

Frankfurt +491710650000

+491720061097

Stuttgart +491710700000

+491720076097

München +491710870000

+491720082097



## Selbsttest [+49 xxx]



Compass Security AG  
Glärnischstrasse 7  
Postfach 1628  
CH-8640 Rapperswil

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

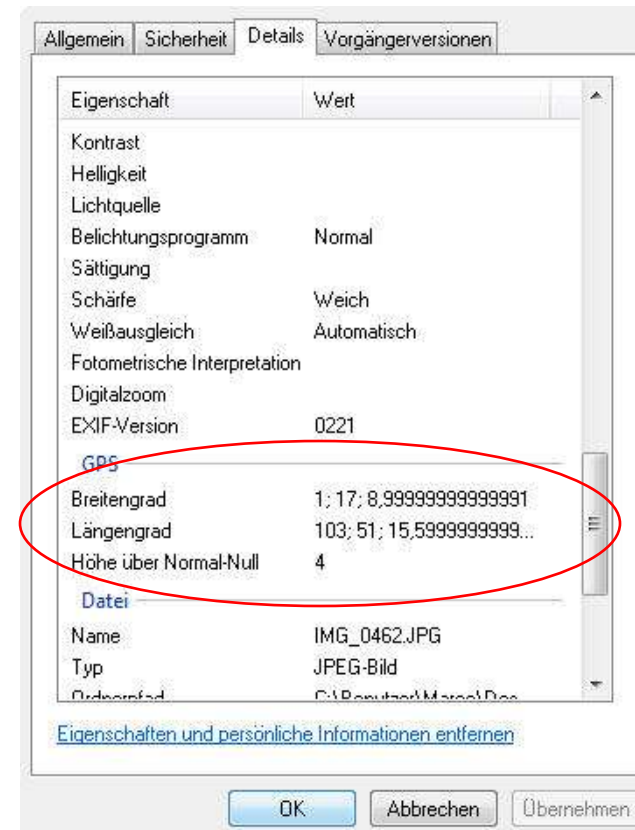
A vertical decorative strip on the left side of the slide. It features a close-up, slightly blurred image of a computer keyboard with a prominent yellow padlock resting on one of the keys. The background of the strip is a solid dark blue color.

## Ach ja... eine kleine Randnotiz...

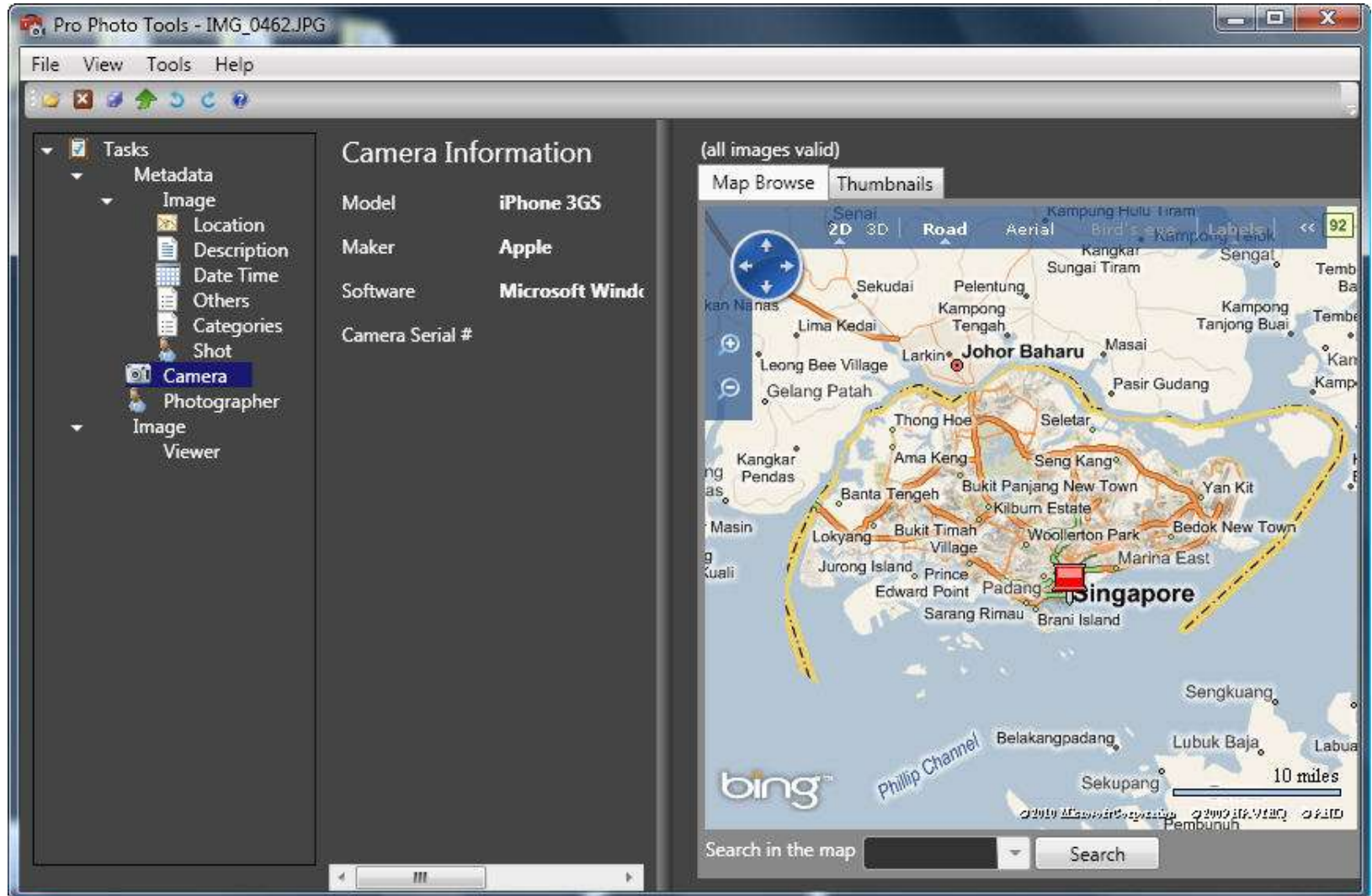
Compass Security AG  
Glärnischstrasse 7  
Postfach 1628  
CH-8640 Rapperswil

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

Übrigens: Wussten Sie, dass Ihr Smartphone GeoTags in Ihren Fotos speichert?



# Ortung durch GPS/Geotagging



Übrigens: Haben Sie mittlerweile die Verschlüsselung Ihres BlackBerrys oder den Zugangsschutz Ihres iPhones aktiviert? Ich hatte Sie eingangs daran **erinnert...**



A vertical decorative image on the left side of the slide. It shows a close-up of a computer keyboard with a yellow padlock resting on one of the keys. The image is slightly blurred and has a blue tint.

# Identifikationsfälschung [Call-ID-Spoofing]


Compass Security AG  
Glärnischstrasse 7  
Postfach 1628  
CH-8640 Rapperswil

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

## Weshalb ein Angriff mittels gefälschter Rufnummer?

- ★ Oft dient die Rufnummer (CLIP) als Identifikationsmerkmal des Anrufers (z.B. bei Telefongesprächen, Fernzugängen, Anwendungen etc.)
- ★ Zugriffsbeschränkungen mittels Rufnummernidentifizierung können umgangen, bzw. beim Social-Engineering unterstützend eingesetzt werden.
- ★ Matching der Rufnummern in EU-Endgeräten erfolgt nur bis zur max. 7. Stelle

## Anbieter kommerzieller Call-ID-Spoofing-Dienste



The screenshot shows the SpoofCard website interface. At the top, there is a navigation menu with links for HOME, BUY CREDITS, FAQ, MEDIA, TESTIMONIALS, SUPPORT, and PIN LOGIN. Below the navigation is a blue banner with the text "Mobile Applications". The main content area is titled "Which device do you own?" and is divided into three columns. The first column is for "Apple iPhone", showing an iPhone with the SpoofCard app interface and instructions to go to iSpooftCard.com. The second column is for "Google Android", showing an Android phone with the SpoofAPP app interface and instructions to search for SpoofAPP in the Android Market. The third column is for "Blackberry", showing a BlackBerry phone with the SpoofAPP app interface and instructions to use the BlackBerry Browser to visit m.spooftapp.com. To the right of the device options is a "Subscribe to our newsletter!" form with fields for "Your Name" and "Your Email Address" and a "Subscribe" button.

<http://spooftcard.com>

## Werkzeuge zum Call-ID-Spoofing

- ✦ Telefonanschluss mit Dienstmerkmal CLIP -no screening-oder
- ✦ SIP-Gateway ins PSTN (z.B. [www.sipgate.de](http://www.sipgate.de))
- ✦ Softphone (z.B. [www.phoner.de](http://www.phoner.de))

A vertical decorative image on the left side of the slide showing a close-up of a computer keyboard with a yellow padlock resting on one of the keys.

## LiveDemo [Call-ID-Spoofing]



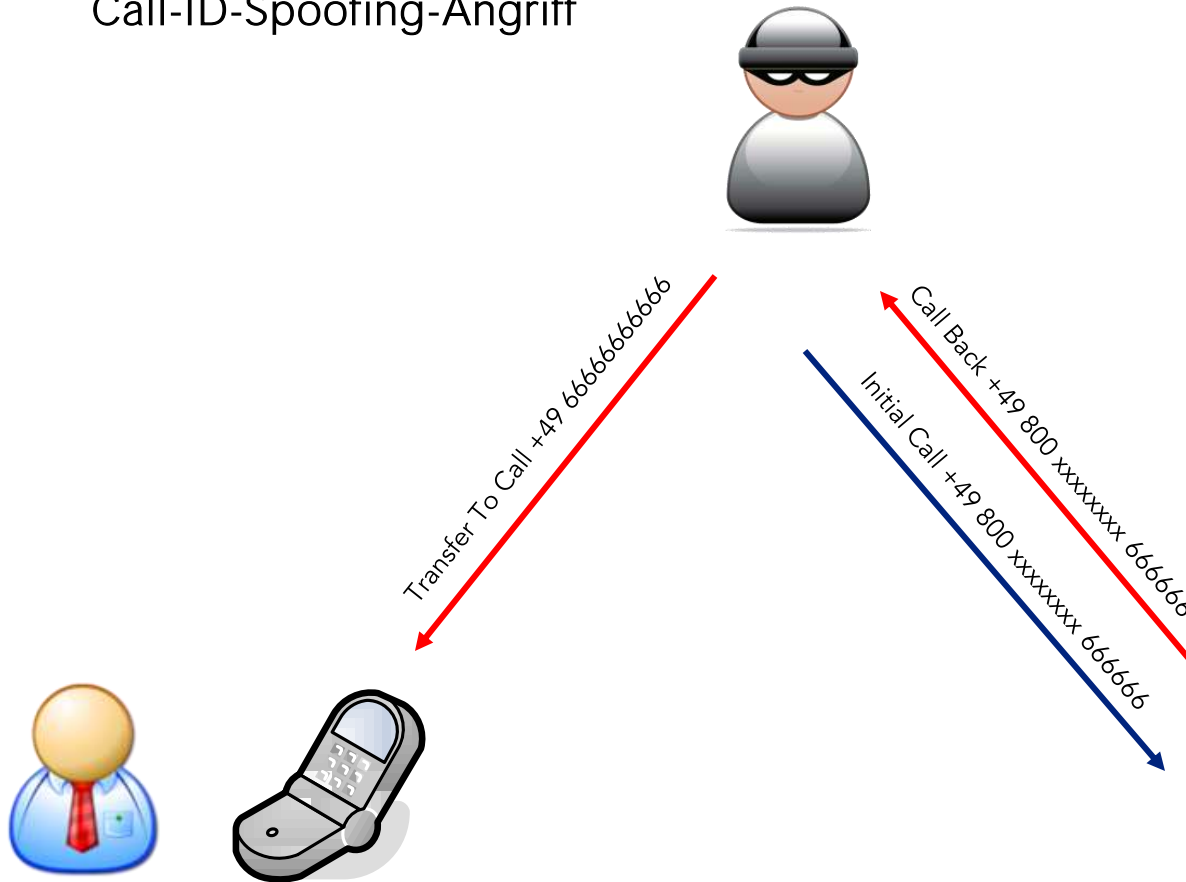
Compass Security AG  
Glärnischstrasse 7  
Postfach 1628  
CH-8640 Rapperswil

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

# Call-ID-Spoofing (MITM-Angriff)



## Call-ID-Spoofing-Angriff



A vertical decorative strip on the left side of the slide features a close-up image of a computer keyboard with a yellow padlock resting on one of the keys.

## Der umgekehrte Fall – ist anonym gleich anonym

Compass Security AG  
Glärnischstrasse 7  
Postfach 1628  
CH-8640 Rapperswil

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

## Werkzeuge zum Call-ID-Identifikation

- ✦ Anbindung als VoIP-Provider ans PSTN  
oder
- ✦ Vermittlungsstelle/Gateway mit Fehlinterpretierung des „Presentation indicator“ (z.B. Betamax GmbH & Co KG/Köln oder KeyCollect SA/Zürich)

Hinweis:

- ✦ **Presentation indicator:** mit diesem Wert kann man festlegen, ob die eigene Rufnummer beim B-TIn. Angezeigt wird oder nicht.
- ✦ **Screening indicator:** dieser gibt an, wie die CgPyNr zustande kam:
  - ✦ User-provided, not screened (in der Vst),
  - ✦ User-provided, verified and passed
  - ✦ User-provided, verified and failed (wird in EDSS1 nicht verwendet)
  - ✦ Network provided: das Netz hat die CgPyNr erzeugt

A vertical decorative image on the left side of the slide showing a close-up of a computer keyboard with a magnifying glass resting on it. A solid blue vertical bar is positioned to the left of the keyboard image.

## LiveDemo [Nummer Identifizieren]



Compass Security AG  
Glärnischstrasse 7  
Postfach 1628  
CH-8640 Rapperswil

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

A vertical decorative strip on the left side of the slide shows a close-up of a computer keyboard with a yellow padlock resting on one of the keys.

Please Call Me [+49 xxx]

Tipp: #31#

A vertical decorative image on the left side of the slide. It shows a close-up of a computer keyboard with a yellow padlock resting on one of the keys. The image is partially obscured by a dark blue vertical bar on the far left.

# Identifikationsfälschung [SMS-ID-Spoofing]

Compass Security AG  
Glärnischstrasse 7  
Postfach 1628  
CH-8640 Rapperswil

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

## Weshalb ein Angriff mittels gefälschter Rufnummer?

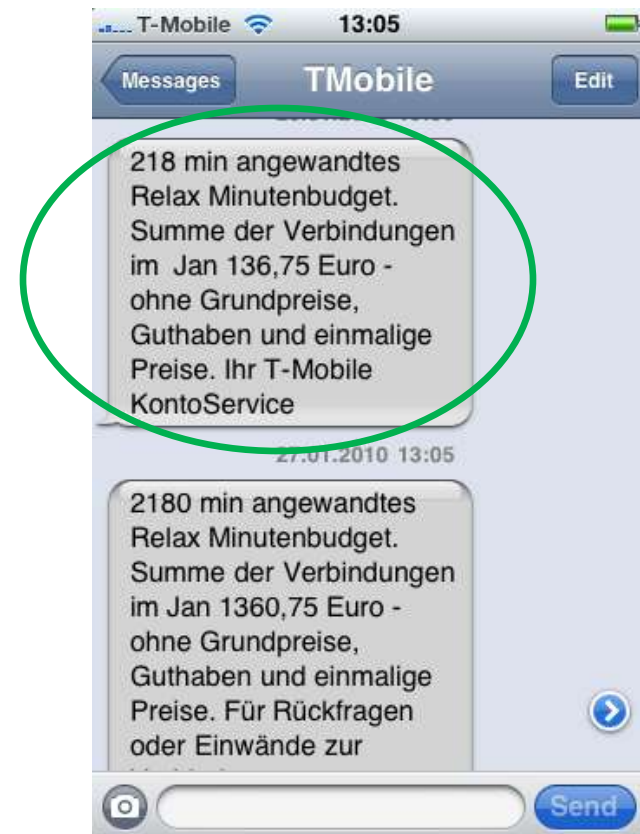
- ✦ Ähnlich wie mittels Rufnummernidentifizierung kann Social-Engineering unterstützend eingesetzt werden.
- ✦ Anstatt Nummern-Identifizierung kann der Absender direkt benannt werden.
- ✦ Phishing via SMS ist noch weitgehend unbekannt und daher aussichtsreicher.
- ✦ Keine Content-Filter vorhanden (wie z.B. bei E-Mails)

## Beispiele



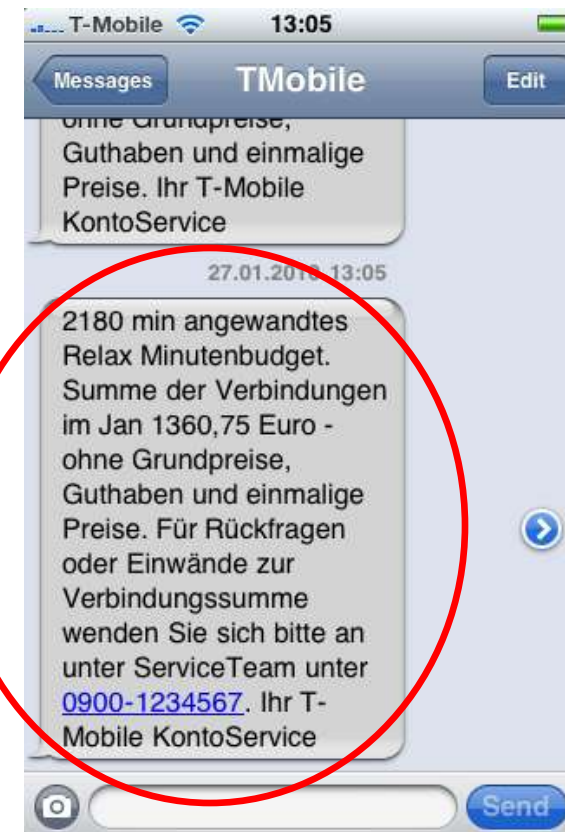
## Beispiel 1: SMS-Phishing mittels SMS-Spoofing

- ★ Beispiel einer Phishing-SMS
- ★ Originalnachricht des Netzbetreibers



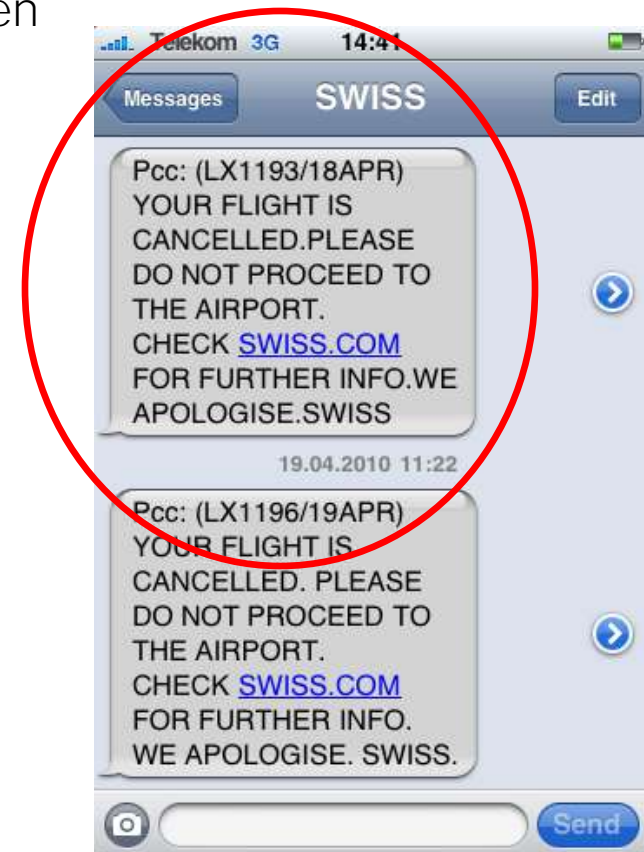
## Beispiel 1: SMS-Phishing mittels SMS-Spoofing

- ★ Beispiel einer Phishing-SMS
- ★ Gefälschte Nachricht auf Grundlage der Netzbetreiber-SMS



## Beispiel 2: SMS-Phishing mittels SMS-Spoofing

- ✦ Den Wettbewerber zuhause lassen



## Werkzeuge zum SMS-ID-Spoofing

- ★ Anbindung an einem SMS-Hub eines Providers (z.B. [www.routomessaging](http://www.routomessaging))

oder

- ★ Zugang zu einem Short Message Service Centre (SMSC)

Beispielsweise:

Germany D2 01722278020 8n1 UCP

Switzerland Swisscom 079 4998990 8n1 UCP

- ★ Schnittstelle als Provider ans SS7

Übertragung zwischen MSC und SMSC erfolgt im MAP (Mobile Application Part) des SS7



# LiveDemo [SMS-ID-Spoofing]

Compass Security AG  
Glärnischstrasse 7  
Postfach 1628  
CH-8640 Rapperswil

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

A vertical decorative strip on the left side of the slide. It features a close-up, slightly blurred image of a computer keyboard with a prominent yellow padlock resting on one of the keys. The background is a light blue/teal color.

## Missbrauch des Soundlogos [Early Media]

Compass Security AG  
Glärnischstrasse 7  
Postfach 1628  
CH-8640 Rapperswil

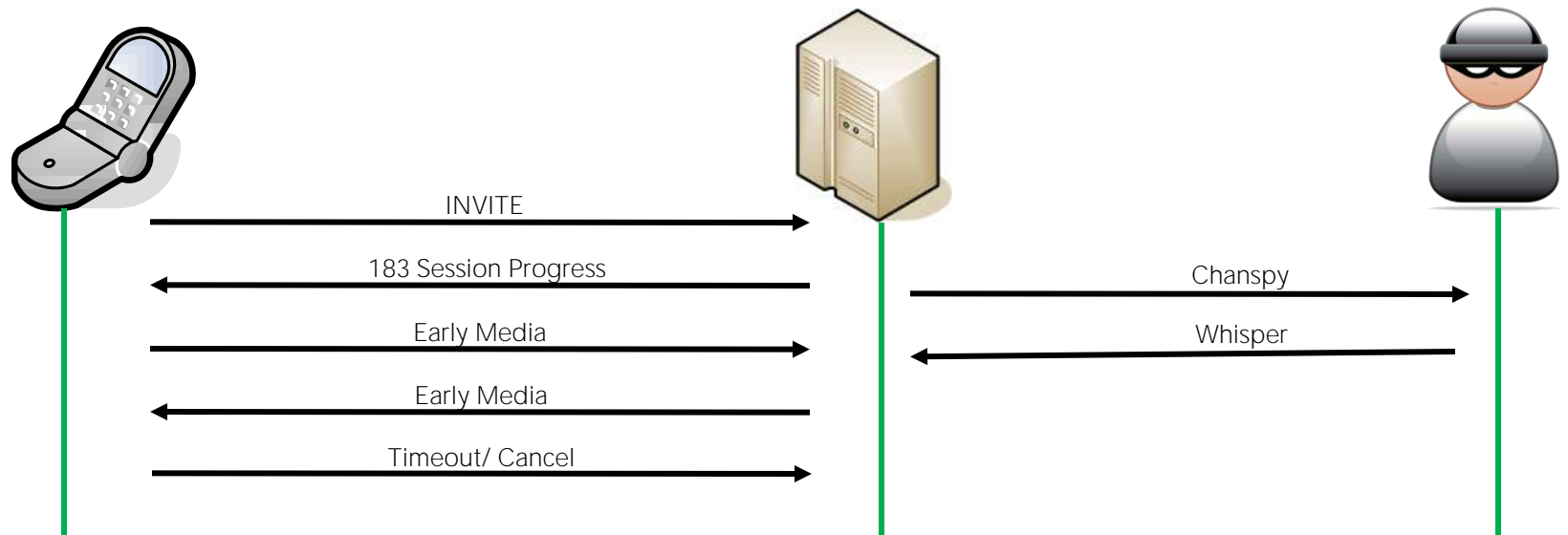
Tel.+41 55-214 41 60  
Fax+41 55-214 41 61  
team@csnc.ch  
www.csnc.ch

## Der Early Media Stream

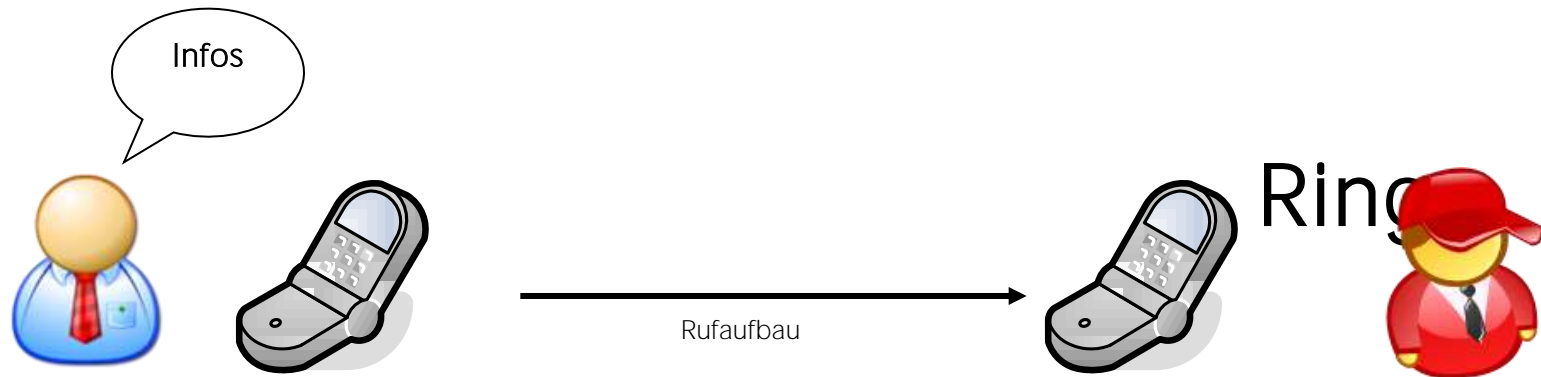
- ✦ Übermittelt bereits während des Rufaufbaus Audioinformationen
- ✦ Eigentlich für individuelle Freizeichen und Ansagen wie „Kein Anschluss unter dieser Nummer“, „Teilnehmer ist vorübergehend nicht erreichbar“ und Preisansagen gedacht
- ✦ Erfolgt vor dem Verbindungsaufbau und ist daher kostenfrei

## Nutzung von „Chanspy“ und „Whisper“ unter Asterisk

- ★ Ursprünglich zu Schulungszwecken in Callcenter entwickelt
- ★ Umgehung von Vorratsdatenspeicherung
- ★ Mikrofone von Teilnehmern sind schon während der Rufphase geöffnet
- ★ Erfolgt vor dem Verbindungsaufbau und ist daher kostenfrei



Gespräche belauschen während des Freitons



A vertical decorative strip on the left side of the slide. It features a close-up, slightly blurred image of a computer keyboard with a prominent yellow padlock resting on one of the keys. The background of the strip is a solid dark blue color.

## LiveDemo Lauschangriff [Early Media]



Compass Security AG  
Glärnischstrasse 7  
Postfach 1628  
CH-8640 Rapperswil

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



Please Call Me [+49 xxx]

Compass Security AG  
Glärnischstrasse 7  
Postfach 1628  
CH-8640 Rapperswil

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

A vertical decorative strip on the left side of the slide features a close-up image of a computer keyboard with a prominent yellow padlock resting on one of the keys.

## Selbsttest [+49 xxx]

1. Call (Record)
2. Call (Play Back)

The background of the slide is a close-up photograph of a computer keyboard. A yellow padlock is placed over the keys, symbolizing security. A vertical blue bar is on the left side of the image.

# SIM-Schnittstelle als Angriffsvektor auf mobile Endgeräte [SIM Application Toolkit]

Compass Security AG  
Glärnischstrasse 7  
Postfach 1628  
CH-8640 Rapperswil

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

## Weshalb ein Angriff auf die SIM-Schnittstelle?

- ★ SIM Schnittstelle als universeller Angriffsvektor auf mobile Endgeräte
- ★ Standardisierte Schnittstelle
- ★ Realisierung: Hardware-basierter Man-in-the-middle-Angriff
- ★ Fernwirken von Endgeräten (wie teilweise schon von den Netzbetreibern genutzt)

## Funktionen des SIM Application Toolkit

- ◆ Versand und Empfang von Kurznachrichten (SEND SHORT MESSAGE, SMS-PP Download)
- ◆ Initiieren ausgehender Anrufe (SET UP CALL)
- ◆ Umleiten ausgehender Anrufe (CALL CONTROL)
- ◆ Positionsbestimmung
- ◆ Datenübertragung via GPRS/UMTS
- ◆ Senden von AT-Kommandos an das Endgerät
- ◆ usw..

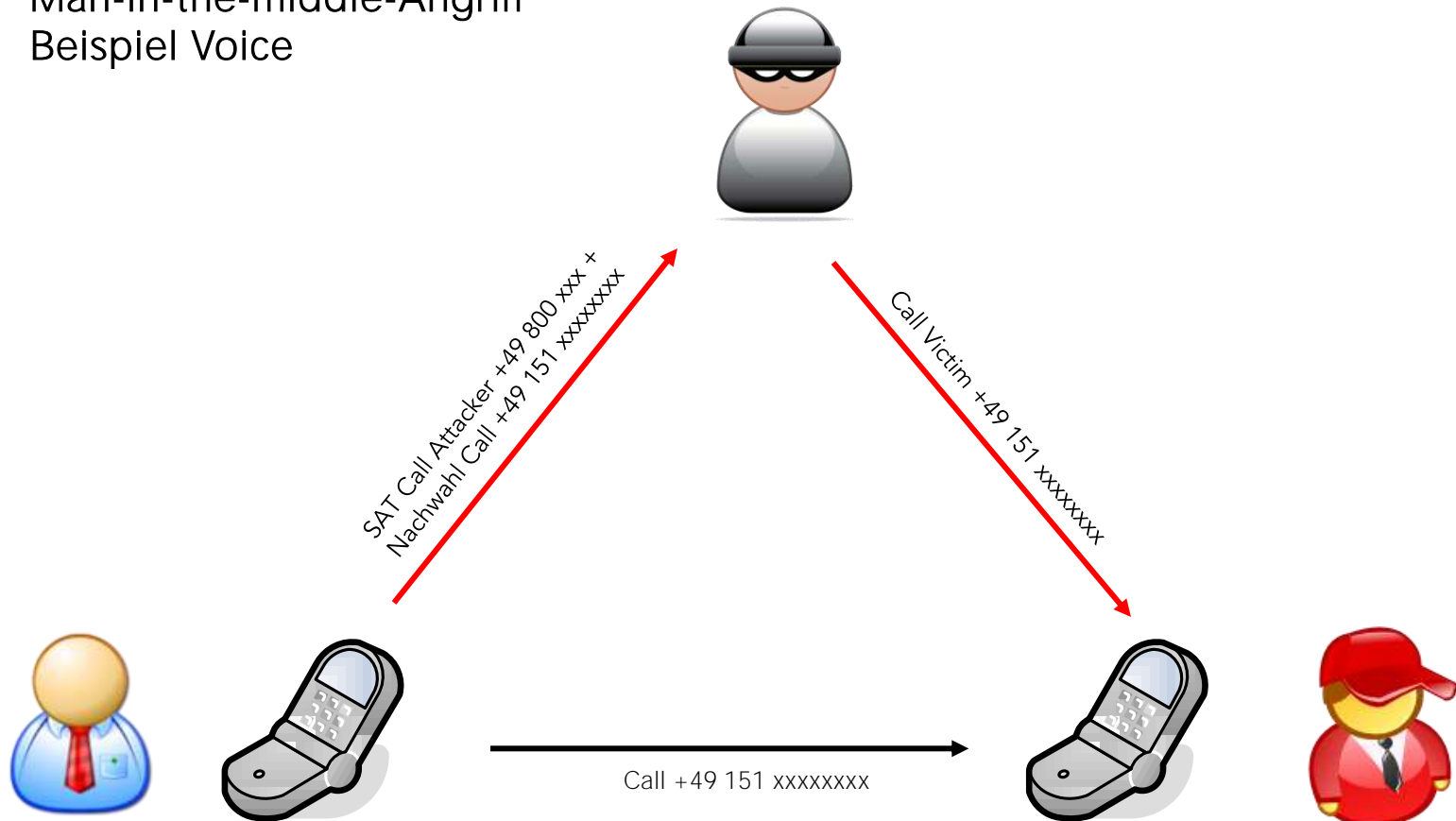
## Funktionsweise eines SAT-Angriffs

- ★ SIM-Karte kann die beschriebenen SAT-Funktionen nutzen
- ★ Keine Kryptografie zwischen SIM und Endgerät
- ★ Einschleusen eigener SAT-Kommandos möglich
- ★ SIM wird weiterhin zur Authentisierung benötigt
  - ★ Man-in-the-middle-Angriff durch Einbau eines Mikrocontrollers

## Entwicklungshistorie



## Man-in-the-middle-Angriff Beispiel Voice





## LiveDemo [SAT-Angriff]

Compass Security AG  
Glärnischstrasse 7  
Postfach 1628  
CH-8640 Rapperswil

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

Und? Haben Sie Ihre Sicherheitsfeatures  
aktiviert? Nein? Zu spät!  
**All Your Data Belong To Us.....**



Compass Security AG  
Glärnischstrasse 7  
Postfach 1628  
CH-8640 Rapperswil

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

A vertical decorative strip on the left side of the slide shows a close-up of a computer keyboard with a yellow padlock resting on one of the keys.

# Angriffe auf mobile Endgeräte mittels Malware [Trojaner & Co.]

Compass Security AG  
Glärnischstrasse 7  
Postfach 1628  
CH-8640 Rapperswil

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

Handyviren/Mobile Phone Malware sind Schadprogramme, die sich in mobile Geräte einschleusen

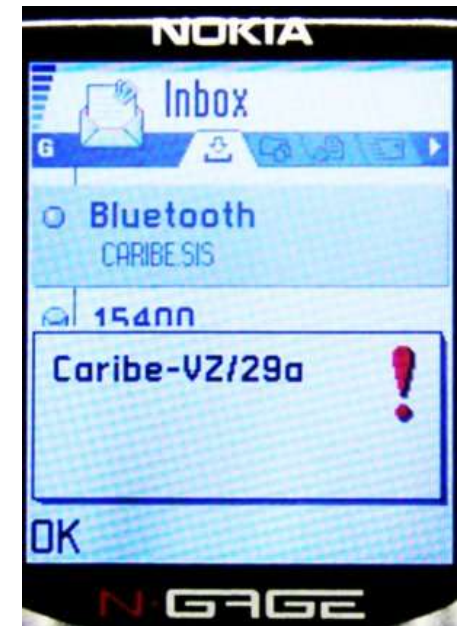
- ✦ Lange Zeit waren Handys geschützt, da sie geschlossene Systeme darstellten.
- ✦ Die Vielzahl der Schnittstellen (E-Mail, Bluetooth, W-LAN, Messaging, Spiele und Logos zum Download sowie Bluetooth, UMTS etc.) mit der Außenwelt stellt ein potenzielles Einfallstor für die „Malware“ dar.
- ✦ Software Development Kits (SDK) stehen frei zur Verfügung – jeder kann diese für seine „Entwicklungen“ nutzen.
- ✦ Systeme verfügen in aller Regel über keinerlei (mitgelieferten) Sicherheitsfunktionen.
- ✦ Endgeräte stehen oftmals ungeschützt im Internet (W-LAN, UMTS etc.).
- ✦ Smartphone liegen oft unbeobachtet herum.
- ✦ Endgeräte sind oftmals nicht Bestandteil des Security-Konzepts.
- ✦ Viele User nutzen ihre Endgeräte ohne Passwort-Schutz.

Wie kommen Trojaner und Spyware auf mobile Geräte?



Einer der ersten war Cabir → nutzt zur Verbreitung Bluetooth

- ✦ Ein Handy-Wurm, der sich über Bluetooth auf Smartphones mit dem Betriebssystem Symbian OS verbreitet – mit hohem Verbreitungspotential. Betroffen sein könnten Nokia Smartphones der 60er-Serie, N-Gage, Panasonic X700, Siemens SX-1, Sendo X und andere.



## Sexy Space: Handy-Trojaner mit Zertifizierung

- ✦ Der Trojaner "Sexy Space" erhielt eine digitale Signatur für Symbian-Handybetriebssysteme.
- ✦ Der Schädling vernetzt sich mit anderen befallenen Geräten und klagt Benutzerdaten, um Spam per E-Mail oder SMS an die auf dem Handy gefundenen Kontakte zu senden.
- ✦ Kann hohe SMS-Kosten verursachen



## Java/Swapi.B: Der Java-Dialer versendet Premium-SMS

- ✦ Nach der Infektion schickt diese Malware regelmäßig SMS an teure Premium-Dienste.
- ✦ Da der Trojaner auf einer J2ME-Engine basiert, die auf nahezu 90 Prozent der im Markt erhältlichen Telefone installiert ist, lässt er sich nicht auf ein spezifisches Handy festlegen.

```
[INFO] [sms      ] ## javacall: SMS sending...

#####
Outgoing SMS : <finsex ██████████
#####
[INFO] [sms      ] ## javacall: SMS sending...

#####
Outgoing SMS : <finsex ██████████
#####
[INFO] [sms      ] ## javacall: SMS sending...

#####
Outgoing SMS : <finsex ██████████
#####
[INFO] [sms      ] ## javacall: SMS sending...

#####
Outgoing SMS : <finsex ██████████
#####
[INFO] [sms      ] ## javacall: SMS sending...

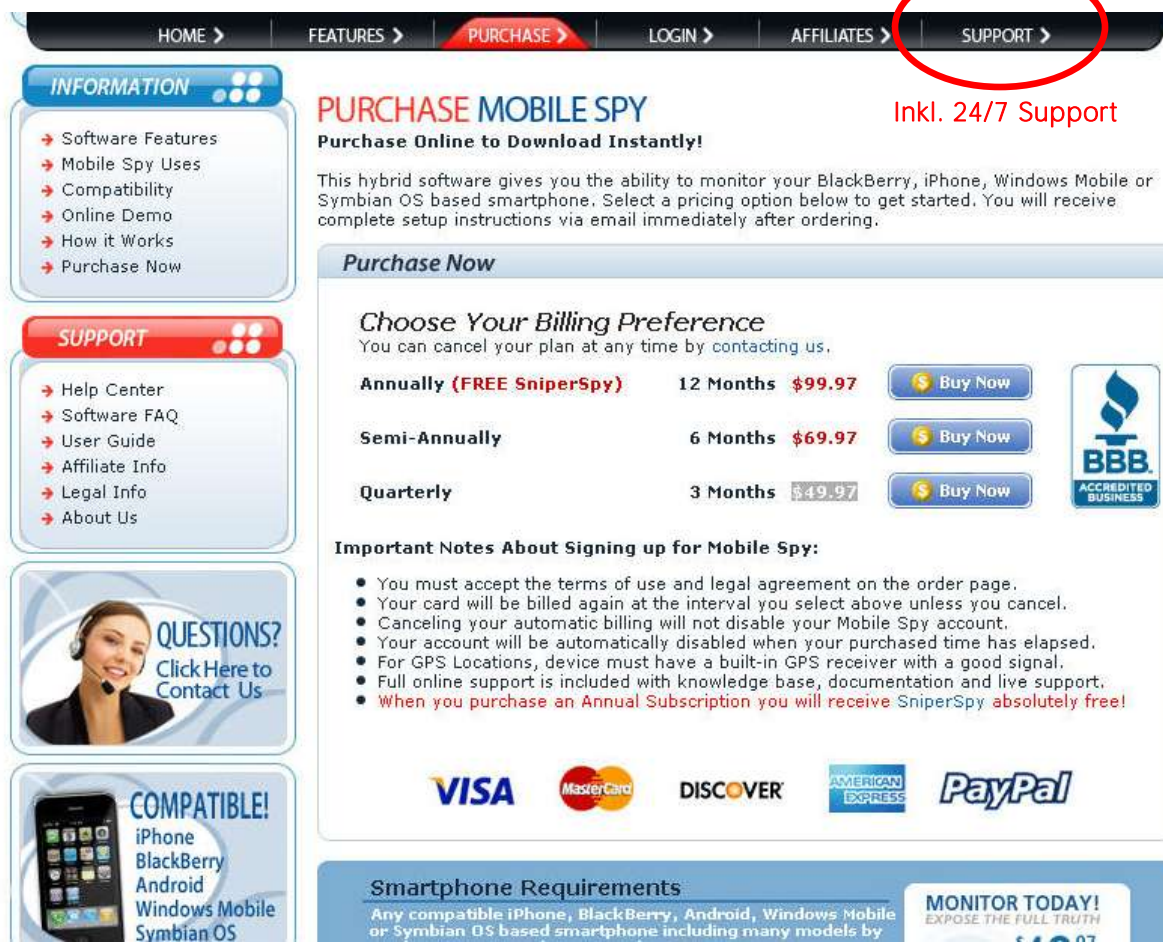
#####
Outgoing SMS : <munet ██████████
#####
```

ikee: Bringt Popsängers Rick Astley zu erneuten Ruhm

- ★ Proof-of-Concept: Der Wurm ist nach Malware-Maßstäben relativ harmlos.
- ★ Er ersetzt lediglich das aktuelle Hintergrundbild dauerhaft durch ein Foto des Sängers Rick Astley.
- ★ Danach macht er sich auf die Suche nach weiteren Geräten, die er infizieren kann.



## Kommerzielle Trojaner: MOBILE SPY überwacht iPhone und viele anderen Handys ab \$49.00 im Quartal



Navigation: HOME > FEATURES > **PURCHASE >** LOGIN > AFFILIATES > SUPPORT >

**INFORMATION**

- Software Features
- Mobile Spy Uses
- Compatibility
- Online Demo
- How it Works
- Purchase Now

**SUPPORT**

- Help Center
- Software FAQ
- User Guide
- Affiliate Info
- Legal Info
- About Us

**QUESTIONS?**  
Click Here to Contact Us

**COMPATIBLE!**  
iPhone  
BlackBerry  
Android  
Windows Mobile  
Symbian OS

**PURCHASE MOBILE SPY** Inkl. 24/7 Support  
**Purchase Online to Download Instantly!**

This hybrid software gives you the ability to monitor your BlackBerry, iPhone, Windows Mobile or Symbian OS based smartphone. Select a pricing option below to get started. You will receive complete setup instructions via email immediately after ordering.

**Purchase Now**

**Choose Your Billing Preference**  
You can cancel your plan at any time by contacting us.

Billing Preference	Duration	Price	Buy Now
<b>Annually (FREE SniperSpy)</b>	12 Months	<b>\$99.97</b>	Buy Now
<b>Semi-Annually</b>	6 Months	<b>\$69.97</b>	Buy Now
<b>Quarterly</b>	3 Months	<b>\$49.97</b>	Buy Now

**Important Notes About Signing up for Mobile Spy:**

- You must accept the terms of use and legal agreement on the order page.
- Your card will be billed again at the interval you select above unless you cancel.
- Canceling your automatic billing will not disable your Mobile Spy account.
- Your account will be automatically disabled when your purchased time has elapsed.
- For GPS Locations, device must have a built-in GPS receiver with a good signal.
- Full online support is included with knowledge base, documentation and live support.
- **When you purchase an Annual Subscription you will receive SniperSpy absolutely free!**

Payment Methods: VISA, MasterCard, DISCOVER, AMERICAN EXPRESS, PayPal

**Smartphone Requirements**  
Any compatible iPhone, BlackBerry, Android, Windows Mobile or Symbian OS based smartphone including many models by

**MONITOR TODAY!**  
EXPOSE THE FULL TRUTH

## Kommerzielle Trojaner: Der Klassiker „FlexiSpy“.



The screenshot shows the FlexiSpy website interface. At the top, the logo reads 'FLEXISPY' with a magnifying glass icon over a mobile phone, and the tagline 'Protect Your Children | Catch Cheating Spouses'. A navigation menu includes 'Home', 'Features', 'Phones', 'News', 'Demo', 'Support', 'Reseller', 'Affiliates', 'About Us', and 'Cart'. There are also flags for the UK, Germany, and Russia. The main content area features a promotional banner with the text 'Is Someone Keeping Secrets from You? Reveal All with the Worlds Most Powerful Spyphone'. Below this, there are three bullet points describing the software's capabilities. To the right of the banner, there is a section titled 'FlexiSpy America' with a red circle highlighting links for 'Blackberry Start here', 'Nokia Start here', 'Win Mobile Start here', and 'iPhone Start here'. Below the banner, there are two product listings: 'FLEXISPY - PRO-X' and 'NEW FLEXISPY iPhone'. Each listing includes a 'FULL DETAILS' link and a list of features. The 'PRO-X' listing includes features like 'Listen to actual phone calls', 'Use as a secret mobile gps tracker', and 'Includes all PRO features'. The 'iPhone' listing includes features like 'Secretly read SMS, Email, Call Logs', 'Track location on map', and 'Make secret spy calls'. Both listings have an 'ORDER NOW: €250.0 (per year)' button. At the bottom right of the screenshot, there is a 'START' button with a play icon. Below the product listings, there is a section titled 'HOW CAN FLEXISPY HELP YOU' with a list of use cases: 'UNCOVER Employee espionage', 'CATCH cheating husbands and cheating wives', and 'TRACK THEIR location using GPS'.

Für fast alle Plattformen verfügbar...

www.flexispy.com

## Kommerzielle Trojaner: Der Klassiker „FlexiSpy“.

- ★ Konfigmenü von FlexiSpy



flexispy.com

## Kommerzielle Trojaner: Der Klassiker „FlexiSpy“.

- ★ Konfigmenü von FlexiSpy



flexispy.com

## Kommerzielle Trojaner: Der Klassiker „FlexiSpy“.

A screenshot of the FlexiSpy web interface. At the top, there is a navigation menu with tabs for "All", "Voice", "SMS", "Email", "Location", "System", "Search", "Download", "GPS Tracking", "My Profile", and "I Need Help". Below the menu is a "Log Detail" section with a light beige background. The log entry shows the following information:

#: 1  
IMEI: 011773000316504  
Client Time: **27/01/10 11:31:57**  
Server Time: 27/01/10 11:34:12  
Event Type: SMS  
Direction: IN  
Phone Number: BahnComfort  
Contact Name: BahnComfort  
Contents: Ihre Buchung vom 27.01.2010 wurde unter der Auftragsnummer 824567110 zur Abholung am Automaten hinterlegt. Gute Reise, Ihre DB

At the bottom of the log entry, there are links for "Back", "< Previous", and "Next >".

## Wie sammelt FlexiPsy die User-Daten?



Der Trojaner übermittelt alle Daten wie SMS, Calls, eMail, etc. in definierten Intervallen direkt an den Server.



Der Angreifer kann die Daten jederzeit übers Internet abrufen.



A vertical decorative strip on the left side of the slide shows a close-up of a computer keyboard with a yellow padlock resting on one of the keys.

## LiveDemo [Handy-Trojaner]

Compass Security AG  
Glärnischstrasse 7  
Postfach 1628  
CH-8640 Rapperswil

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

A vertical decorative strip on the left side of the page features a close-up photograph of a computer keyboard with a yellow padlock resting on one of the keys.

## Resümee

Compass Security AG  
Glärnischstrasse 7  
Postfach 1628  
CH-8640 Rapperswil

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

Beziehen Sie mobile Endgeräte unbedingt in Ihren Security überlegen mit ein!

## Ansatzpunkte:

- ★ Sensibilisierung der Anwender
- ★ Implementierung eines Mobile Device Managements (siehe auch Open Mobile Alliance Standard – OMA Device Management)
  - ★ Backup
  - ★ Update
  - ★ Sicherheitseinstellungen
  - ★ Fernlöschung und Ortung bei Diebstahl
- ★ Verwendung von Firewall und Virens Scanner (ggf. von Drittanbietern)
- ★ Reglementierung von Anwenderzugriffen
  - ★ Passwort-Richtlinien

Fragen?!



Vielen Dank!



Vielen Dank für Ihre  
Aufmerksamkeit!

# Kontakt



Compass Security Network Computing

**Glärnischstrasse 7  
Postfach 1628  
CH - 8640 Rapperswil**

**team@csnc.ch | www.csnc.ch | +41 55 214 41 60**

** Secure File Exchange: [www.csnc.ch/filebox](http://www.csnc.ch/filebox)**

**PGP-Fingerprint:**

