



Gibt es einen Business Case für Hacking?



Gibt es einen Markt für illegale Güter?



Sind wir verwundbar?



**Sind wir vorbereitet?
Bereit für den Cyber Warfare?**

Ethical Hacker / Penetration Tester



Gründer & CEO Compass Security AG, Switzerland

Lecturer @ University of Applied Science Rapperswil



Lecturer @ University of Applied Science Lucerne



Lecturer @ University of St.Gallen



Speaker @ **BlackHat Las Vegas 2008**
SmartCard (In) Security



Speaker @ **IT Underground Warsaw 2009**
Advanced Web Hacking



Speaker @ **Swiss IT Leadership Forum Nice 2009**
Cyber Underground



Founder **Swiss Cyber Storm** Sec Conference
next in May 2011



Board member of the Information Security
Society Switzerland (**ISSS**)



The Swiss Security Conference 2011



CYBERSTORM 2011
THE SWISS CONFERENCE ON IT SECURITY TECHNOLOGY
12-15 MAY 2011 / RAPPERSWIL SG

"New Hacking-Lab LiveCD v4.3 available!
<http://www.hacking-lab.com/news/> @swisscyberstorm
via

Home | Conference Program | Speakers | Travel & Hotel | Impressions | Register | Sponsors | Community

Internationale Speaker / 4-day Conference / 12-15 Mai 2011

- ✦ Gloor USA (MIT) Forecast the Future
- ✦ Chiesa (ITA) Hacker Profiling Project
- ✦ Nikkels (CH, UBS) Investigation Team
- ✦ Henauer (CH, MELANI) NDB (Nachrichtendienst)
- ✦ Beek (NL) Virtualization / Research
- ✦ FBI Agent (UK) Not confirmed yet

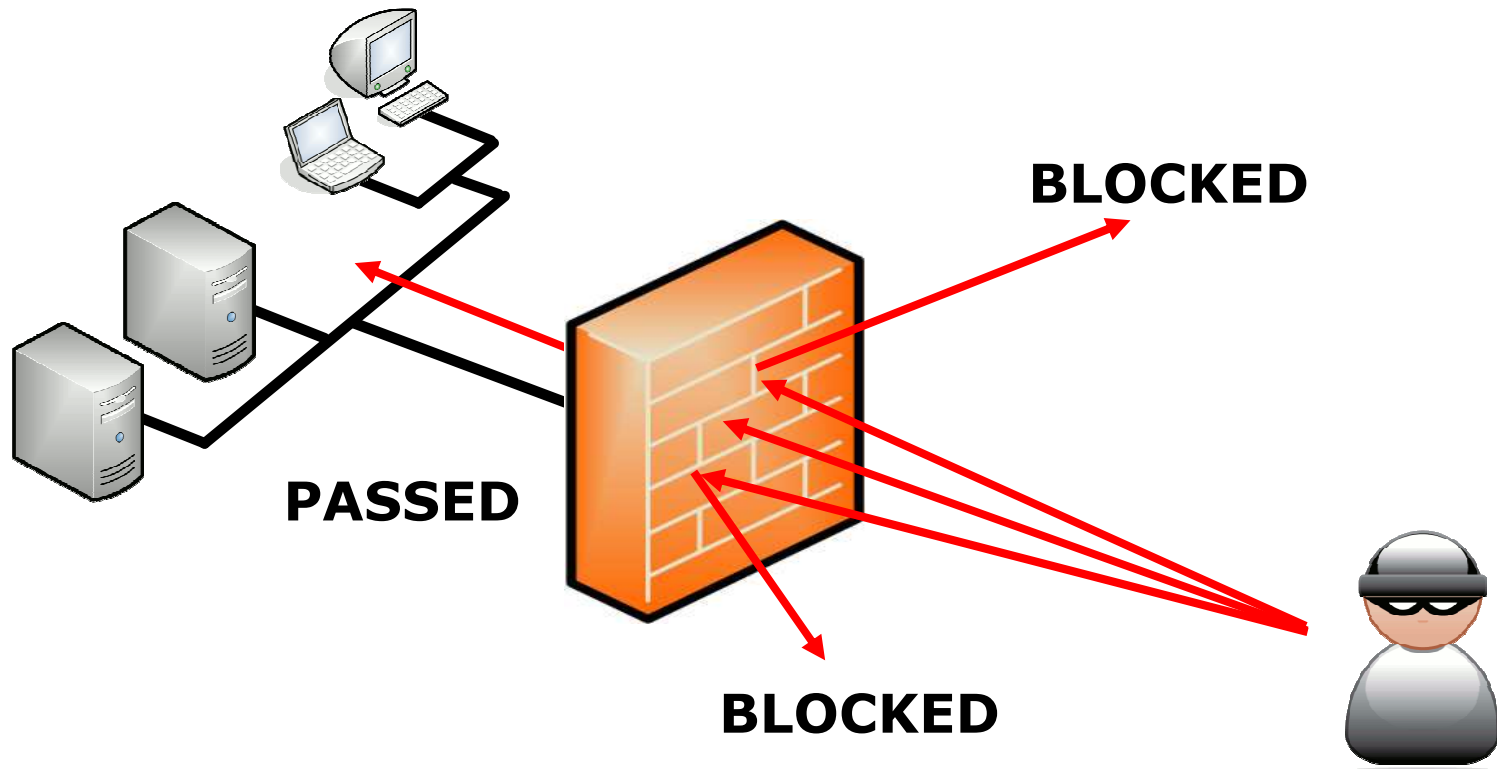
<http://www.swisscyberstorm.com/>

Direkte Attacken



Web Server Hacking – VPN Zugänge – Internet Angriffe

Denial of Service – Distributed Denial of Service, Spam





DEMO SQL INJECTION

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

Ghost Market



A New Era To Virtual Marketing

GhostMarket CC Shop

Search...

GO

Advanced s

GhostMarket.Net A New Era to Virtual Marketing

[Board index](#)

It is currently Tue Jun 02, 2009 11:37 am

[View unanswered posts](#) • [View active topics](#)

FAQ

REGISTER

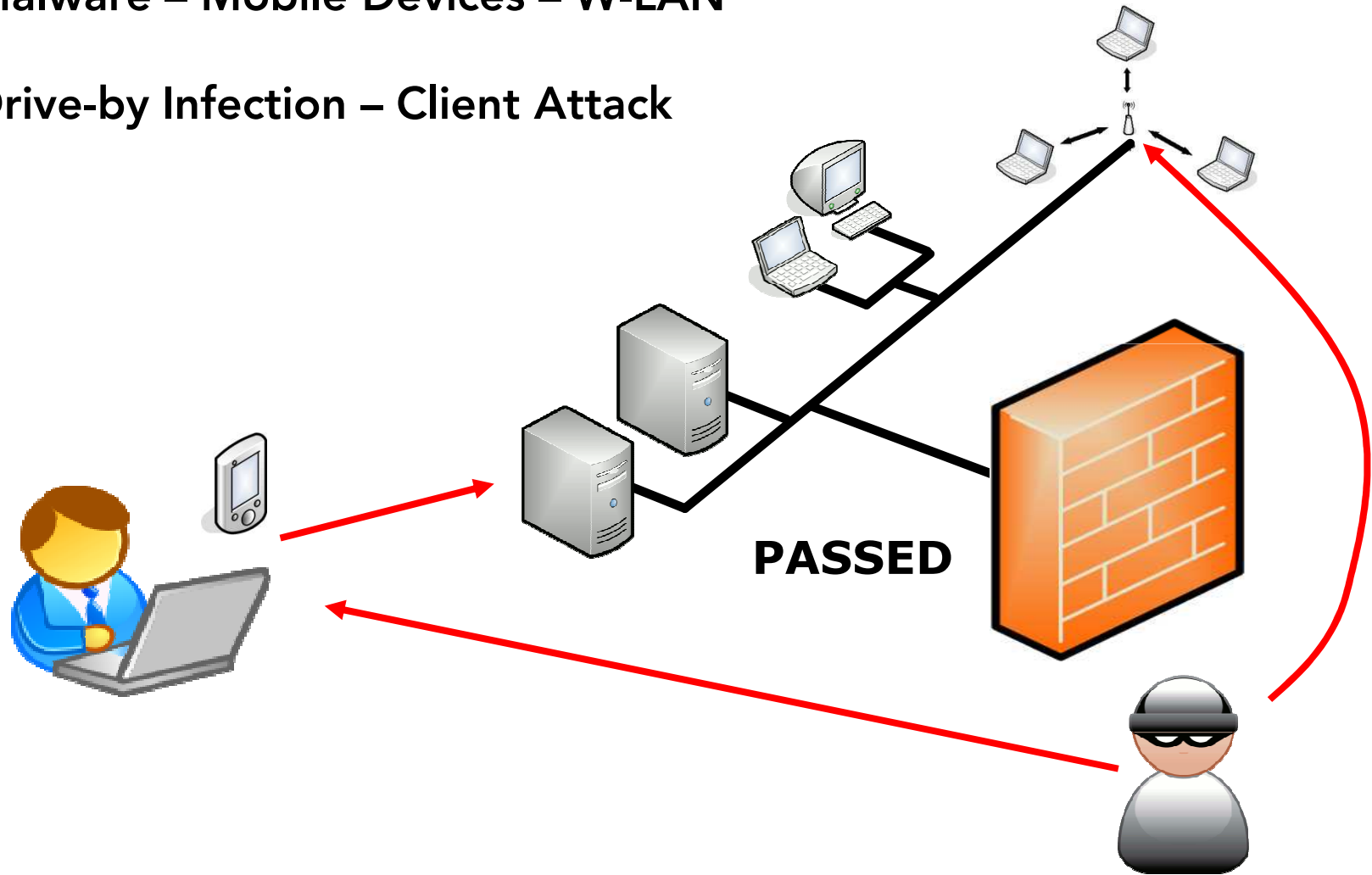
GENERAL	TOPICS	POSTS	LAST POST
Announcements Info about what's going on...	8	94	by shubham Tue Jun 02, 2009 10:30 am
Introductions Introduce yourselves here.	100	567	by N2C Tue Jun 02, 2009 9:43 am
Chat / Off Topic General Chat and off topic chat.	100	1028	by Tue Jun 02, 2009 11:07 am
Suggestions I can't run this site by myself, so suggestions are welcome	32	216	by N2C Mon Jun 01, 2009 5:32 pm
Help General Help	72	548	by Verified Mon Jun 01, 2009 9:56 pm
Show Off Show us your skills here...	85	663	by HCapost Tue Jun 02, 2009 10:48 am
Trusted Apply to be a Trusted Member Here...	44	306	by HCapost Tue Jun 02, 2009 10:37 am

Indirekte Attacken



Malware – Mobile Devices – W-LAN

Drive-by Infection – Client Attack





DEMO USB TROJAN

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

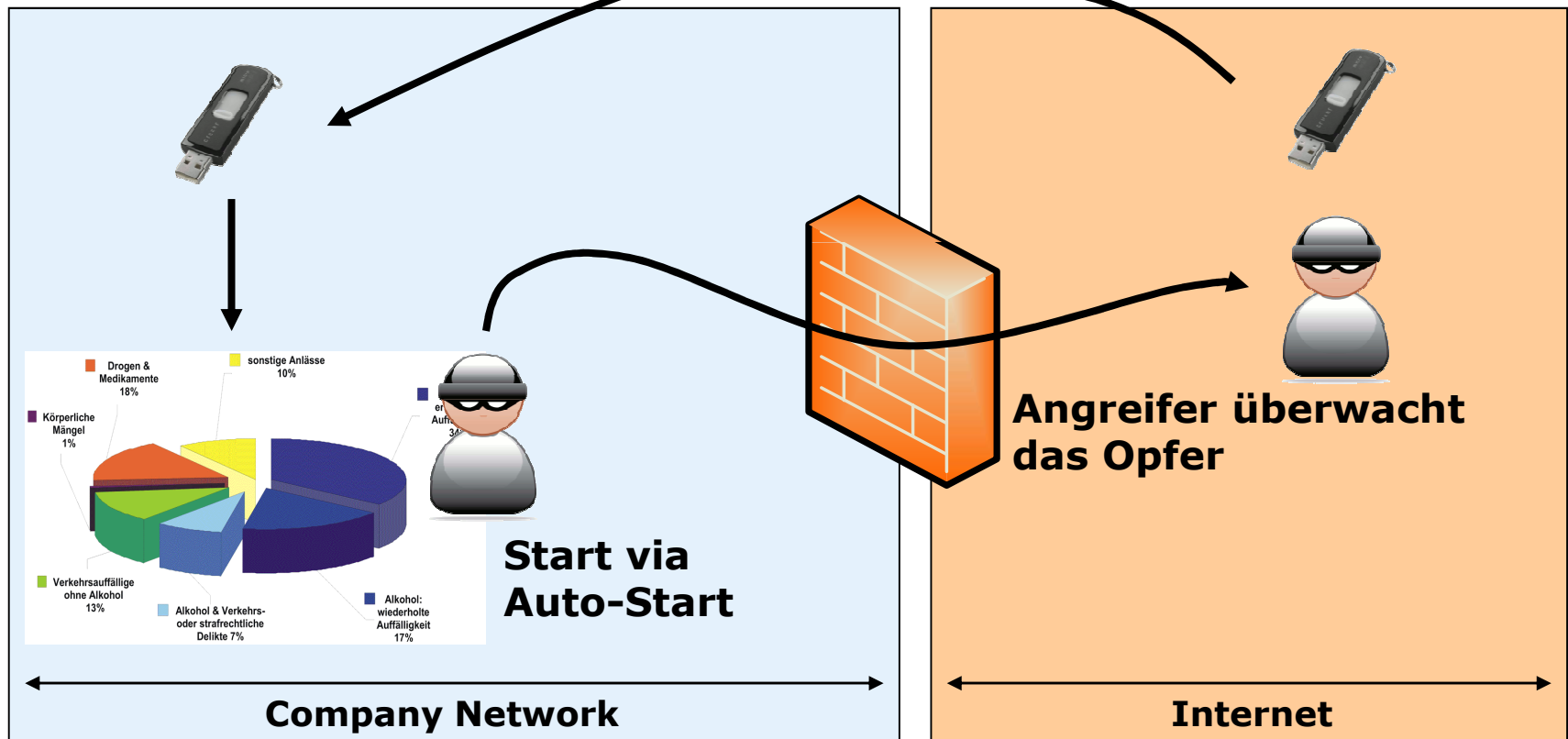
Tel.+41 55-214 41 60
Fax+41 55-214 41 61
team@csnc.ch
www.csnc.ch

USB Stick Angriff - MELANI

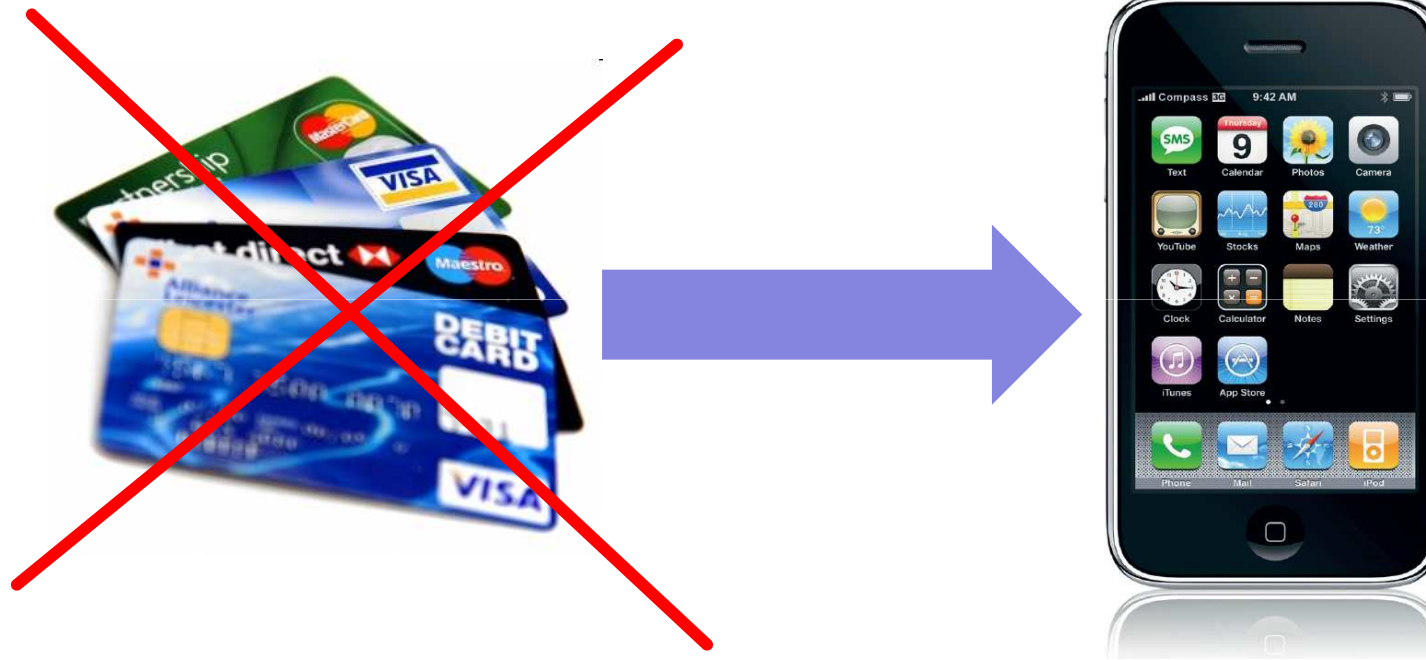


Covert Channel & Inside-Out

Trojaner Lieferung auf USB Stick



Zahlungssysteme





Demo iPhone

iPhone Hacking @ Compass Event – 9. September 2010
www.csnc.ch/event

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

Cyber Market – Illegale Güter



JOIN THE BATTLE

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

5000 Unexpired/Valid CC

Dumps \$2000

Money Rule: Wie kann man die Ware zahlen?



Payment mit Liberty Reserve

>5000 Unexpired/Valid CC Dump \$2000 OBO

POST REPLY Search this topic... Search

>5000 Unexpired/Valid CC Dump \$2000 OBO

by [Synovore071](#) Mon Jun 01, 2009 2:27 am

I am looking for a buyer who would be interested in a decrypted database containing over 5000 valid and unexpired credit cards. Most are from France(50-70% estimated) and other European countries. I am currently in the process of moving some data around and will provide more specific stats on cards per country when it is complete. Each card will have the owners name, address, postal code, CC number, CVV, and Expiration Date. I am hoping to get around 2000\$ (less than .50 cents a piece) for the entire collection but am open to suggestions and offers.

Payment will be via Liberty Reserve.

Serious inquiries only please!
Minimum Purchase is 20\$ worth
10 Cards = 20\$
50+ cards = 1.50\$ a piece
Next price break is if you buy the whole lot off me =p

Beispiel Credit Card Betrug

Money Rule: Veräusserung Ware

- Dumps Gestohlene Kreditkarten
- Carders Lieferanten von "Dumps"
- Carding Benützung von Dumps
- WU Western Union
- **WMZ** **Web Money**
- WU Western Union
- **LR** **Liberty Reserve**
- CVVs Card Verification Value
- Drops Wiederversand Standort (remailing location)
- Rippers Service, der die CVV verifiziert

Was ist Liberty Reserve?



-> Internet Währung (anonym)

A screenshot of the Liberty Reserve website. The top navigation bar includes the Liberty Reserve logo on the left and "Create Account" and "Login" links on the right. A red horizontal bar separates the header from the main content. On the left side, there is a vertical menu with links: "Security", "Services new!", "Service Fees", "Referral System", "Buy/Sell LR", "Merchants", "Downloads", and "Consumer Alert". Below this menu is a "LR Blog" button. The center of the page features a photograph of a woman in a striped shirt sitting at a desk, working on a laptop and holding a white mug. On the right side, there are sections for "Merchant Of The Week" and "Featured Exchange Services".

Liberty Reserve [Create Account](#) [Login](#)

[Security](#)
[Services new!](#)
[Service Fees](#)
[Referral System](#)
[Buy/Sell LR](#)
[Merchants](#)
[Downloads](#)
[Consumer Alert](#)

LR Blog

Merchant Of The Week

[Hushmail](#) — free, secure and encrypted email accounts.
[Marketiva](#) — popular Forex company!
[Finexo.com](#) — trade Forex & receive 10% deposit bonus!

Featured Exchange Services

[EBuyGold](#) (English, Chinese)
[WMIRK.biz](#) (English)
[LondonGoldExchange.com](#) (accepts credit cards) (English)

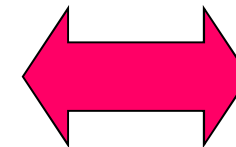
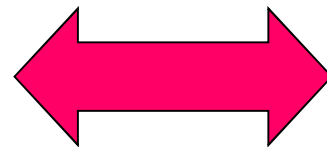
Liberty Reserve als E-Währung



Käufer/Verkäufer brauchen ein LR Konto!

Dann kann man Business betreiben

LR Konto ist anonym



Script Kiddies & Joy Rider



Anonym



Anonym

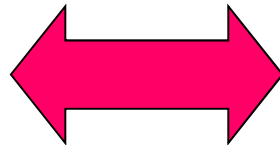
Liberty Reserve setzt „Exchanger“ voraus



Reales Geld wird über Exchanger auf LR Konto überwiesen

Kein direktes „Einzahlen“ auf LR Konto möglich

Es gibt ca. 100 Exchanger Firmen



EXCHANGER



Persönlich

Woher kommt die Anonymität?



Konto bei Liberty Reserve (LR) ist **anonym**

- Eröffnung des Kontos durch Angabe einer E-Mail möglich
- Kaufen/Verkaufen ist anonym

Konto bei „Exchanger“ ist **persönlich**

- Bei der Eröffnung des Konto wird ein Ausweis verlangt

Realisierung „Gewinn“ -> Überweisung LR Konto auf CHF Konto



1/3 Sell ecurrency (c-gold, liberty reserver)

Sell ecurrency : Liberty reserve c-gold

Choose ecurrency:



Max limit for c-gold OutExchange is 1000 EUR (1000 USD)

Max limit for Liberty reserve OutExchange is 1000 EUR (1000 USD)

I sell Liberty Reserve: amount / currency* EUR

To my Bank account: located / currency* EUR

Your Liberty Reserve account: *

BANK DETAILS (ecurrency to bank wire)

Country: *

Bank account number / IBAN *

Bank acc. number / IBAN (confirm) *

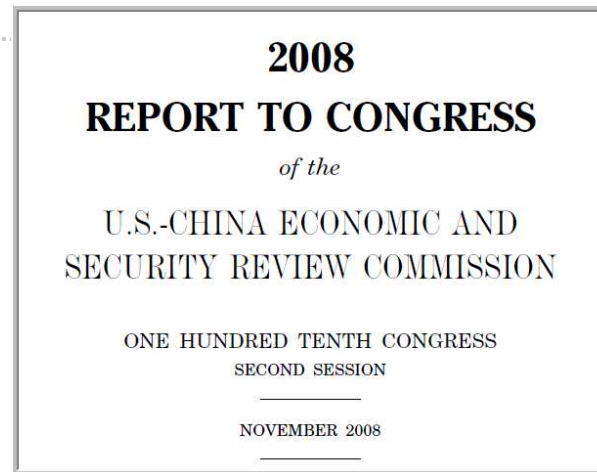
Bank SWIFT / BIC code *

Bank account holder name *

Überweisung des LR Konto auf ein anderes Real-Geld Konto



US Report Nov. 2008



China has an active cyber espionage program. Since China's current cyber operations capability is so advanced, it can engage in forms of cyber warfare so sophisticated that the United States may be unable to counteract or even detect the efforts. By some estimates, there are 250 hacker groups in China that are tolerated and may **even be encouraged** by the government to enter and disrupt computer networks

Business Case: Datenklau



http://www.swissinfo.ch/ger/politik_schweiz/Weg_freie_fuer_Kauf_der_Steuer-CD.html?cid=8236784

Ein anonym Informant offeriert den deutschen Behörden für 2,5 Mio. Euro eine CD mit den gestohlenen Namen von bis zu 1500 Deutschen, die Steuern hinterzogen haben sollen.

A screenshot of the Handelsblatt website. The top navigation bar is orange and contains the date "Montag, 08.02.2010" with a weather icon, and links for "Zeitung", "Abo-/Leser-Services", "Premium-Services", "E-Paper", "Shop", "Veranstaltungen", "Newsletter", and "Jobs". The main header is orange and features the "Handelsblatt" logo in white, a search bar with "Suchbegriff / WKN / ISIN" and a "Suchen" button, and links for "Login Depot/Services", "Premium", and "Registrieren". Below the header is a secondary navigation bar with links for "Startseite", "Finanzen", "Unternehmen", "Politik", "Technologie", "Meinung", and "Magazin". The main content area has a sub-navigation bar with "Deutschland", "International", "Konjunktur", and "Ökonomie". The featured article is titled "NEUE SCHÄTZUNG" and "Steuer-CD soll 400 Mio. Euro wert sein", dated "04.02.2010, aktualisiert 04.02.2010 18:17 Uhr". The article text reads: "Die Landesregierung in Nordrhein-Westfalen hat grünes Licht für den Ankauf der Steuersünder-CD aus der Schweiz gegeben. Credit Suisse steht im Zentrum der Spekulationen um die mutmaßlichen Steuerbetrüger. Bei der Aufklärung der Straftaten haben deutsche Strafverfolgungsbehörden laut Staatsanwaltschaft Berlin die Pflicht, auch Betriebsgeheimnisse zu nutzen."

A vertical decorative image on the left side of the slide. It shows a close-up of a computer keyboard with a yellow sticky note placed on one of the keys. A solid blue vertical bar is positioned to the left of the keyboard image.

Schlussfolgerung

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

Schlussfolgerungen



- Wir sind hochgradig **verwundbar** gegen Hacker Angriffe
- Wir bewegen uns beinahe im Blindflug und verlassen uns zu stark auf Firewall und Anti Virus Produkte
- Der Cyber Underground Markt entwickelt sich ständig

A vertical decorative image on the left side of the page. It shows a close-up of a computer keyboard with a yellow sticky note placed on one of the keys. A solid blue vertical bar is positioned to the left of the keyboard image.

Empfehlungen

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

Was tun für die Zukunft?



- Stellen Sie den Grundschutz vor Script Kiddies sicher.
- Identifizieren Sie die **kritischen Faktoren** für das Überleben des Unternehmen und sichern Sie diese speziell ab, selbst gegen interne Mitarbeiter (weil deren Computer von Hackern missbraucht werden könnten)
- Simulieren Sie Hacking Angriffe – **Penetration Tests**
- Investieren Sie in **Security Monitoring** – um Angriffe überhaupt erst detektieren zu können – Korrelation der Ereignisse
- Bilden Sie ihre Mitarbeiter aus – **Swiss Cyber Storm 3** Konferenz vom 12-15. Mai 2011

Vielen Dank für Ihre Aufmerksamkeit



Wir finden die Löcher

**Compass Security AG
Ivan Bütler
www.csnc.ch**

