



SOPHOS

Compass Security AG

[The ICT-Security Experts]



COMPASS
SECURITY



Live Hacking: Cloud Computing - Sonnenschein oder (Donnerwetter)?
[Sophos – Anatomy of an Attack – 14.12.2011]

Marco Di Filippo

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

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

Agenda



Was ist „Cloud Computing“?

Was ist neu an „Cloud Computing“?

Bedrohungen bei Cloud Services


Angriffsszenarien

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.

Was ist „Cloud Computing“?

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

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

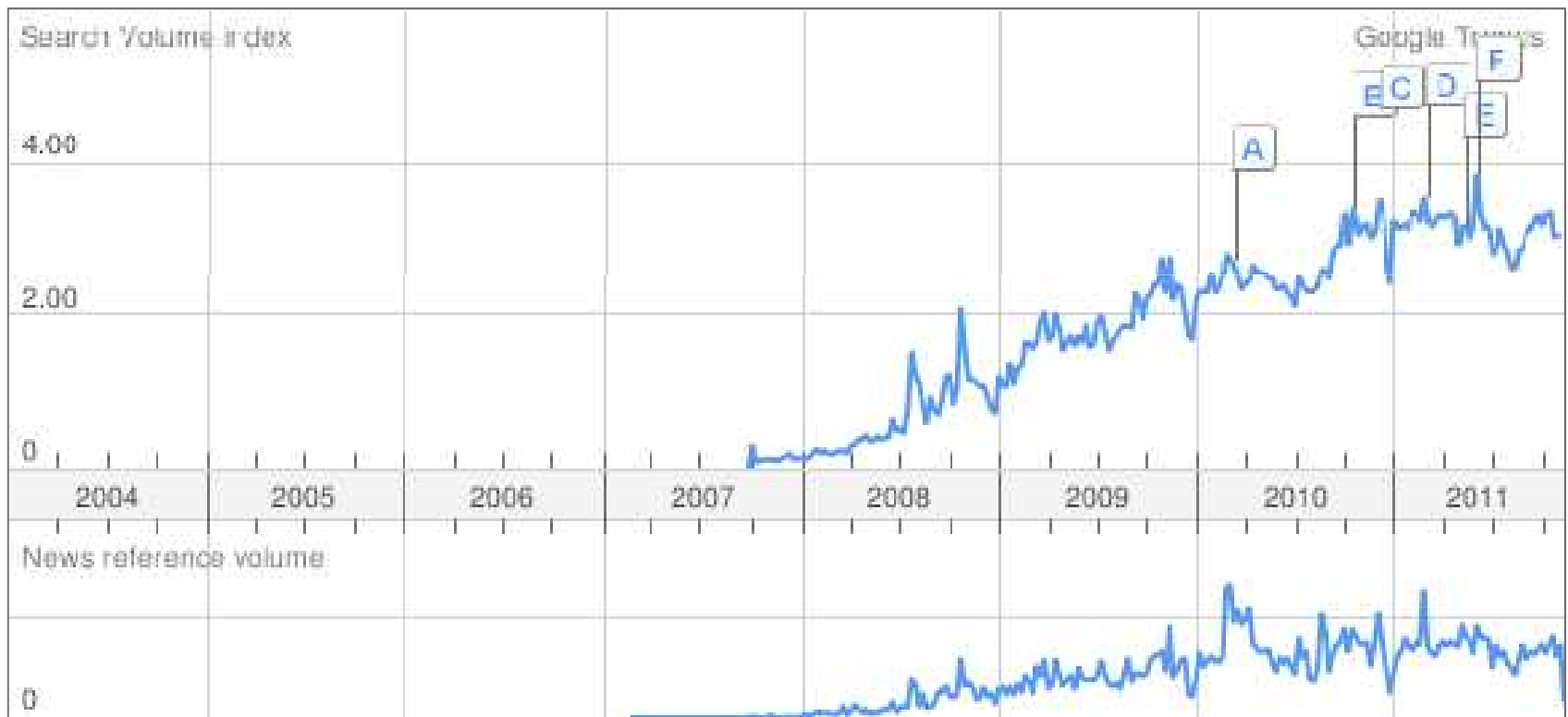
A vertical strip on the left side of the slide shows a close-up of a computer keyboard. The keys are light blue and white, with a yellow key visible. A solid dark blue vertical bar is positioned to the left of the keyboard image.

**Cloud Computing ist ein
modulares System, in dem
Ressourcen für den Anwender
transparent sowie dynamisch
zugewiesen und verarbeitet
werden.**

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

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

Cloud Computing ist voll im Trend (Google Trends)



Search Index "Cloud Computing"

Cloud Computing Architektur

SaaS

Software

PaaS

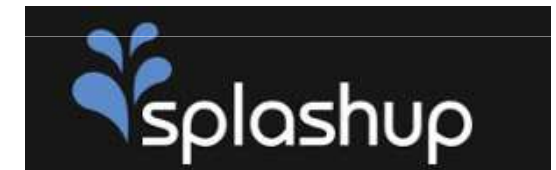
Platform

IaaS*

Infrastrucutre

auch S(storage)aaS*

Cloud Computing SaaS (Software as a Service)



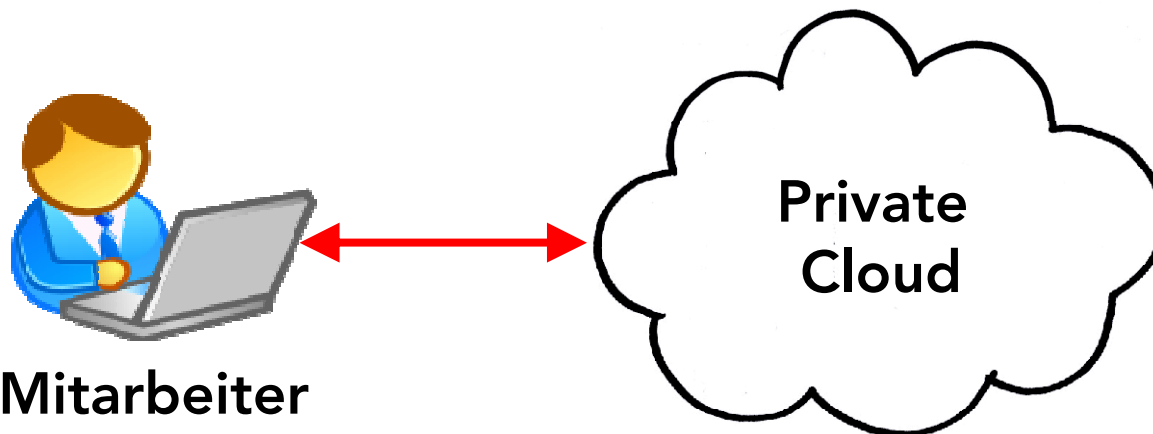
Cloud Computing PaaS (Platform as a Service)



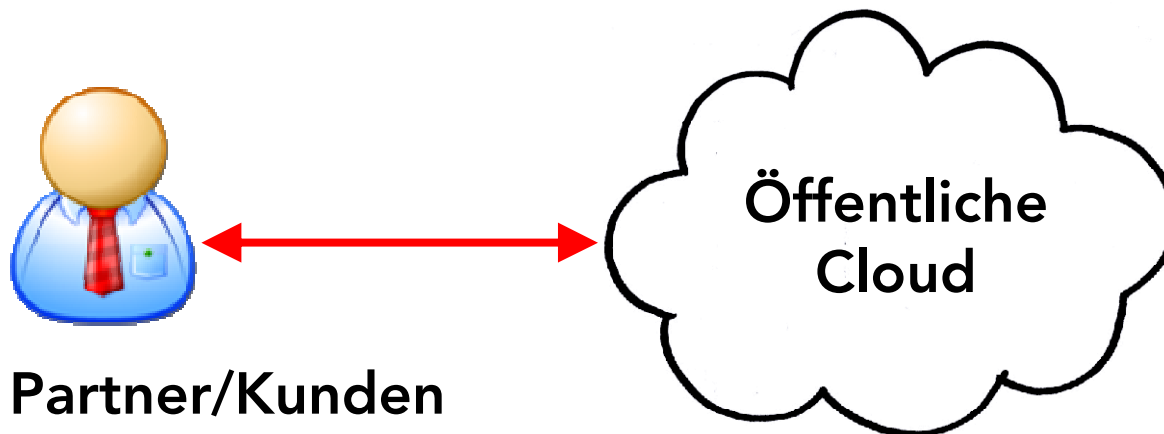
Cloud Computing SaaS (Infrastructure as a Service)



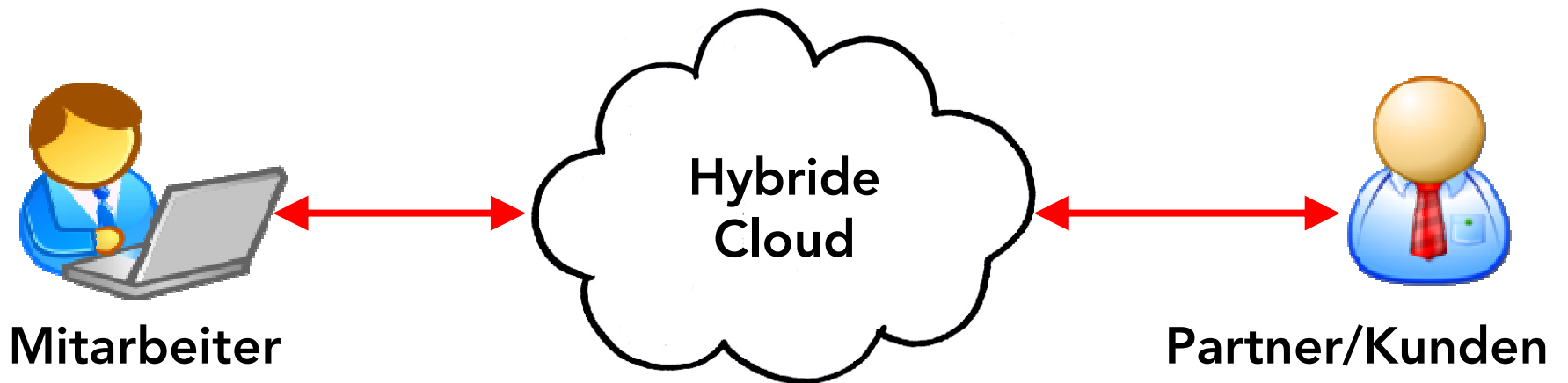
Cloud Computing Infrastrukturen



Cloud Computing Infrastrukturen



Cloud Computing Infrastrukturen





Cloud Services sind Schnee von gestern

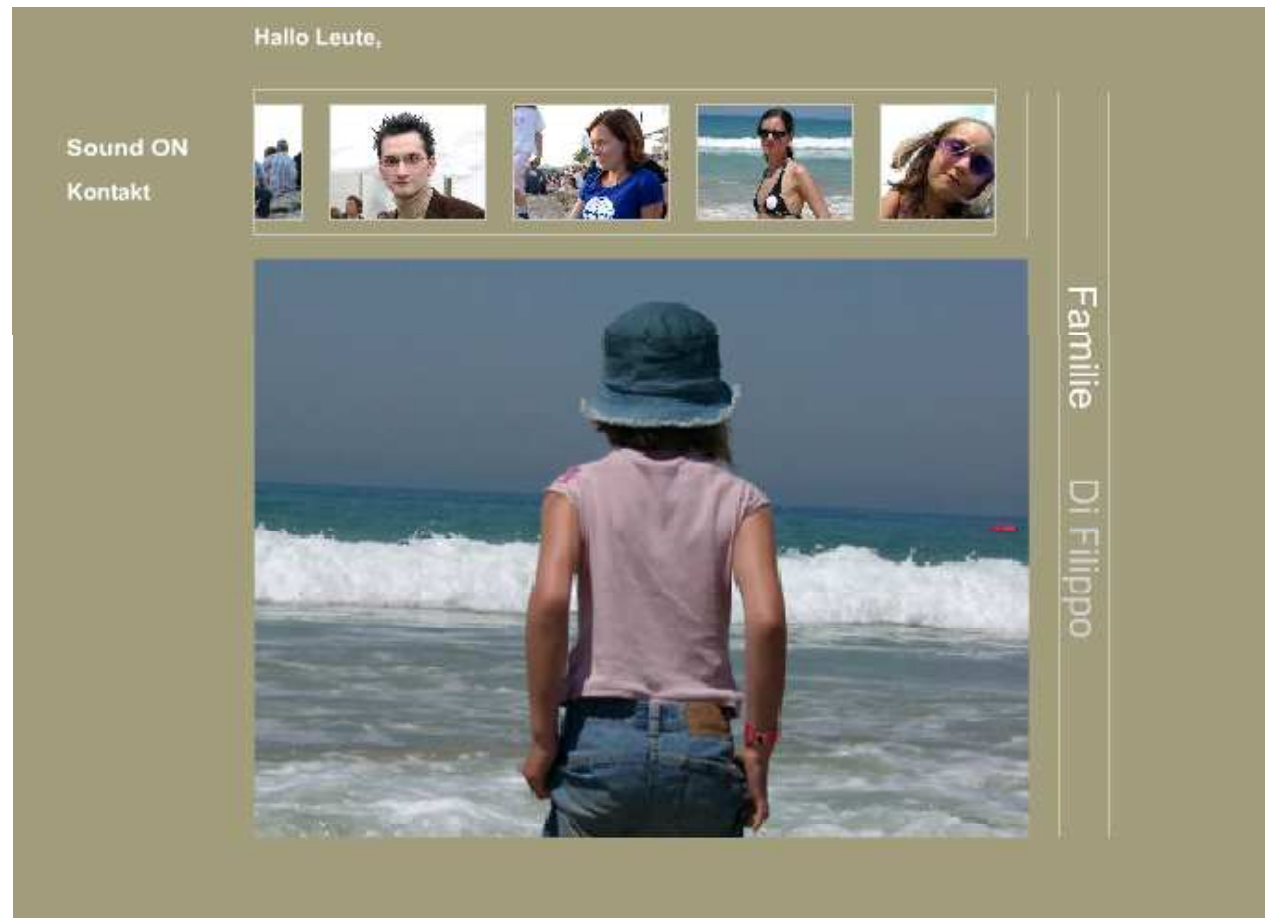
Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

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

(Alt)Bekannte Cloud Services



Cloud Computing Services



(Alt)Bekannte Cloud Services



Cloud Computing Services



A vertical image 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. A solid blue vertical bar is positioned to the left of the keyboard image.

Etablierte Techniken erfordern etablierte Angriffsmethoden....

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

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



LiveDemo [Capture the (Apple) iCloud]



Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

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

Capture the (Apple) iCloud



So sollte eine Cloud sein: automatisch und einfach.

- ✦ Usern stehen jederzeit ihre Files zur Verfügung
- ✦ User hat Zugriff auf seinen PIM (Kalender, eMail, Aufgaben etc.)
- ✦ User kann seine Geräte orten
- ✦ User kann Backup in Cloud speichern
- ✦ User weiss nicht was und wann synchronisiert wird

Capture the (Apple) iCloud



So sollte eine Cloud sein: automatisch und einfach.

- ✦ **Angreifern** stehen jederzeit **Ihre** Files zur Verfügung
- ✦ **Angreifer** haben Zugriff auf **Ihren** PIM (Kalender, eMail, Aufgaben etc.)
- ✦ **Angreifer** können **Ihre** Geräte orten
- ✦ **Angreifer** können Backup aus der Cloud holen
- ✦ **Angreifer** wissen was und wann synchronisiert wird

Capture the (Apple) iCloud



```
Firefox  
iCloud  
Hacking-La... http...g.pl  
http://deli.csnc.ch  
iCloud Password Phishing  
  
User= Password=  
User= Password=  
User= Password=  
User=ggdg Password=fdghh  
User=fvnbcx Password=gugus  
User=Ivan Password=buetler  
User=Axa Password=cool4you  
User=riccardo.trombini@inverted.ch  
Password=cucucorsin  
User= Password=  
User=Ggggg Password=fddddd  
User=Axa Password=megacoolo  
User=Cguuuyyy Password=htw  
User=Dddddddd Password=phhgggfgff  
User=Ffhjjjjh Password=ccvfff  
User=MyUserID Password=noway  
User=test Password=test  
User=test Password=spbv  
User=Test Password=test
```



Capture the (Apple) iCloud



Noch einfacher...





LiveDemo [All Your Data Are Belong To Us] Amazon Elastic Compute Cloud (EC2)



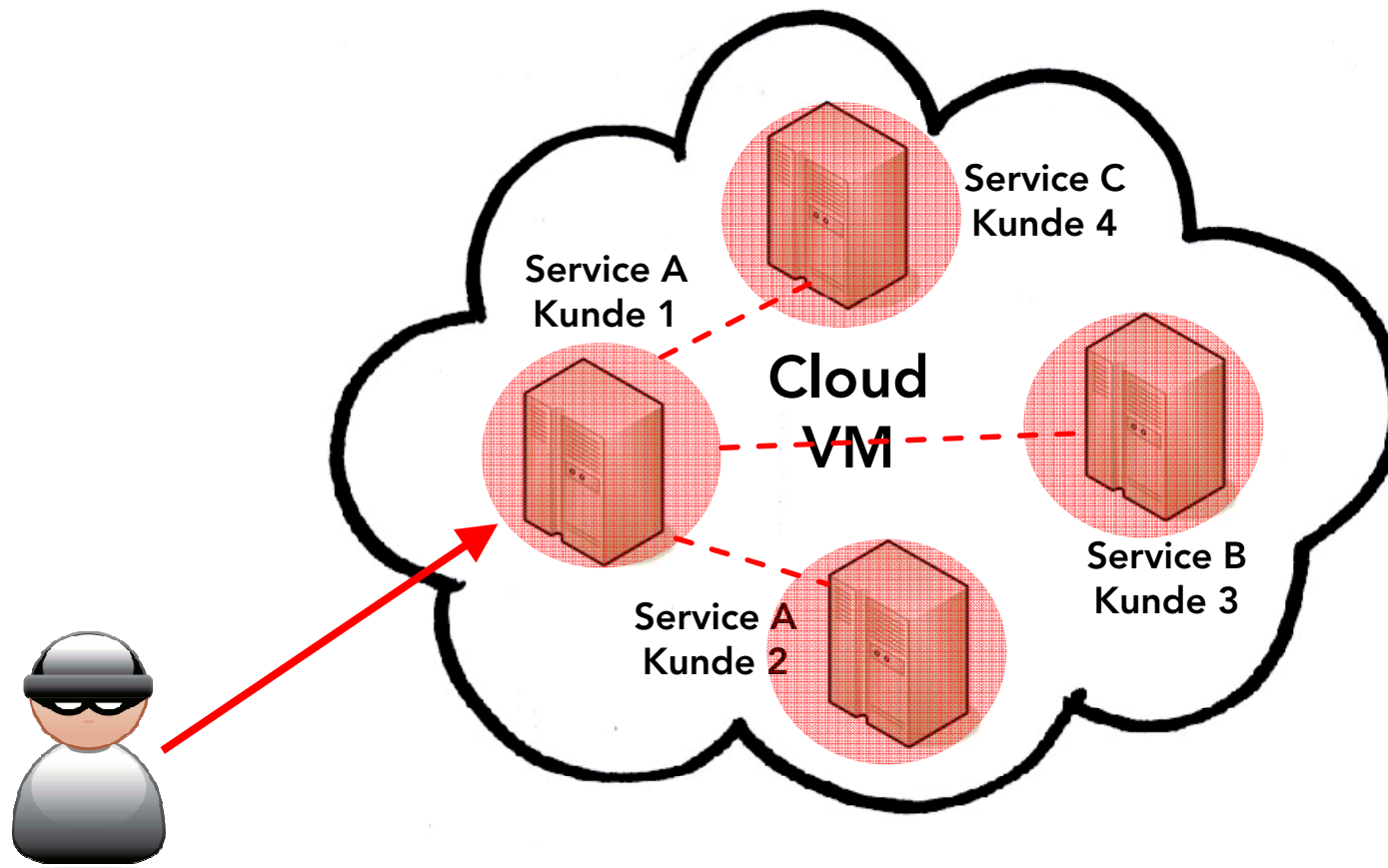
Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

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

All Your Data Are Belong To Us



Cloud Computing (All-In-One)





LiveDemo [All Storage]



Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

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

Brute Force Logik



- ◆ Username = Public Mail
- ◆ Passwort = Username
- ◆ Passwort = Realname (Kombinationen)
- ◆ Passwort = Username+0-9999
- ◆ Passwort = Wohnort (inkl. PLZ)
- ◆ Passwort = Produktnamen
- ◆ Passwort = Bekannte Persönlichkeiten

Top 7 Bedrohungen (CSA)



Folgende Gefahren hat die Cloud Security Alliance (CSA) ausgemacht:

1. Registrierung und Überwachung
2. Unsichere Schnittstellen und APIs
3. Böswillige Insider
4. Verteilte Infrastrukturen
5. Datenverluste und Datenlecks
6. Account- und Service- Hijacking
7. Unbekannte Risiken

1. Registrierung und Überwachung



- ✦ Malware Speicherung und Verteilung
- ✦ Illegale Inhalte
- ✦ Kontrollserver für Botnets
- ✦ Anonymität des Dienstes nutzen für Angriffe
- ✦ Schwache Benutzerauthentisierung

[Home](#) / [News & Blogs](#) / [Zero Day](#)

Zeus crimeware using Amazon's EC2 as command and control server

By Dancho Danchev | December 9, 2009, 8:13am PST

Summary

A recently intercepted variant of the most popular piece of crime, the Zeus bot is using

Action	URL	Details
GET	http://ec2-170.compute-1.amazonaws.com/zeus/config bin	svchost.exe
POST	http://ec2-170.compute-1.amazonaws.com/zeus/gate.php	svchost.exe
POST	http://ec2-170.compute-1.amazonaws.com/zeus/gate.php	svchost.exe
POST	http://ec2-170.compute-1.amazonaws.com/zeus/gate.php	svchost.exe
POST	http://ec2-170.compute-1.amazonaws.com/zeus/gate.php	svchost.exe

2. Unsichere Schnittstellen und APIs



- ✦ Anonymer Zugriff/Wiederverwendung von Zugriffstokens
 - ✦ Authentisierung/Kommunikation nicht verschlüsselt
 - ✦ Ungenügende Authorisation
 - ✦ Fehlendes Monitoring/Keine Log-Files
 - ✦ unknown service or API dependencies
- ✦ In Kürze: Alle Web-Applikations Schwachstellen möglich

Plesk : ProFTPD Remote Code Execution Vulnerability and Exploit

by [dino](#) on Nov.11, 2010, under [Plesk](#)

A flaw in the popular ProFTPD FTP server potentially allows unauthenticated attackers to compromise a server. The problem is caused by a buffer overflow in the `pr_netio_telnet_gets()` function for evaluating TELNET IAC sequences.

3. Böswillige Insider



- ✦ Wer betreibt die Cloud und wie wurden die Mitarbeiter ausgewählt
- ✦ Wer hat Zugang zur Cloud (z.B. ausländische Behörden)
- ✦ Wie sieht die physische Sicherheit beim Provider aus
- ✦ Wie wird Data Leakage Prevention auf eine Cloud ausgeweitet
- ✦ Wie Transparent ist der Cloud Anbieter

4. Verteilte Infrastrukturen



- ✦ Auf welchem Level ist die Mandanten-Trennung implementiert
- ✦ Wie wirkt sich ein Angriff auf einen Mandanten auf die anderen aus?
- ✦ Unterschiedliche Datentypen (öffentlich, intern, vertraulich)
- ✦ Unterschiedliche Branchen (Finanz, Behörden, Industrie, Kriminelle)

Microsoft Security Bulletin MS10-010 - Important

Vulnerability in Windows Server 2008 Hyper-V Could Allow Denial of Service (977894)

Published: February 09, 2010 | Updated: February 10, 2010

CLouDBURST

A VMware Guest to Host Escape Story

Kostya Kortchinsky
Immunity, Inc.

BlackHat USA 2009, Las Vegas

5. Datenverluste und Datenlecks



- ✦ Schwache Authentisierung, Authorisation und Audit Controls
- ✦ Ungenügende Verschlüsselung
- ✦ Operationelle Schwächen
- ✦ Verfügbarkeit des Daten-Centers
- ✦ Disaster Recovery
- ✦ Unklarheit wo Daten und Backups sind



TagesAnzeiger

DIGITAL

ZÜRICH SCHWEIZ AUSLAND WIRTSCHAFT BÖRSE SPORT KULTUR PANORAMA

Computer & Software Mobil **Internet** Wild Wide Web Multimedia Preisvergleich Bildstreifen

Gmail und das Problem mit der Datenwolke

Aktualisiert um 12:33 Uhr

Empfehlen 4

Einige Nutzer des Dienstes Gmail haben durch eine Panne vorübergehend ihre Mails verloren. Der Fall zeigt, wie das viel gepriesene Cloud Computing auch zum Problem werden kann.

6. Account- und Service- Hijacking



- ✦ Phishing Angriffe und Ausnutzen von Software Schwachstellen führen zu grösserem Schaden
- ✦ Oft werden dieselben Passworte für unterschiedliche Dienste benutzt
- ✦ Für den Zugriff auf Unternehmensdaten reicht dem Angreifer oft das Belauschen oder Herausfinden eines Passwortes
- ✦ Monitoring und Einbruchserkennung schwieriger
- ✦ Informationen fehlen um den Angriffsort/Angreifer zu ermitteln



7. Unbekannte Risiken



- ✦ Software Versionen, Updates, Einbruchsversuche, Security Design sind oft unbekannt.
- ✦ Unklar, wer sonst noch die Wolke nutzt
- ✦ Unbekannte Prozesse, Umsetzungen, Veränderungen
- ✦ Kann die Sicherheit geprüft werden, Security Reports vorhanden, werden Angriffe gemeldet?





Die Basis für Cloud Computing sind Vertrauen und Kompetenz.

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

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

Weitere Bedenken



- ✦ Wie werden die Daten in die Cloud respektive aus der Cloud gebracht
- ✦ Wie ist die Kompatibilität/Schnittstelle zu bestehenden Systemen/Applikationen
- ✦ Können Daten unwiderruflich gelöscht werden
- ✦ Wie steht es um die Aufbewahrungspflicht
- ✦ Wie Abhängig wird ihr Unternehmen vom Cloud Betreiber
- ✦ Kann der Anbieter gewechselt werden
- ✦ Wie kann den unterschiedlichen gesetzlichen Anforderungen Rechnung getragen werden
- ✦ Wissen ist nicht mehr im Unternehmen vorhanden
- ✦ Probleme können nicht mehr im eigenen Unternehmen gelöst werden

- ◆ Cloud Computing ist auf dem Vormarsch und wird uns alle betreffen.
- ◆ Cloud Computing erbt die Gefahren von Web-Applikationen, Virtualisierung und Outsourcing.
- ◆ Die Sicherheitsanforderungen können an die Cloud Anbieter gestellt werden, verantwortlich für die Sicherheit ist trotzdem die Firma.
- ◆ Bei vertraulichen Daten muss der Einsatz und Kostenaufwand von Cloud Computing sehr gut abgewägt werden.

Fragen?



Contact



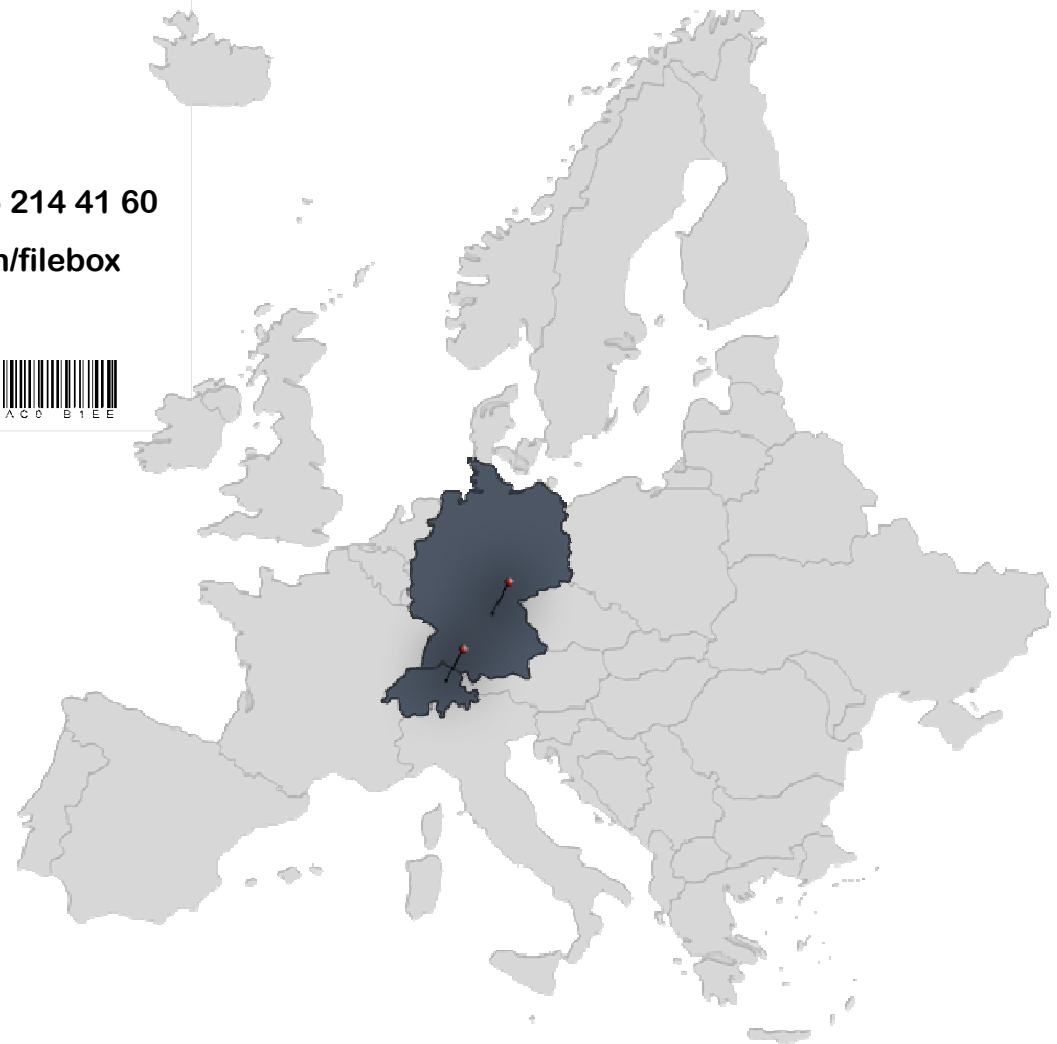
Compass Security Network Computing

Werkstrasse 20
Postfach 2038
CH - 8645 Jona

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

 Secure File Exchange: www.csnc.ch/filebox

PGP-Fingerprint:



Soziale Medien

- ✦ Sophos - Security Toolkit Social Media
<http://www.sophos.de/lp/threatbeaters/>

Cloud Computing

- ✦ BSI-Mindestsicherheitsanforderungen an Cloud-Computing-Anbieter
https://www.bsi.bund.de/cln_156/DE/Publikationen/publikationen_node.html
- ✦ CSA Top 7 Threats to Cloud Computing und Security Guidance
<http://cloudsecurityalliance.org/>
- ✦ ENISA Studie – Risikoanalyse
http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport