Best practice, iniziative e opportunità per la sicurezza del cloud

Matteo Cavallini

Giornate di Studio - 12 giugno 2012, ISACA

Chi sono

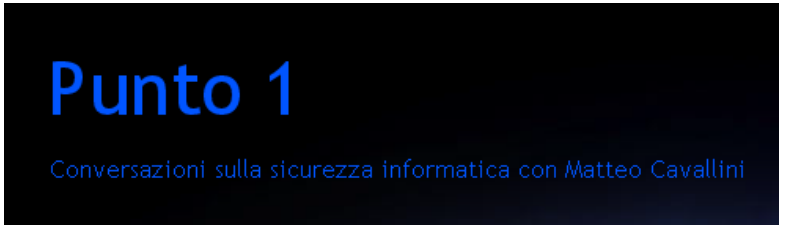
- Sono il Responsabile dell'Area Security di Consip
- Dal 2007 sono il Resp. della Unità Locale Sicurezza MEF/Consip
- Sono il Vice Presidente del capitolo italiano della Cloud Security Alliance

- Ho partecipato al progetto GovCERT.it
- Sono stato nominato esperto di sicurezza della Commissione di Collaudo del Sistema Pubblico di Connettività
- Sono stato Resp. della sicurezza perimetrale del MEF e di Consip

Cosa faccio

- Coordino i team di sicurezza di Consip
- Coordino le attività di Prevenzione e Gestione degli incidenti informatici per il Ministero dell'Economia e Consip
- Sono il riferimento gli aspetti di Cloud Security per Consip e il MEF
- Partecipo alle attività di ricerca di CSA-Italy

Nel (poco) tempo libero curo il blog di sicurezza



twitter account: @Nientenomi

Cloud: è tutto reale o è... solo marketing?

Il cloud computing è diventato una buzzword con cui il mercato si deve confrontare

Gli investimenti in gioco sono notevoli e il marketing è particolarmente attivo

Ma quali sono i reali vantaggi e le reali problematiche legate a questo cambio di paradigma nell'Information Technology?

Cominciamo dai vantaggi...

I vantaggi economici

- Capacità di diminuire i costi di start-up di un sistema
- Possibilità di dimensionare sistemi e applicazioni sulla base dei normale carico di lavoro gestendo i picchi di carico tramite la capacità di scalare tipica delle infrastrutture cloud
- Capacità di ottimizzare i costi sia in termini di risorse computazionali, sia in termini di risorse umane di gestione
- Possibilità di ridurre gli investimenti (CAPEX) a fronte di maggiori spese correnti (OPEX)

I vantaggi operativi

- Drastica riduzione dei tempi di realizzazione e di messa in esercizio di nuovi servizi
- Rapida capacità di scalare le risorse rapidamente per venire incontro a nuove esigenze o a requisiti modificati;
- Rapido ed efficiente provisoning e deprovisioning delle risorse;
- Decisa ottimizzazione dei consumi energetici sia per le esigenze computazionali sia per le esigenze di refrigerazione dei centri di elaborazione

I vantaggi per la sicurezza

Esistono potenziali vantaggi per la sicurezza dovuti a:

- specializzazione del personale e strutture dedicate che permettono soluzioni di sicurezza di maggior qualità rispetto a quelle consuete;
- migliori soluzioni per la business continuity e disaster recovery
- maggiore efficienza ed efficacia nei processi di change management, patch management, hardening, security assessment e security testing.

E dopo i vantaggi... ecco i problemi!

Problema 1: cos'è una cloud?

CARATTERISTICA	DEFINIZIONE
On demand self-service	L'utente ha la facoltà, unilaterale, di approvvigionarsi di risorse computazionali, come ad esempio tempo macchina e storage di rete, automaticamente, senza che ci sia la necessità di una interazione umana con i fornitori del servizio.
Broad network access	Le risorse sono accessibili via rete attraverso meccanismi standard che promuovono l'uso di piattaforme client eterogenee (ad esempio smartphone, laptop, PDA, ecc.)
Resource pooling	Le risorse computazionali del fornitore sono messe in comune per servire molteplici utenti, usando uno schema multi-cliente, che gestisce risorse fisiche e virtuali dinamicamente assegnate e riassegnate, in accordo con le indicazioni degli utenti. Gli utenti, in alcuni casi, possono avere la facoltà di indicare la locazione fisica delle risorse, ma solo a un elevato livello di astrazione (ad esempio Stato o data center). Per risorse si intendono: lo storage, le capacità elaborative, la memoria, le capacità di rete e le macchine virtuali.

Problema 1: cos'è una cloud?

Rapid elasticity	Le risorse sono in grado di essere allocate rapidamente ed elasticamente, in alcuni casi automaticamente, per soddisfare, in maniera veloce, le maggiori o minori richieste degli utenti. Gli utenti hanno l'impressione che le risorse disponibili siano illimitate e che possano essere acquistate in qualsiasi quantità e in qualsiasi momento.
Measured service	I sistemi cloud controllano automaticamente e ottimizzano l'utilizzo delle risorse tramite strumenti di misura basati su adeguati livelli di astrazione (ad esempio storage, capacità elaborativa, banda, e account utente attivi). L'utilizzo delle risorse può essere monitorato, controllato ed elaborato, in piena trasparenza sia per il provider sia per l'utente del servizio.

Problema 2: chi è l'owner di una cloud?

	Infrastructure Managed By[1]	Infrastructure Owned By[2]	Infrastructure Located[3]	Accessible and Consumed By[4]
Public	Third Party Provider	Third Party Provider	Off-Premise	Untrusted
Private/ Community	Or Organization / Third Party Provider	Organization / Third Party Provider	On-Premise / Off-Premise	Trusted
Hybrid	Both Organization & Third Party Provider	Both Organization & Third Party Provider	Both On-Premise & Off-Premise	Trusted & Untrusted

Problema 3: chi sono gli attori?

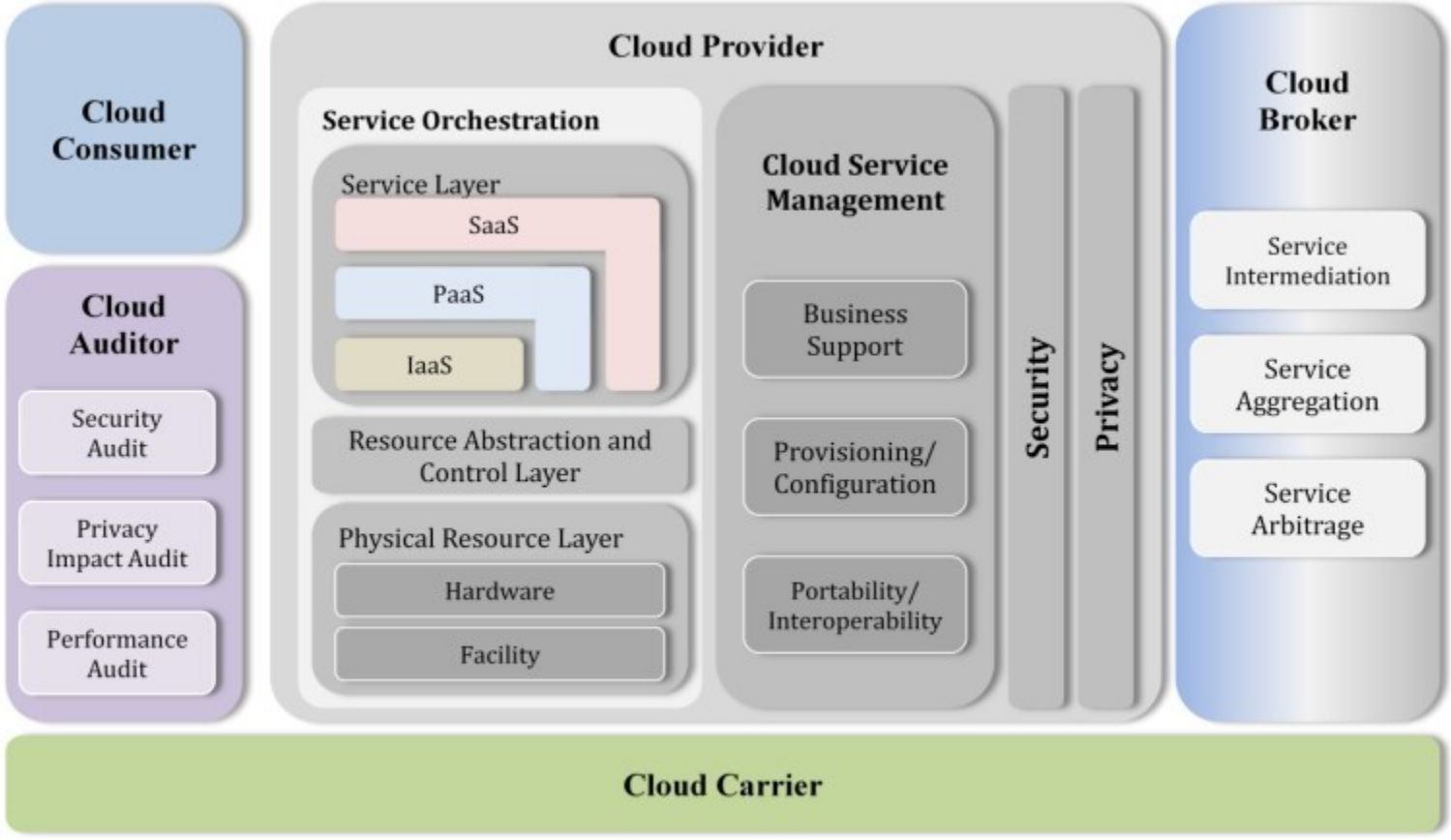
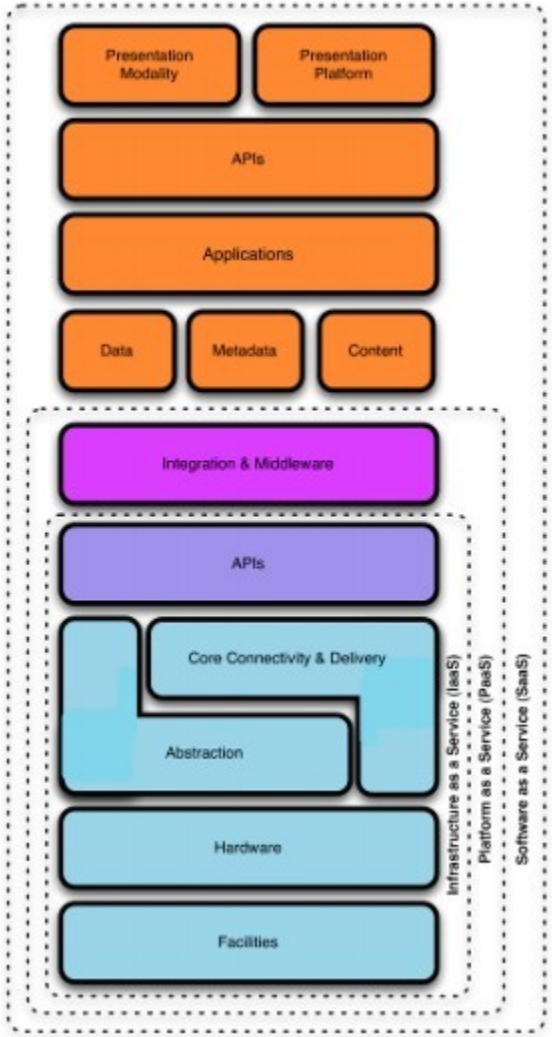


Figure 1: The Conceptual Reference Model

Problema 4: chi è il responsabile?



Problema 4: chi è il responsabile?

INFRASTRUCTURE AS A SERVICE

Customer
• Maintenance of identity man system • Management of identity man system • Management of authenticati (including enforcing passwor • Management of guest OS pat hardening procedures (check conflict between customer ha procedure and provider secu • Configuration of guest securit (firewall rules, IDS/IPS tuning • Guest systems monitoring • Security platform maintenance (firewall, Host IDS/IPS, antivirus, packet filtering) • Log collection and security monitoring

PLATFORM AS A SERVICE

Customer
• Maintenance of identity mar system • Management of identity mar system • Management of authenticati (including enforcing passwor

SOFTWARE AS A SERVICE

Customer	Provider
• Compliance with data protection law in respect of customer data collected and processed	• Physical support infrastructure (facilities, rack space, power, cooling, cabling, etc) • Physical infrastructure security and availability (servers, storage, network bandwidth, etc)
• Maintenance of identity management system • Management of identity management system • Management of authentication platform (including enforcing password policy)	• OS patch management and hardening procedures (check also any conflict between customer hardening procedure and provider security policy) • Security platform configuration (Firewall rules, IDS/IPS tuning, etc) • Systems monitoring • Security platform maintenance (Firewall, Host IDS/IPS, antivirus, packet filtering) • Log collection and security monitoring

I media e la cloud security

REUTERS EDITION: U.S.

Analysis: Sony woes rethink cloud comput

Bloomberg Anywhere | Professional | Solutions | About

Sony Network Breach Shows Amazon Cloud's Appeal for Hackers

By Joseph Galante, Olga Kharif and Pavel Alpeyev - May 16, 2011 10:45 PM GMT+0200

Epsilon breach: hack of the century?

27 comments

SISTEMI OPERATIVI

Vivere sulla nuvola? Non è male ma la chiave è la sicurezza

la Repubblica.it | Tecnologia

Da Amazon a Sony, cloud computing al collasso

03 maggio 2011 — pagina 1 sezione: AFFARI FINANZA

SECURITY WEEK

INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

Cloud Security Offense. Don Attacks. Avoid Them.

By Joh

la Repubblica.it | Tecnologia

IL CONVEGNO

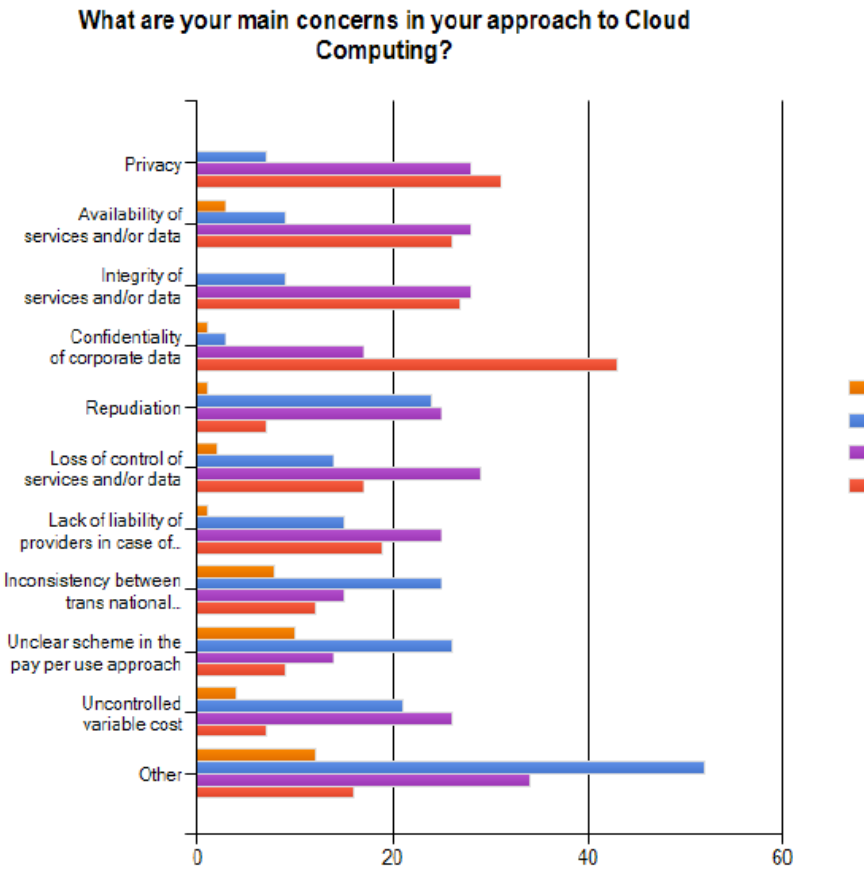
Regole per il Cloud computing "nuvola" sicura per l'utente

infosec ISLAND

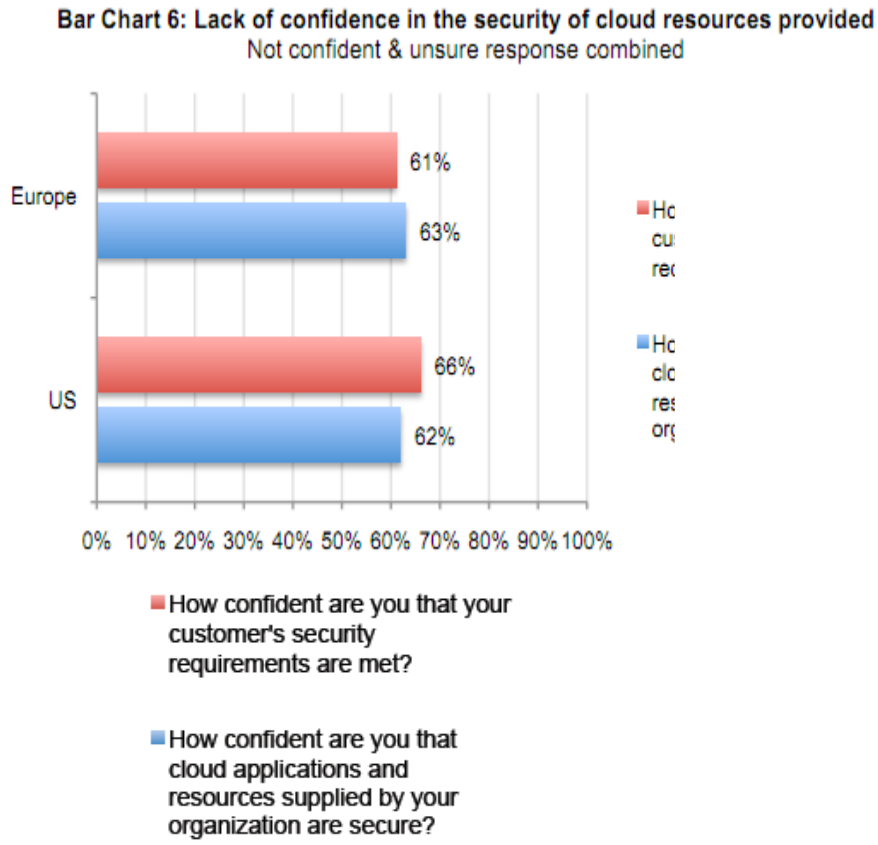
Epsilon Breach Deals Another Blow to Cloud Security

Friday, April 08, 2011

Le preoccupazioni



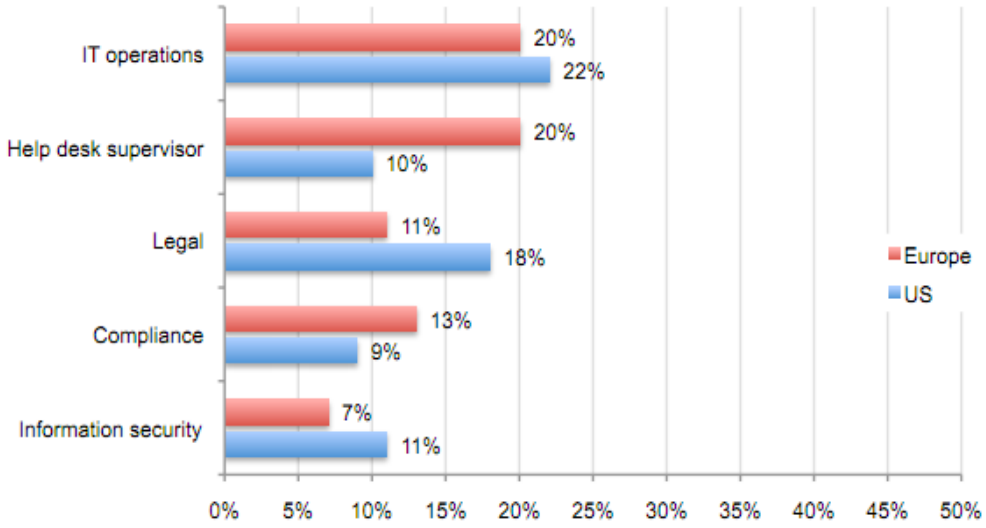
Fonte ENISA – Novembre 2009



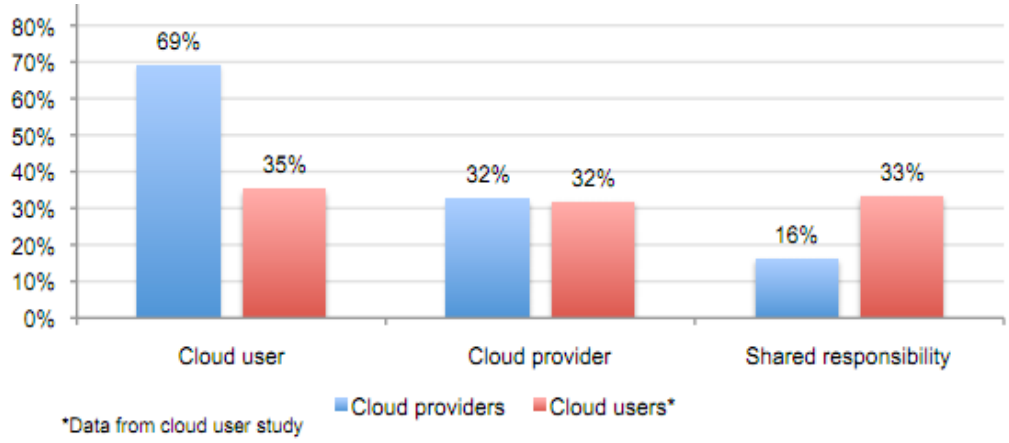
Fonte Ponemon Institute – Aprile 2011

Le responsabilità

Bar Chart 7: Who is most responsible for ensuring security of the providers' solutions

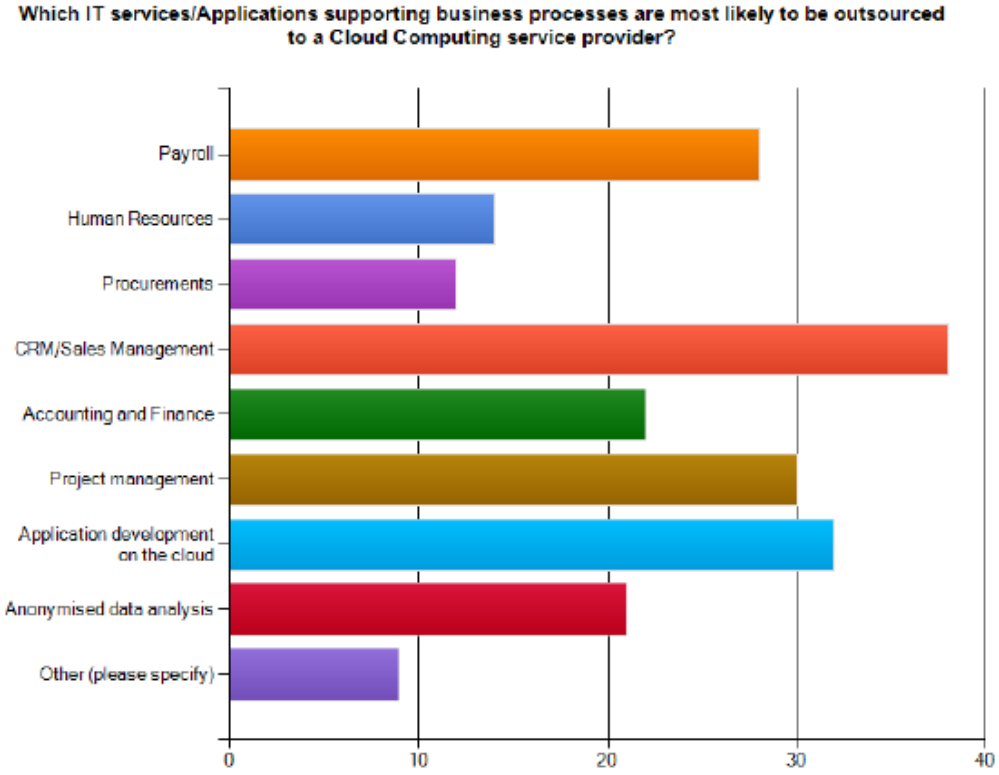


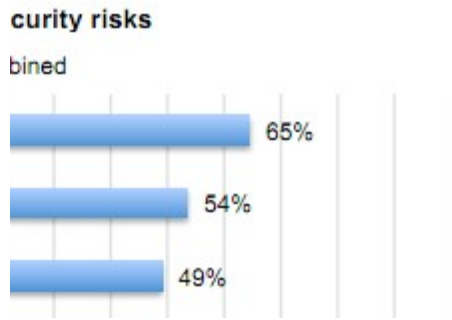
sible for ensuring the security of cloud resources by cloud providers?

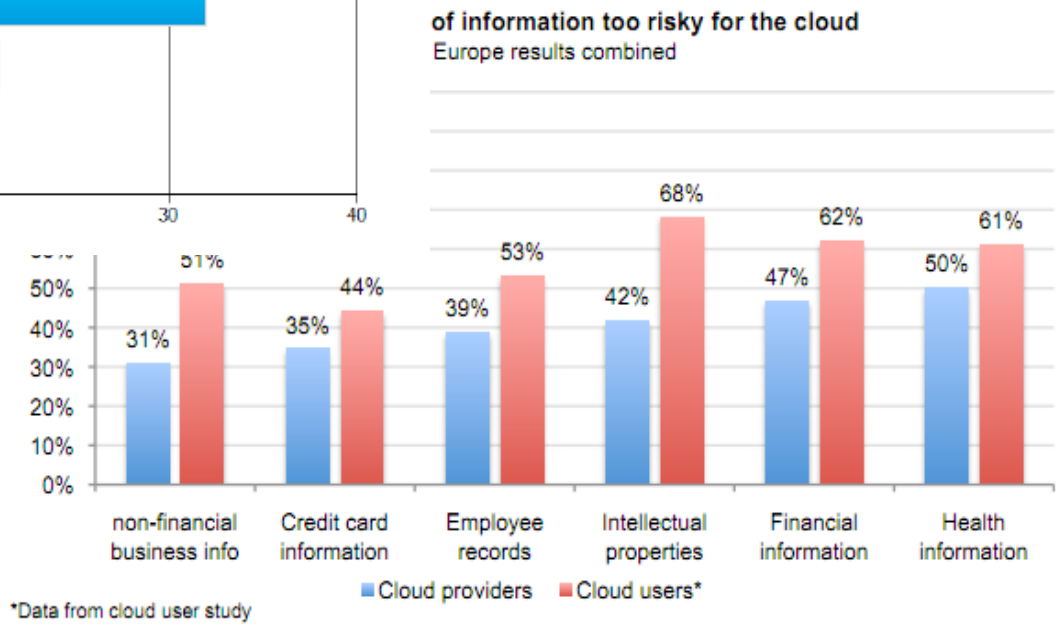


*Data from cloud user study

I rischi


Which IT services/Applications supporting business processes are most likely to be outsourced to a Cloud Computing service provider?
Payroll
Human Resources
Procurements
CRM/Sales Management
Accounting and Finance
Project management
Application development on the cloud
Anonymised data analysis
Other (please specify)
0
10
20
30
40


curity risks
bined
65%
54%
49%


of information too risky for the cloud
Europe results combined
50%
40%
30%
20%
10%
0%
31%
51%
35%
44%
39%
53%
42%
68%
47%
62%
50%
61%
non-financial business info
Credit card information
Employee records
Intellectual properties
Financial information
Health information
Cloud providers
Cloud users*
*Data from cloud user study

La sicurezza è il fattore abilitante

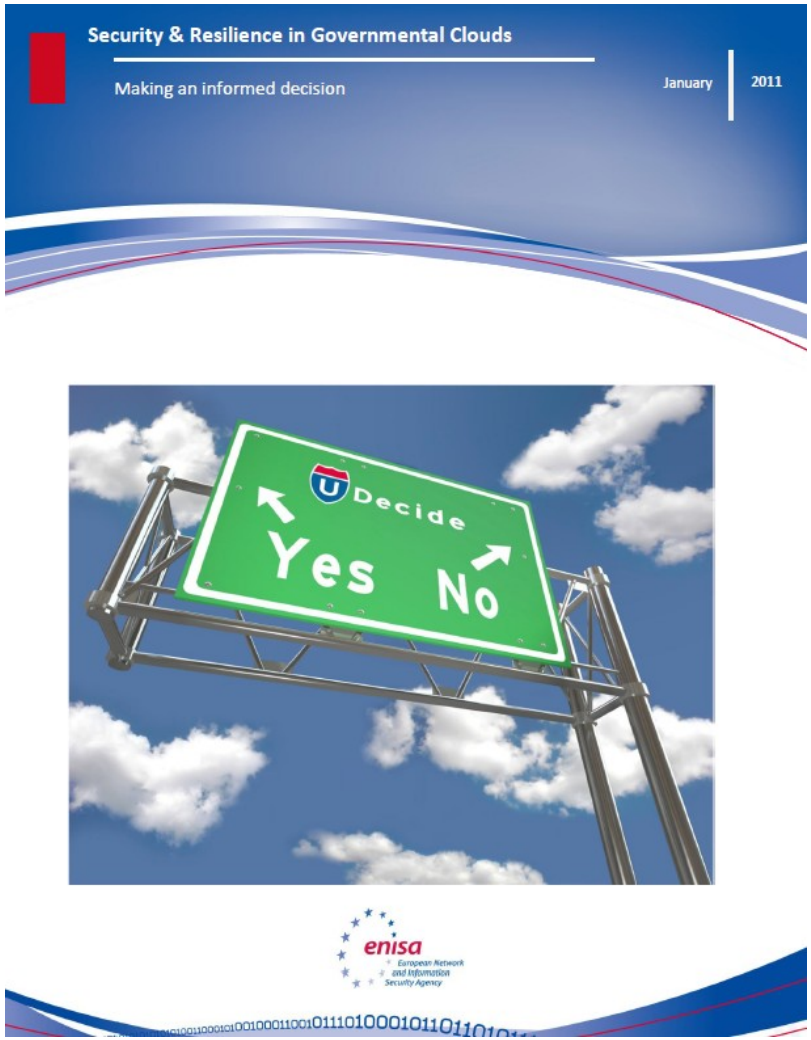
- Per non correre inutili rischi
- Per consentire di fruire dei grandi vantaggi del cloud
- Per evitare “spiacevoli” sorprese
- Per mantenere il necessario controllo su dati e applicazioni

I riferimenti

cloud security alliance SM

Security Guidance
for
Critical Areas of Focus
in
Cloud Computing V2.1

Prepared by the
Cloud Security Alliance
December 2009

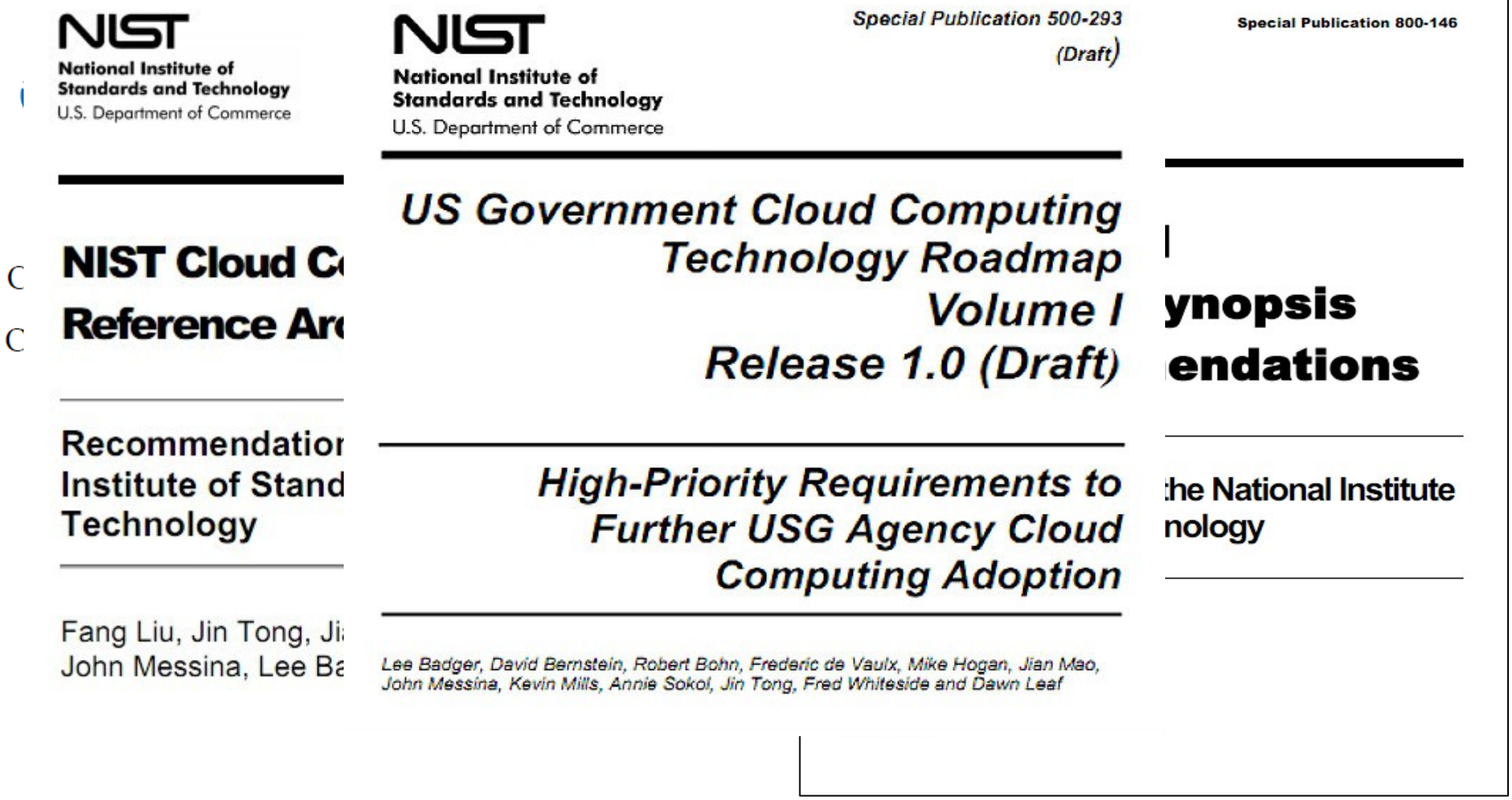


Proposed Security
Assessment & Authorization
for U.S. Government Cloud Computing

CIO COUNCIL

Draft version 0.96
November 2, 2010

I riferimenti



NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NIST Cloud C
Reference Ar

Recommendatio
Institute of Stand
Technology

Fang Liu, Jin Tong, Ji
John Messina, Lee Ba

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 500-293
(Draft)

US Government Cloud Computing
Technology Roadmap
Volume I
Release 1.0 (Draft)

High-Priority Requirements to
Further USG Agency Cloud
Computing Adoption

Lee Badger, David Bernstein, Robert Bohn, Frederic de Vaulx, Mike Hogan, Jian Mao,
John Messina, Kevin Mills, Annie Sokol, Jin Tong, Fred Whiteside and Dawn Leaf

Special Publication 800-146

ynopsis
endations

he National Institute
nology

I riferimenti

I riferimenti

enisa
European Network and Information Security Agency

Procure Secure

A guide to monitoring of security service levels in cloud contracts

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-146

Cloud Computing Synopsis and Recommendations

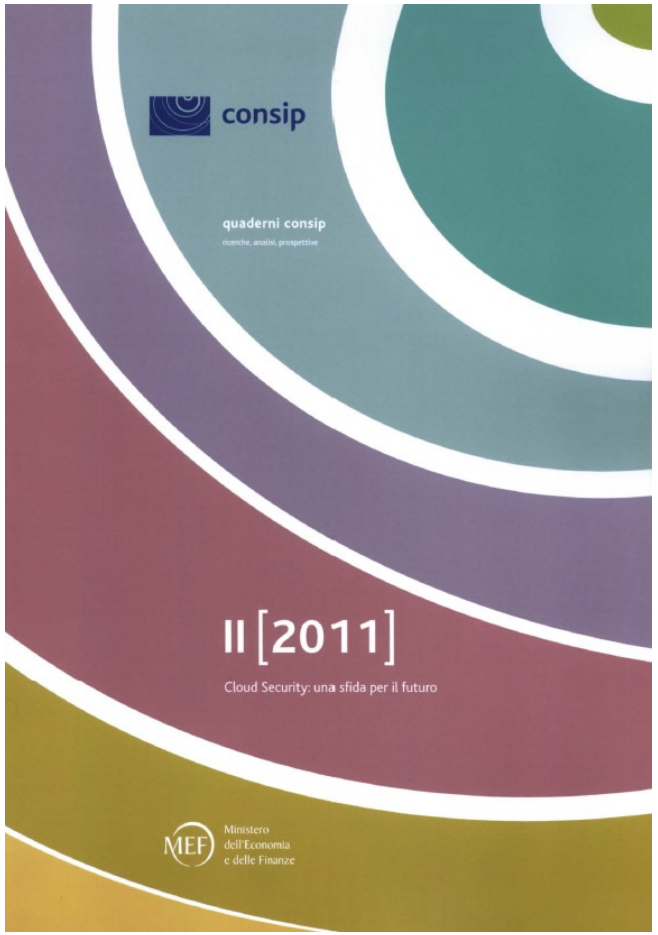
Recommendations of the National Institute of Standards and Technology

Lee Badger
Tim Grance
Robert Patt-Corner
Jeff Voas

E in Italia che succede?

Il Garante privacy, ha pubblicato:
"Indicazioni per l'utilizzo consapevole dei servizi"

Consip, ha pubblicato il Quaderno:
"Cloud Security: una sfida per il futuro"



E in Italia che succede?

Il Garante privacy, ha pubblicato:
"Cloud computing: Proteggere i dati per non cadere dalle nuvole"

DigitPA, ha pubblicato:
"Raccomandazioni e proposte sull'utilizzo del cloud nella PA"


DigitPA

RACCOMANDAZIONI E PROPOSTE SULL'UTILIZZO DEL CLOUD COMPUTING NELLA PUBBLICA AMMINISTRAZIONE

Versione 1.7 del 14 maggio 2012

E in Italia che succede?

E' nata Cloud Security Alliance-Italy Chapter
http://cloudsecurityalliance.it

Tema di ricerca:
"Portabilità, Interoperabilità e Sicurezza Applicativa"

CSA-Italy: chi siamo

- **Associazione** senza scopi di lucro (**no-profi**t)
- **62 soci** regolarmente iscritti
- **Soci Affiliati:** Clusit Associazione Italiana per la Sicurezza Informatica; ASSINTEL Associazione Nazionale Imprese ICT
- **Sponsor:** TREND MICRO; ca technologies; iTWAY do IT your way; Allied Telesis
- **Collaborazioni**: AIIC; OWASP Italian Chapter
- **> 320 membri** nel linkedin group CSA Italy

CSA-Italy: la ricerca 2012

Traduzioni delle Guide CSA

- *Coordinatore: Moreno Carbone*

Portabilità, Interoperabilità e Sicurezza Applicativa

- *Coordinatore: Matteo Cavallini*

Privacy & Cloud

- Coordinatore: Valerio Vertua

I 10 rischi top – Quaderno Consip

Rischio	Public	Commun. EXt	Commun. INt	Private
Contrattualistica non sempre adeguata	A	M	B	B
Impossibilità di negoziare termini contrattuali	A	M	M	B
Legge applicabile e foro competente	A	B	B	B
Mancato rispetto normativa sulla privacy	A	A	A	M
Riflessi di azioni giudiziarie su altri clienti	A	A	A	A
Perdita di governance	A	M	B	B
Lock-in	A	A	A	A
Indisponibilità di un servizio o di un provider	A	A	A	M
Compromissione delle caratteristiche di sicurezza dei dati	A	A	A	A
Compromissione della sicurezza di rete	A	A	A	A

Legenda: **A**=Molto rilevante; **M**=Mediamente rilevante; **B**=Poco rilevante;
Community-INT= Community Cloud posseduta, ubicata e gestita internamente
Community-EXT= Community Cloud posseduta, ubicata e gestita da terzi

Rischio 1 – Contrattualistica non adeguata

I CSP, spesso, sono grandi multinazionali americane e i contratti possono riflettere il loro approccio legale e la normativa americana

La flessibilità nell'erogazione del servizio e la semplicità nella stipulazione del servizio a volte portano a contratti troppo “semplici”.

Il problema della descrizione esatta del servizio erogato è piuttosto rilevante e, a volte, gli SLA possono essere poco “significativi” per il CSC

Rischio 2 – Difficile negoziazione dei termini

I CSP, spesso, sono grandi multinazionali americane e i contratti sono, di norma, predisposti per rappresentare i loro interessi.

I potenziali CSC, in Italia, sono per la stragrande maggioranza PMI e PA locali e centrali che hanno difficoltà di confronto con i grandi CSP.

La grande forza del cloud è data dalle economie di scala e i contratti, per forza di cose, devono riflettere degli approcci standard, poco negoziabili.

Rischio 3 – Legge applicabile e Foro competente

La libertà di scelta del foro competente deve essere attentamente valutata in quanto deve rappresentare correttamente gli interessi di entrambe le parti.

Alcune scelte “esotiche” del foro competente potrebbero essere molto vantaggiose per i CSP ma potrebbero essere estremamente onerose per i CSC.

Rischio 4 – Mancato rispetto privacy

La normativa in materia di protezione dei dati personali non è nata pensando ad uno scenario di tipo “cloud”

Le classifiche figure prevista dalla normativa (Titolare, responsabile e incaricato) mal si adattano alle cloud

Alcune previsioni normative nazionali (ad es. Amministratori di sistema) sono difficilmente realizzabili nelle cloud

Il problema dei problemi... la distribuzione geografica dei data center

Rischio 4 – Mancato rispetto privacy

Il Garante Privacy Italiano ha una grande attenzione al tema del cloud, infatti partecipa a molti gruppi di lavoro e ha messo nel proprio piano ispettivo i fornitori di servizi informatici con particolare riferimento ai servizi cloud.

La Commissione Europea ha avviato la revisione della normativa sulla protezione dei dati personali.

Rischio 5 – Riflessi di azioni giudiziarie

Rischio 6 – Perdita di governance

Uno dei rischi più tipici (e difficili da affrontare) dei servizi cloud.

Quando il CSP, non solo ha in mano dati e codice applicativo, ma decide in merito alle misure di sicurezza e alle modalità di gestione, si può ancora pensare di essere i “data owner”?

Anche gli audit, che sono la misura normalmente utilizzata per mantenere una certa quota di governance sulla fornitura, sono di difficile realizzazione in ambito cloud.

Rischio 7 - “Lock-in”

Ogni “Cloud Service Consumer” dovrebbe essere in grado di:

- cambiare il proprio Cloud Service Provider (CSP)
- riportare al proprio interno il servizio se gestito da un CSP esterno
- affidare a un CSP esterno un servizio gestito internamente nella propria cloud privata

Rischio 7 - “Lock-in”

Chiare clausole contrattuali che specifichino tutte le condizioni e le modalità operative di uscita dal servizio, con particolare riferimento a:

- le modalità con le quali vengono forniti i dati e, se del caso, il codice applicativo;
- le modalità di erogazione del supporto alla migrazione;
- i tempi, gli effort previsti e gli eventuali step transitori.

Sono necessari standard e best practice internazionalmente riconosciuti che rendano realmente fattibile ed efficiente la migrazione di dati e applicazioni tra diverse cloud.

Rischio 8 - Indisponibilità

Questo rischio è da considerare particolarmente insidioso per almeno tre buone ragioni:

- Le cloud, per le loro caratteristiche, creano un "falso" senso di resilienza intrinseca che può trarre in inganno

- Senza opportune contromisure i rischi che si corrono possono essere molto elevati
- Le problematiche legate alle subforniture complicano il quadro in maniera esponenziale perché inseriscono elementi che non possono essere adeguatamente controllati

Rischio 9 – Compromissione sicurezza dei dati

La “madre” di tutti i rischi... come abbiamo ricordato le più grandi preoccupazioni sono tutte su questo rischio.

Giusto alcune pillole:

- Reale isolamento tra le risorse virtualizzate
- Compromissione delle interfacce di management
- Reale cancellazione dei dati
- Gestione delle identità

Ricordare che, nel mondo cloud, anche gli aspetti di sicurezza sono regolati da clausole, SLA e penali che quindi devono essere attentamente valutati da chi si occupa di sicurezza.

Rischio 10 – Compromissione sicurezza rete

La rete è il modo con cui si accede ai dati e alle applicazioni nel mondo cloud, è evidente che i rischi correlati alla sicurezza e alla qualità delle network devono essere attentamente valutati.

Le principali contromisure che devono essere valutate sono:

- La cifratura
- L'autenticazione forte
- Politiche a garanzia della qualità dei servizi di rete
- Ridondanza dei collegamenti

Le raccomandazioni

La definizione di una strategia di approccio al cloud

Le raccomandazioni

La definizione dei requisiti

Il Piano della sicurezza

Le raccomandazioni

La valutazione degli SLA

La continuità dei servizi

La gestione degli incidenti

Agenda Digitale Italiana

Gruppo di Lavoro
Infrastrutture e sicurezza

Obiettivi

5 - Gestione in modalità cloud computing dei contenuti e servizi della PA, mediante la realizzazione dei data center federati, mediante l'attuazione del Progetto Strategico Data - Center. essere attentamente valutati.

Altri 4 obiettivi riguardano la banda larga e ultralarga. Un ulteriore obiettivo riguarda la realizzazione di un CERT nazionale. A fine maggio il MISE è stato individuato come la PA presso la quale deve essere realizzato il CERT nazionale.

Intanto, i media sottolineano le opportunità

la Repub

IL CASO

Hp ab
e pun

C
m

REUTERS

The future of computing is in the cloud

How the cloud changed venture capitalism

By Mark Suster | JULY 18, 2011

TERWORLD

o reshape IT in

l costs of cloud

g, security and

Modernità&Territorio

La Tachipirina ha scelto di andare sulla «nuvola»

CORRIERE DELLA SERA.it

INSIGHT

NSIGHT | RSS FEEDS | NEWSLETTERS

Research Slideshow:
Gartner's CIO Agenda: Cloud Computing Tops the List

Tutto questo marketing è servito.
Adesso sono proprio tutti convinti...

Anche i “bad guys”!

Nel cloud, gli incidenti di sicurezza legati al cybercrime possono essere riconducibili a:

- Data breach
- Uso di strumenti per commettere altri crimini

Ecco qualche esempio...

Gennaio 2012, un importante data breach

Zero Day

Ryan Naraine, Emil Protalinski and Dancho Danchev

Mobile
RSS
Email Alerts

Comments 1 | Tweet 192 | Like 116 | Submit | +1 1 | more +

Home / News & Blogs / Zero Day

Zappos hacked, 24 million affected

By Ryan Naraine | January 16, 2012, 8:31am PST

Summary: *The attackers may have swiped names, e-mail addresses, billing and shipping addresses, phone numbers, the last four digits of credit card numbers and/or cryptographically scrambled passwords.*

Online shoe shop Zappos has suffered a massive data breach that exposed user accounts for about 24 million users.

According to an e-mail from Zappos chief executive Tony Hsieh, attackers gained access to parts of the company's internal network and systems through a server in Kentucky.

La comunicazione ai 24 milioni di utenti

Subject: Information on the Zappos.com site - please create a new password

First, the bad news:

We are writing to let you know that there may have been illegal and unauthorized access to some of your customer account information on Zappos.com, including one or more of the following: your name, e-mail address, billing and shipping addresses, phone number, the last four digits of your credit card number (the standard information you find on receipts), and/or your cryptographically scrambled password (but not your actual password).

THE BETTER NEWS:

The database that stores your critical credit card and other payment data was NOT affected or accessed.

SECURITY PRECAUTIONS:

For your protection and to prevent unauthorized access, we have expired and reset your password so you can create a new password. Please follow the instructions below to create a new password.

We also recommend that you change your password on any other web site where you use the same or a similar password. As always, please remember that Zappos.com will never ask you for personal or account information in an e-mail. Please exercise caution if you receive any emails or phone calls that ask for personal information or direct you to a web site where you are asked to provide personal information.

PLEASE CREATE A NEW PASSWORD:

We have expired and reset your password so you can create a new password.

Please create a new password by visiting Zappos.com and clicking on the "Create a New Password" link in the upper right corner of the web site and follow the steps from there.

We sincerely apologize for any inconvenience this may cause. If you have any additional questions about this process, please email us at passwordchange@zappos.com

La comunicazione ai dipendenti

We have also created a web page that we will continue to update as we learn more about what questions customers have:

http://www.zappos.com/passwordchange

In order to service as many customer inquiries as possible, we will be asking all employees at our headquarters, regardless of department, to help with assisting customers. Due to the volume of inquiries we are expecting, we realized that we could serve the most customers by answering their questions by email. We have made the hard decision to temporarily turn off our phones and direct customers to contact us by email because our phone systems simply aren't capable of handling so much volume. (If 5% of our customers call, that would be over 1 million phone calls, most of which would not even make it into our phone system in the first place.)

We've spent over 12 years building our reputation, brand, and trust with our customers. It's painful to see us take so many steps back due to a single incident. I suppose the one saving grace is that the database that stores our customers' critical credit card and other payment data was not affected or accessed.

Over the next day or so, we will be training everyone on the specifics of how to best help our customers through their password change process now that their passwords have been reset and expired. We need all hands on deck to help get through this.

Thanks everyone.

-Tony Hsieh
CEO - Zappos.com

Ed ecco i tools...

WPA CRACKER

about run faq

An Introduction

WPA Cracker is a cloud cracking service for penetration testers and network auditors who need to check the security of WPA-PSK protected wireless networks.

WPA-PSK networks are vulnerable to dictionary attacks, but running a respectable-sized dictionary over a WPA network handshake can take days or weeks. WPA Cracker gives you access to a 400CPU cluster that will run your network capture against a 135 million word dictionary created specifically for WPA passwords. While this job would take over 5 days on a contemporary dual-core PC, on our cluster it takes an average of 20 minutes, for only $17.

NEW :: We now offer Germany dictionary support, a 284 million word extended English dictionary option, and ZIP file cracking.

Simply upload your network capture, start your job, and WPA Cracker will email you the results within minutes! *Run It* →

CloudCracker

CloudCracker provides dictionaries for each cracking format we support, and each dictionary is available in a range of sizes. Below is more information on the available dictionaries, their sizes, and their prices. Payments made by Bitcoin are given a discount of 15% off the listed prices.

WPA / WPA2 Dictionaries

These dictionaries are available for WPA / WPA2 cracking jobs. As a salted format with an 8 character minimum password length and a PBKDF2 iteration count of 4096, we know it is critical for our dictionaries to be as accurate as possible. We iterate on them by modeling the data we

Phone Numbers

Data has shown that 10 digit phone numbers are extremely common choices for WPA passphrases in North America. This dictionary covers every phone number in the US, Canada, Bermuda, and 17 Caribbean nations. It is available in one size:

1,559,000,000

LM / NTLM Dictionaries

These dictionaries are available for LanMan and NT LanMan cracking jobs. As an unsalted, computationally inexpensive password format, we combine both brute forcing as well as dictionary-derived words for maximum coverage.

Default

There is currently only a single LM / NTLM dictionary, available as a single size:

8,000,000,000,000

LM This dictionary provides full coverage for every permutation of alphanumeric and symbol characters, up to the maximum password length.

NTLM This dictionary does bruteforce of alphanumerics and symbols up to 9 characters, plus an extensive corpus of dictionary-derived words.

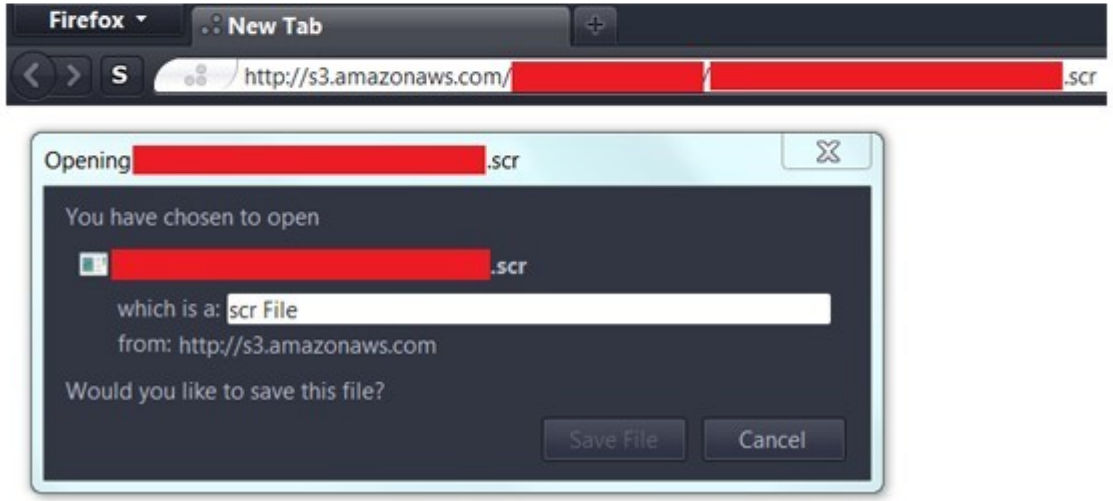
Get Started!

Ed ecco i tools...

Financial data stealing Malware now on Amazon Web Services Cloud

Dmitry Bestuzhev
Kaspersky Lab Expert
Posted June 05, 06:05 GMT
Tags: Instant Messengers, Internet Banking, Identity Theft, Malware Technologies, Rootkits, Amazon

There were some recent comments about Amazon Cloud as a platform for successful attacks on Sony... Well, today I found that Amazon Web services (Cloud) now is being used to spread financial c stealers.



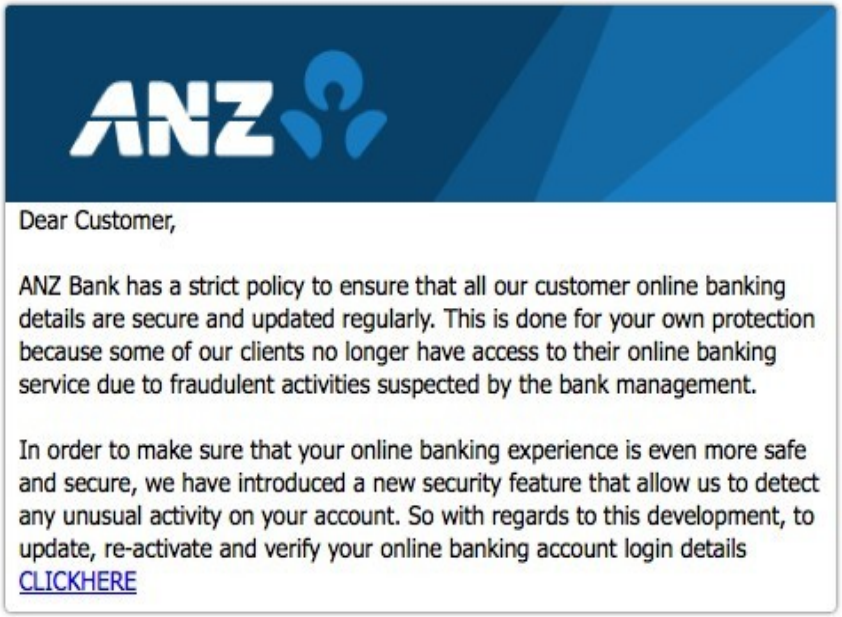
Ed ecco i tools...

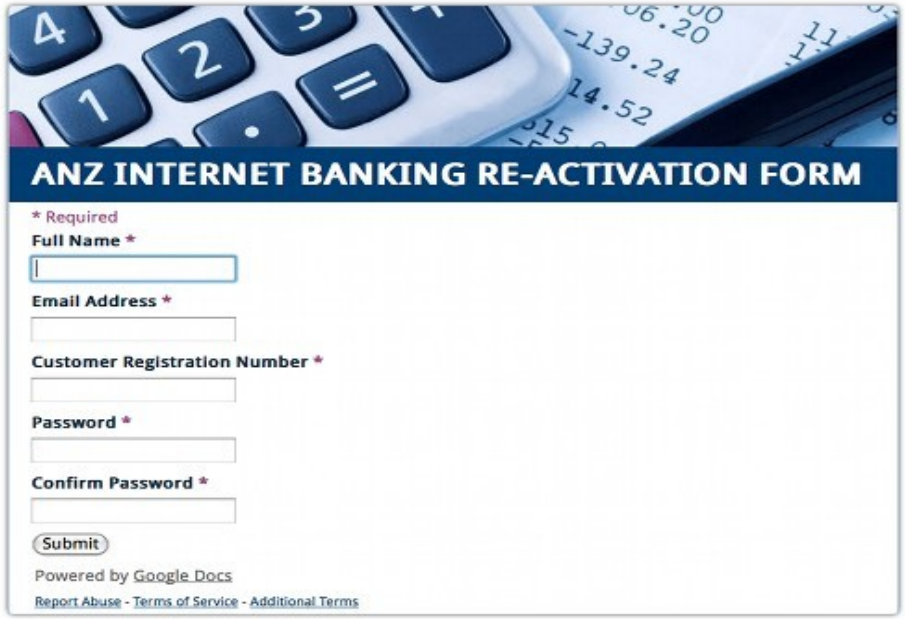
nakedsecurity
IT Security Blog of the Year
News. Opinion. Advice. Research

malware | spam | social networks | data loss | law & order | apple | podcast | video

◀ Will Twitter donate $1 for every retw... Zappos turns off phones after up to ... ▶

Google Docs - a full-featured, full-service phishing facility?





Using Google Docs for phishing 'surveys' benefits the crooks in several ways.

* The web hosting for the phishing forms and the fraudulently-collected data is provided, free of charge, by Google.

* The Google Docs user interface provides a simply and snazzy front end for designing the form.

* Google Docs can automatically generate emails to prospective victims inviting them to click through to the phishing form.

* The results are automatically and conveniently collected into a password-protected spreadsheet, which can be retrieved from anywhere.

* The URL uses HTTPS, which gives it an aura of security.

* The URL takes you to a google.com domain, which gives it an aura of legitimacy.

Interessante... ma perchè parlarne??

DIRETTIVA 2000/31/CE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

dell'8 giugno 2000

relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («Direttiva sul commercio elettronico»)

Articolo 14

«Hosting»

1. Gli Stati membri provvedono affinché, nella prestazione di un servizio della società dell'informazione consistente nella memorizzazione di informazioni fornite da un destinatario del servizio, il prestatore non sia responsabile delle informazioni memorizzate a richiesta di un destinatario del servizio, a condizione che detto prestatore:

a) non sia effettivamente al corrente del fatto che l'attività o l'informazione è illecita e, per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendono manifesta l'illegalità dell'attività o dell'informazione, o

b) non appena al corrente di tali fatti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso.

2. Il paragrafo 1 non si applica se il destinatario del servizio agisce sotto l'autorità o il controllo del prestatore.

3. Il presente articolo lascia impregiudicata la possibilità, per un organo giurisdizionale o un'autorità amministrativa, in conformità agli ordinamenti giuridici degli Stati membri, di esigere che il prestatore ponga fine ad una violazione o la impedisca nonché la possibilità, per gli Stati membri, di definire procedure per la rimozione delle informazioni o la disabilitazione dell'accesso alle medesime.

Quindi, in caso di incidente, quali sono i reali problemi?

I Problemi da affrontare

Quali dati di log sono a disposizione?

Esiste un team dedicato alla risposta agli incidenti?

Quanti sono i danneggiati?

Quali sono gli impatti legali?

Quali strumenti contrattuali sono a disposizione?

Quali strumenti tecnologici sono a disposizione?

Una prima risposta...

Current Status

- CloudSIRT incorporated
- Charter document completed
- Membership criteria document completed
- Lexicon for information sharing document completed
- Traffic Light Protocol completed
- Interim Membership Committee formed
- Multi-Party NDA completed

SIRT
tions

Procure Secure di ENISA...

Concludendo...

PARLA ERIC SCHMIDT

L'ottimismo di Mister Google "La *nuvola* ci renderà felici"

Il neo presidente del gigante web che ha guidato per 10 anni: "In due o tre anni sarà impossibile dimenticare, perdersi, annoiarsi, restare. Una rivoluzione per l'intero pianeta e non solo per una piccola élite. Grazie a smartphone, tablet e, soprattutto, al "cloud computing. Un futuro straordinario e spaventoso"

di JAIME D'ALESSANDRO

OCCHI chiari, completo blu, camicia immacolata. Il futuro è un signore di 56 anni, l'aspetto ordinario dell'uomo comune, che parla con tono neutro del nuovo umanesimo dei cellulari e dei super computer. "Un'era straordinaria e spaventosa", come lui stesso la definisce, "destinata a cambiare la nostra vita". Nella piccola stanza fatta di tramezzi dall'aria troppo vissuta, all'interno della Fira de Barcelona, Eric Schmidt [1] assume l'aria di un profeta. E' stato l'amministratore delegato di Google per dieci anni. Posto che ora ha lasciato a Larry Page, il cofondatore della multinazionale di Mountain View, tornato a dirigerla da poche settimane. Ma Schmidt era e resta, almeno per adesso, il volto pubblico della compagnia con la carica di presidente (Executive Chairman). E così, davanti a un gruppo ristretto di giornalisti, racconta di un avvenire luminoso che non ha precedenti, velato appena da qualche ombra. Lo fa con la sicurezza di chi ha scritto la storia e sta mettendo mano al nostro avvenire. Di chi ieri sapeva quel che sarebbe successo oggi e oggi, grazie alla potenza di Google, può decidere il domani di miliardi di persone.

L'umanesimo delle macchine. "In due o tre anni", ci racconta tranquillo, "sarà impossibile dimenticare, perdersi, annoiarsi, restare soli. Vivremo in un mondo più felice, più trasparente, conosceremo persone nuove e avremo più tempo da dedicare a noi stessi. Sarà, per la prima volta, una rivoluzione per l'intero pianeta e non solo per una piccola elite. Tutto grazie agli smartphone che avete già in tasca, ai tablet che si diffonderanno nei prossimi anni e ai super computer che formano quella nuvola digitale, il "cloud", dove stiamo raccogliendo una grande quantità di informazioni".

Grazie per l'attenzione

matteo.cavallini@tesoro.it