Ministero dell'Economia e delle Finanze

La sicurezza come fattore abilitante nelle forniture di servizi cloud

Matteo Cavallini

Università Roma Tre - 19 gennaio 2012, Roma

consip

ULS Unità Locale di Sicurezza

Chi sono

- Dal 2007 sono il Resp. della Unità Locale Sicurezza MEF/Consip
- Ho partecipato al progetto GovCERT.it
- Sono il Vice Presidente del capitolo italiano della Cloud Security Alliance
- 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

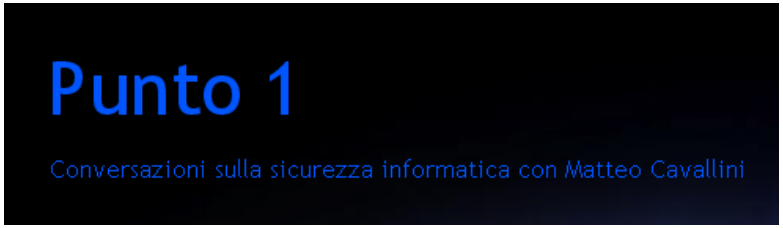
Sono certificato:

- Lead Auditor ISO 27001
- EUCIP Professional con profilo "Security Adviser"

Cosa faccio

- Coordino le attività di Prevenzione e Gestione degli incidenti informatici per il Ministero dell'Economia e Consip
- Sono il focal point per le tematiche di Cyber Security del Competence Center di 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



sito: www.matteocavallini.com
twitter account: @Nientenomi

consip

Ministero dell'Economia e delle Finanze

I media e il cloud computing

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

consip

Ministero dell'Economia e delle Finanze

E' 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

consip

Ministero dell'Economia e delle Finanze

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?

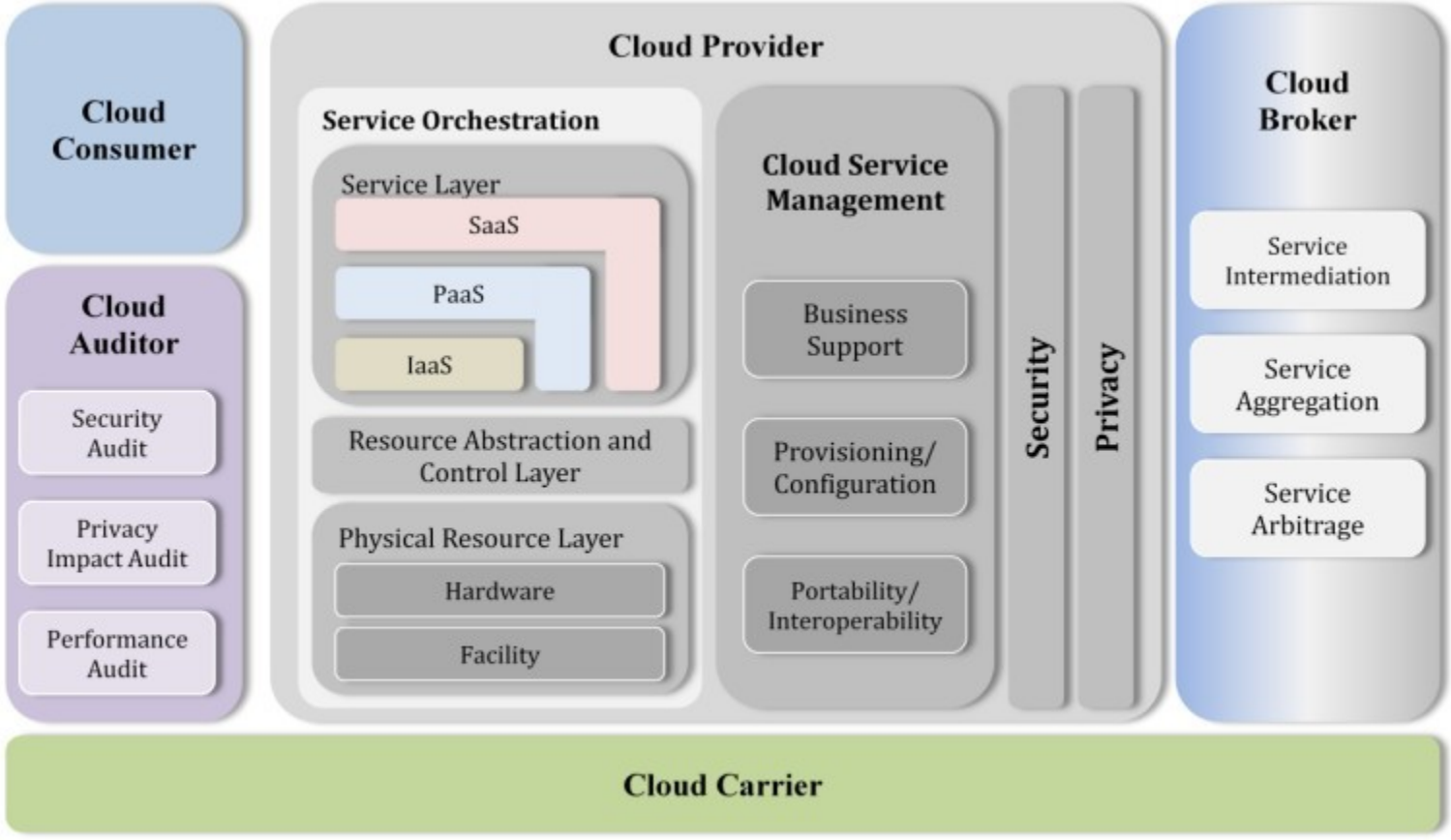
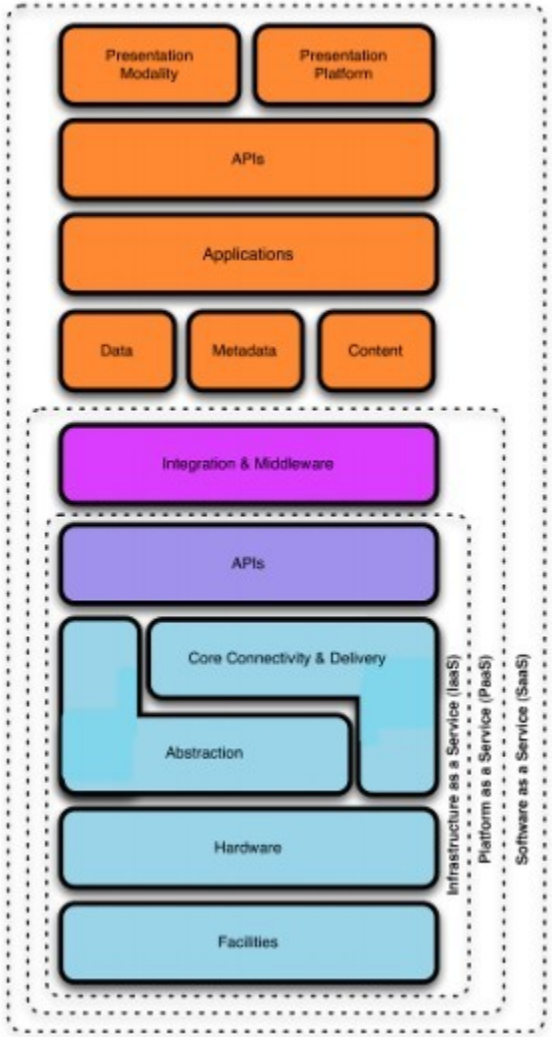


Figure 1: The Conceptual Reference Model

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

Ministero dell'Economia e delle Finanze

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

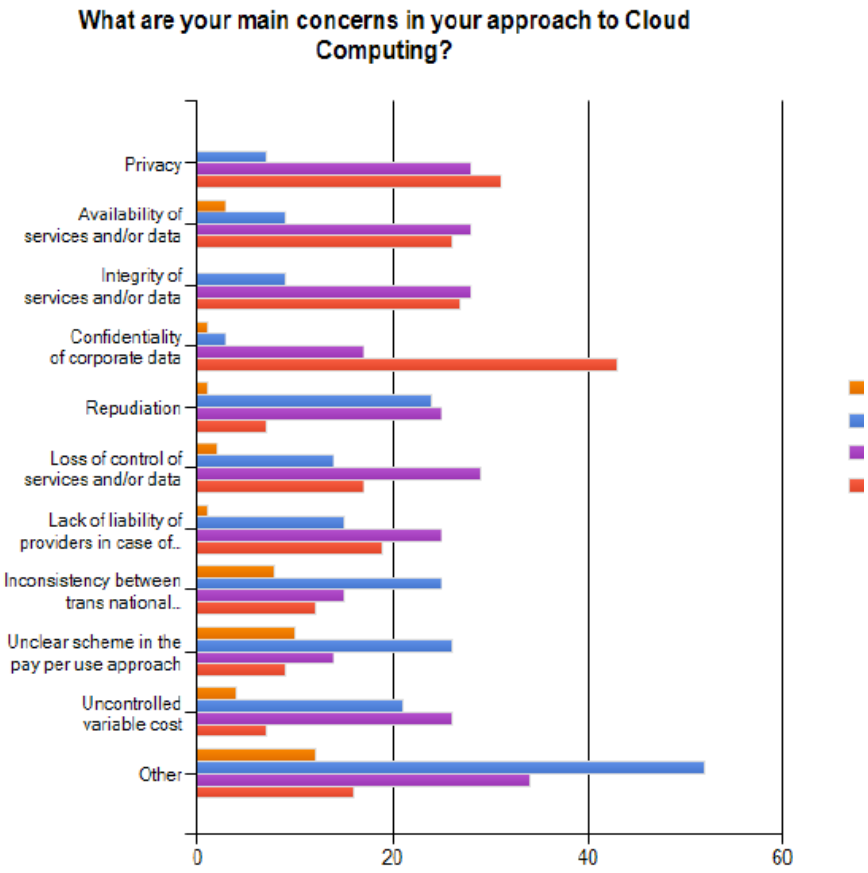
Regole per il Cloud computing "nuvola" sicura per l'utente

infosec ISLAND

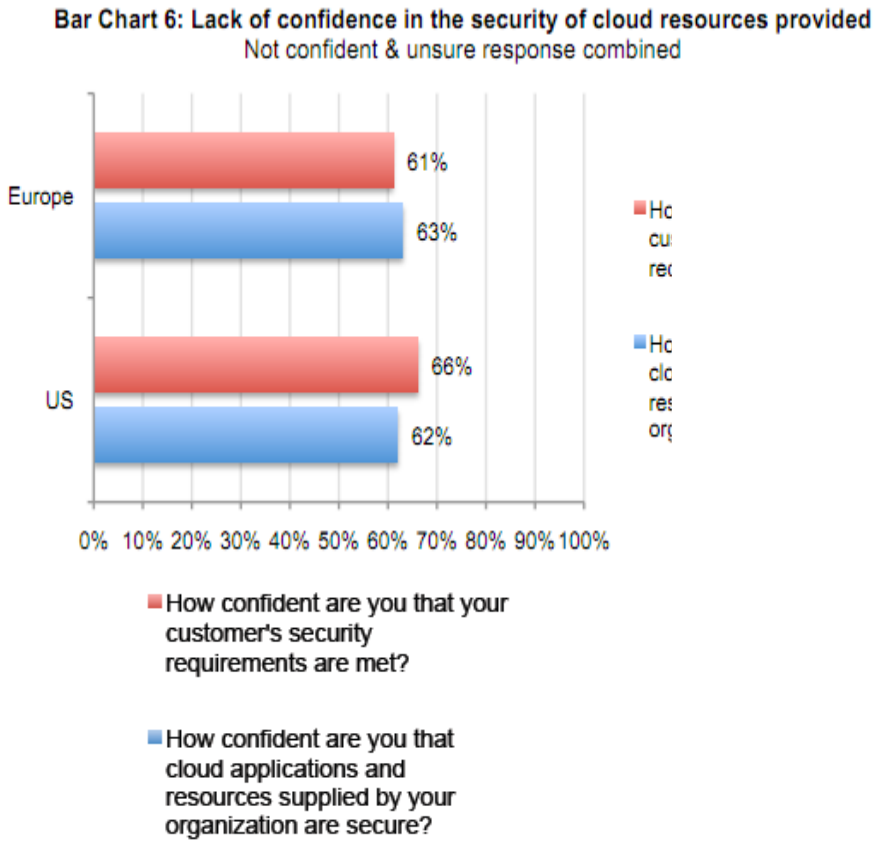
Epsilon Breach Deals Another Blow to Cloud Security

Friday, April 08, 2011

Le preoccupazioni



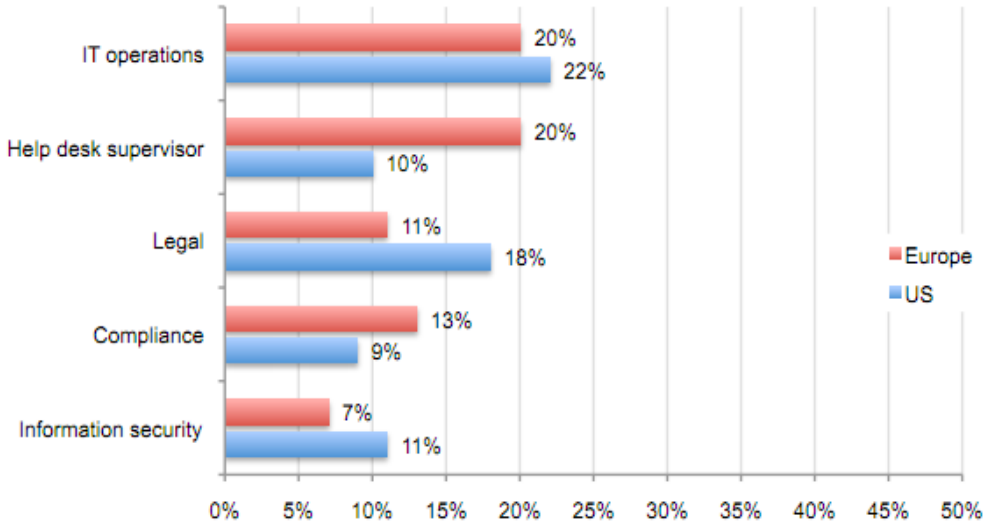
Fonte ENISA – Novembre 2009



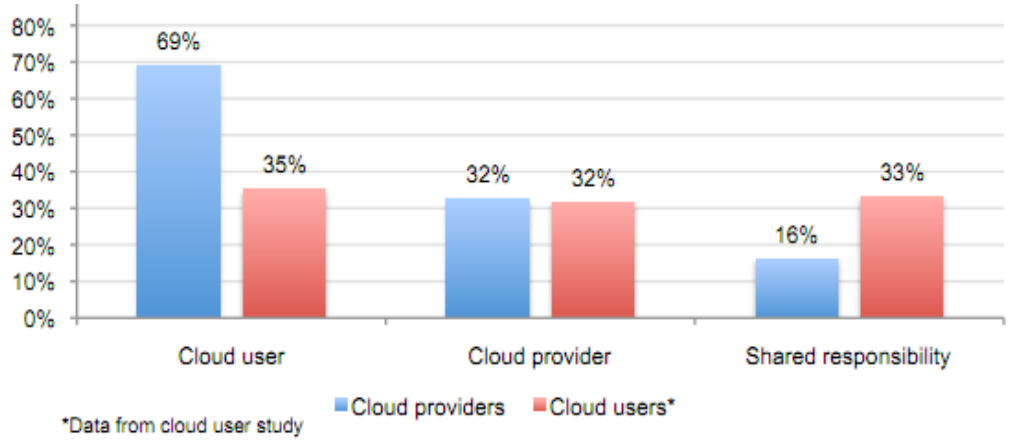
Fonte Ponemon Institute – Aprile 2011

Le responsabilità

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

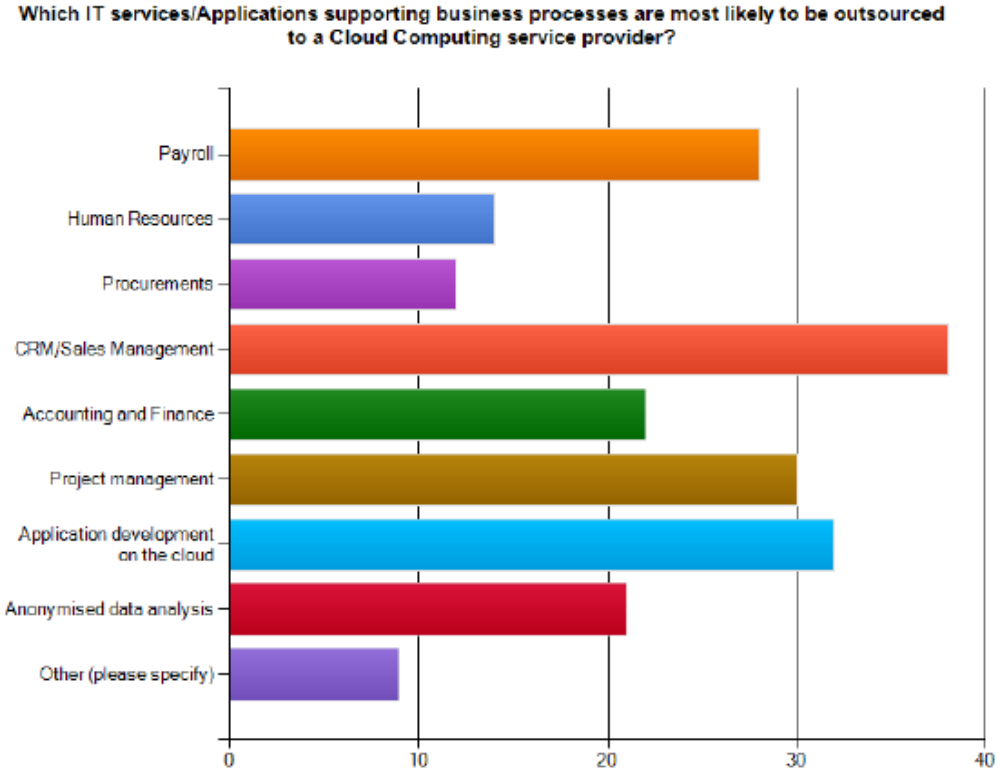


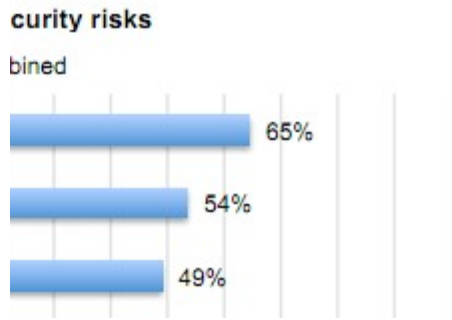
sible for ensuring the security of cloud resources by cloud providers?

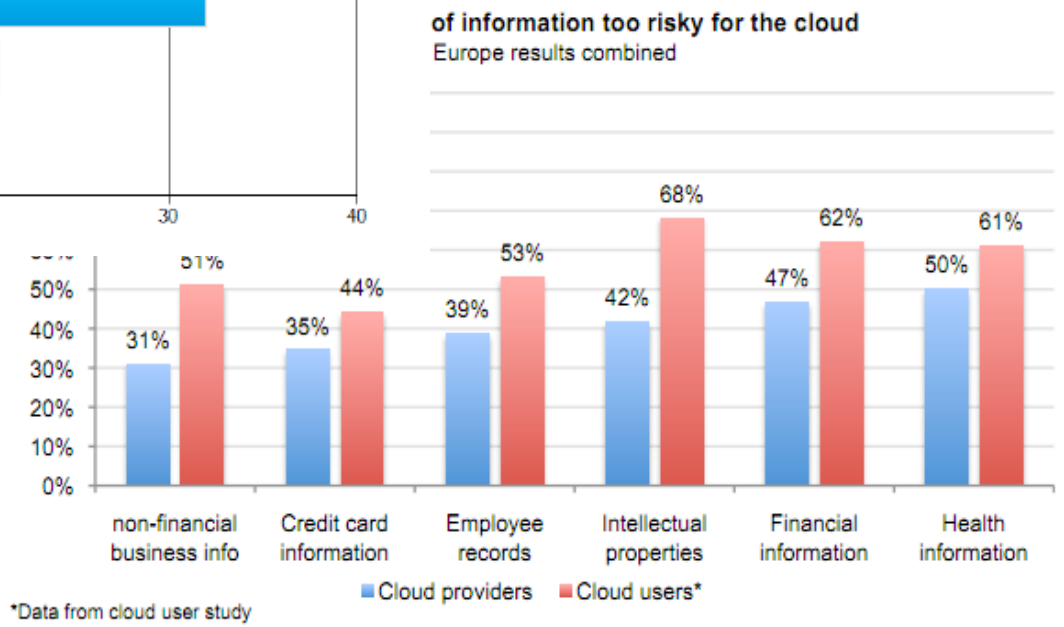


*Data from cloud user study

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

Security & Resilience in Governmental Clouds

Making an informed decision

January 2011

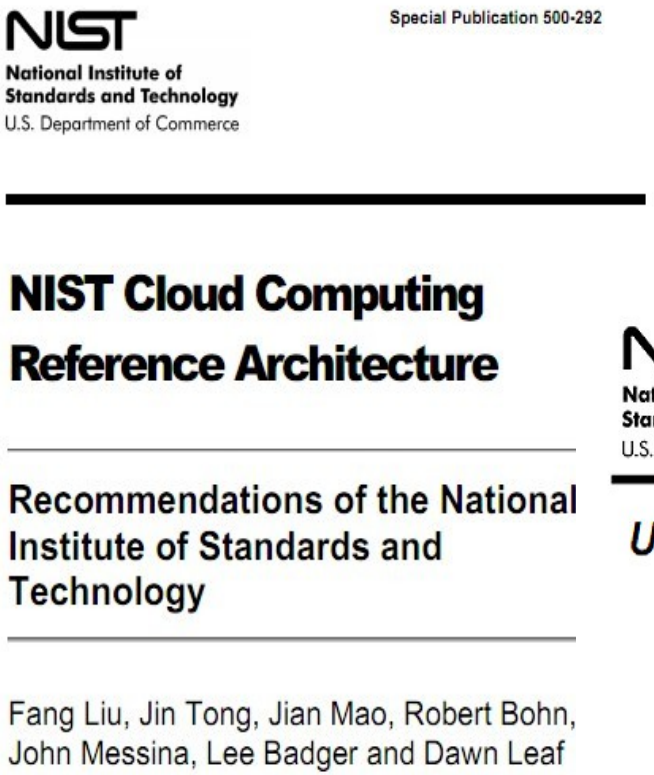
enisa
European Network and Information Security Agency

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

CIO COUNCIL

Draft version 0.96
November 2, 2010

I riferimenti

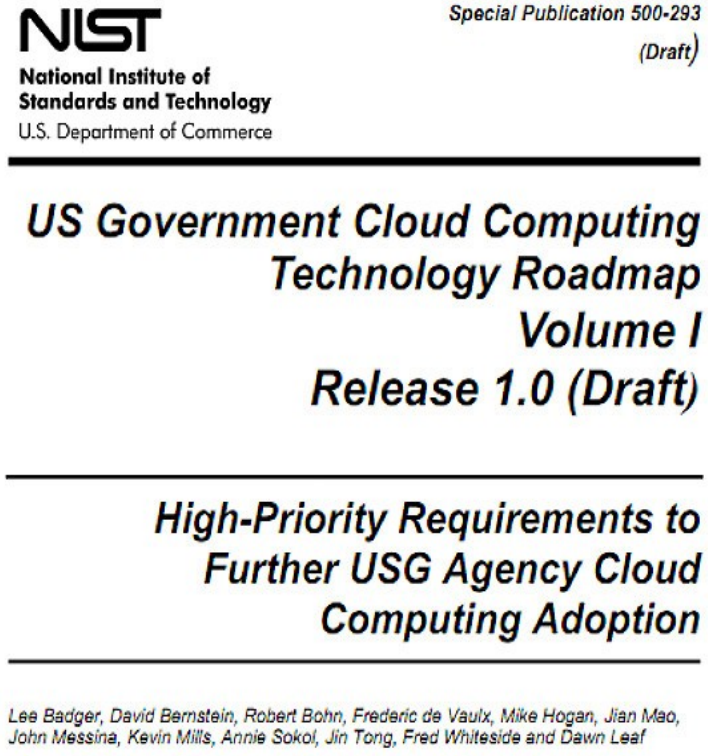

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 500-292

NIST Cloud Computing Reference Architecture

Recommendations of the National Institute of Standards and Technology

Fang Liu, Jin Tong, Jian Mao, Robert Bohn, John Messina, Lee Badger and Dawn Leaf

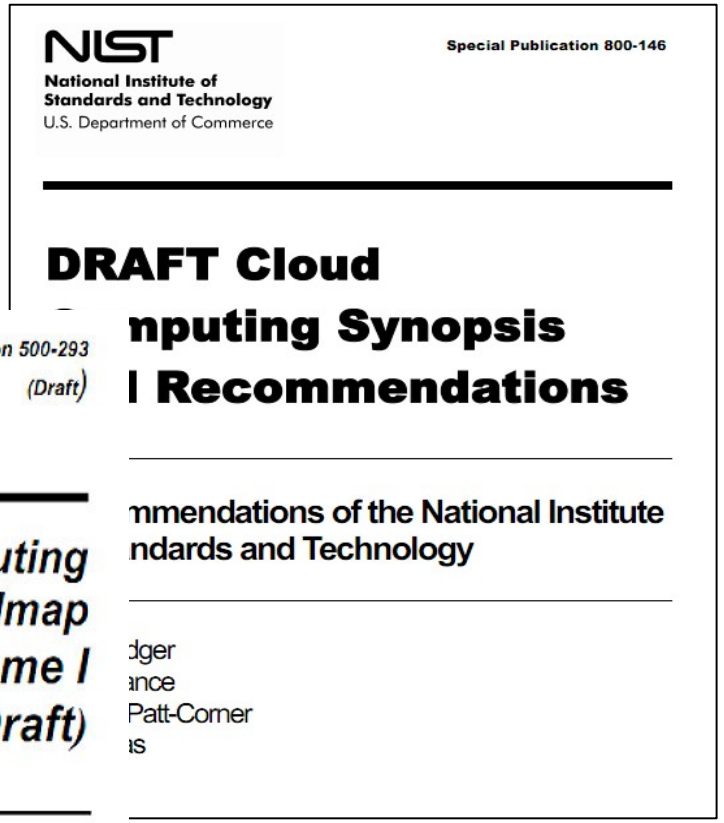

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

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


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

Special Publication 800-146

DRAFT Cloud
nputing Synopsis
l Recommendations

mmendations of the National Institute
ndards and Technology

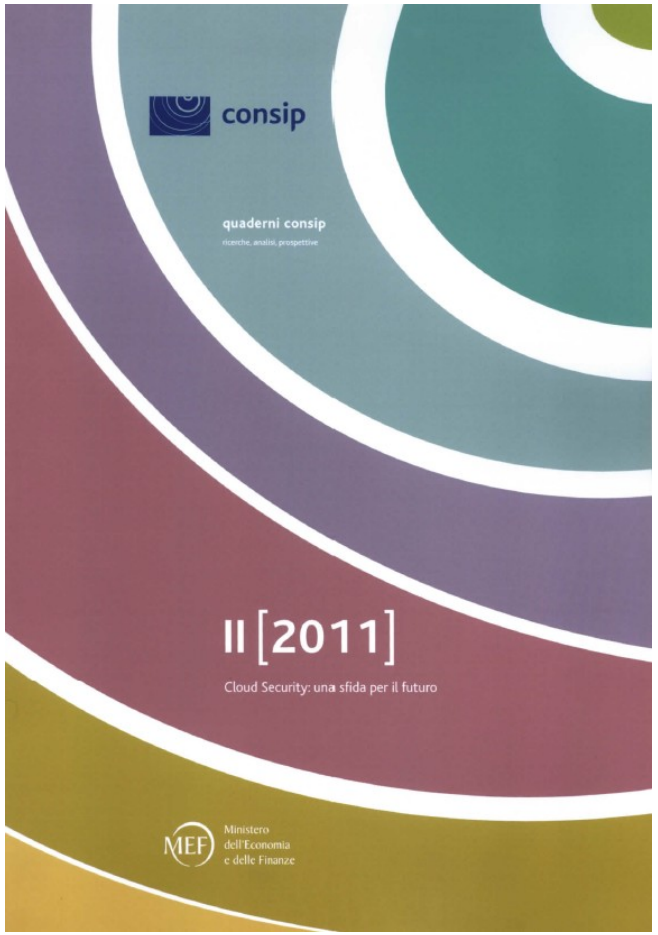
dger
ance
Patt-Corner
as

I riferimenti

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?

E' nata Cloud Security Alliance-Italy Chapter
https://chapters.cloudsecurityalliance.org/italy/

CSA IT Italy Chapter — cloud security alliance℠

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

Le valutazioni – i rischi

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 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 un piano di revisione della normativa sulla protezione dei dati personali.

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, soprattutto in presenza di servizi a valore aggiunto sono molto elevati (il caso Amazon è esemplare)
- 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 9 – 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:

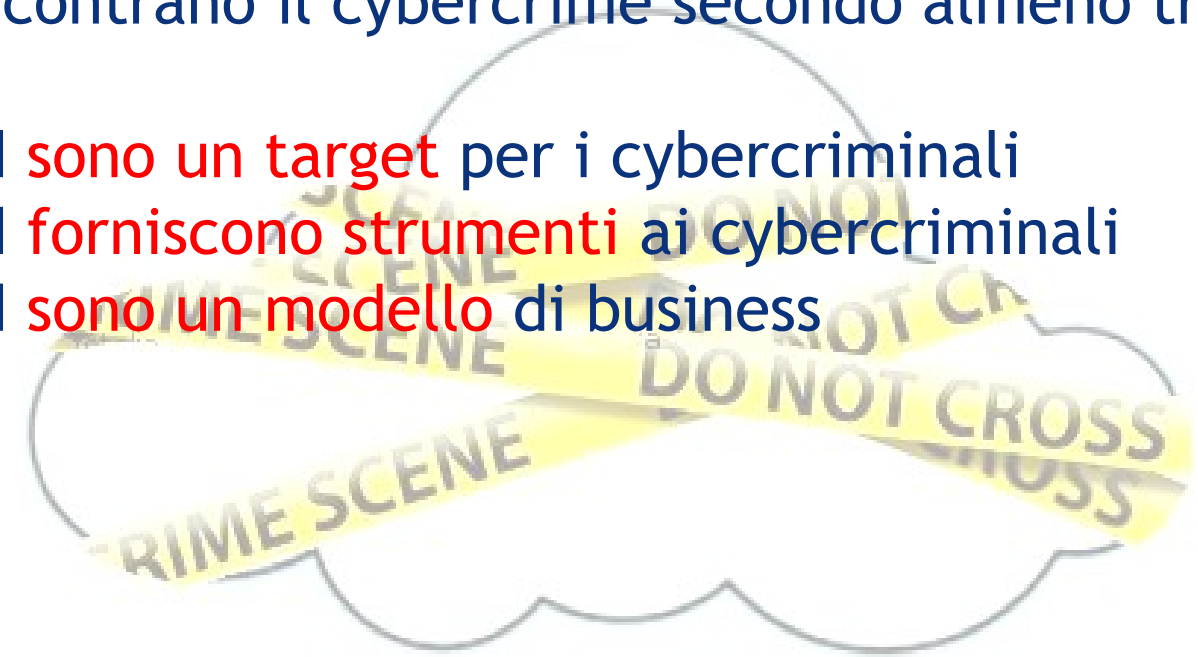
- La cifratura
- L'autenticazione forte
- Politiche a garanzia della qualità dei servizi di rete
- Ridondanza dei collegamenti

E a proposito di incidenti...

Cloud & Cybercrime

Le cloud incontrano il cybercrime secondo almeno tre direttrici:

- le cloud sono un target per i cybercriminali
- le cloud forniscono strumenti ai cybercriminali
- le cloud sono un modello di business



consip

Ministero dell'Economia e delle Finanze

E a proposito di incidenti...

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.

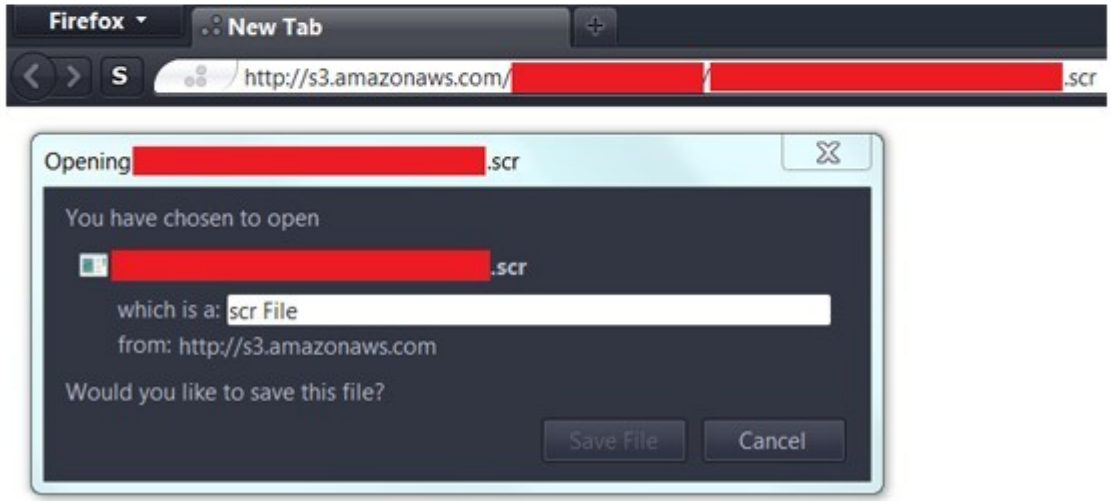
Simply upload your network capture, start your job, and WPA Cracker will email you the results within minutes! *Run It* →

E a proposito di incidenti...

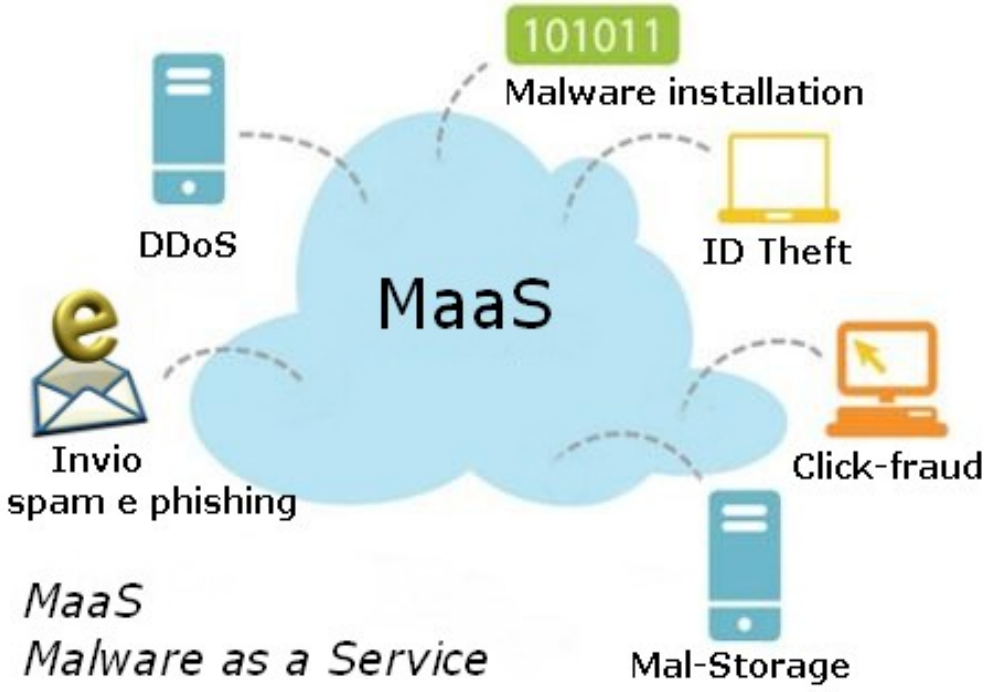
Financial data stealing Malware now on Amazon Web Services Cloud

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.



E a proposito di incidenti...



consip

Ministero dell'Economia e delle Finanze

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

cloud CSA security alliance

Copyright © 2011 Cloud Security Alliance

www.cloudsecurityalliance.org

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".

consip

Ministero dell'Economia e delle Finanze

Grazie per l'attenzione

matteo.cavallini@tesoro.it