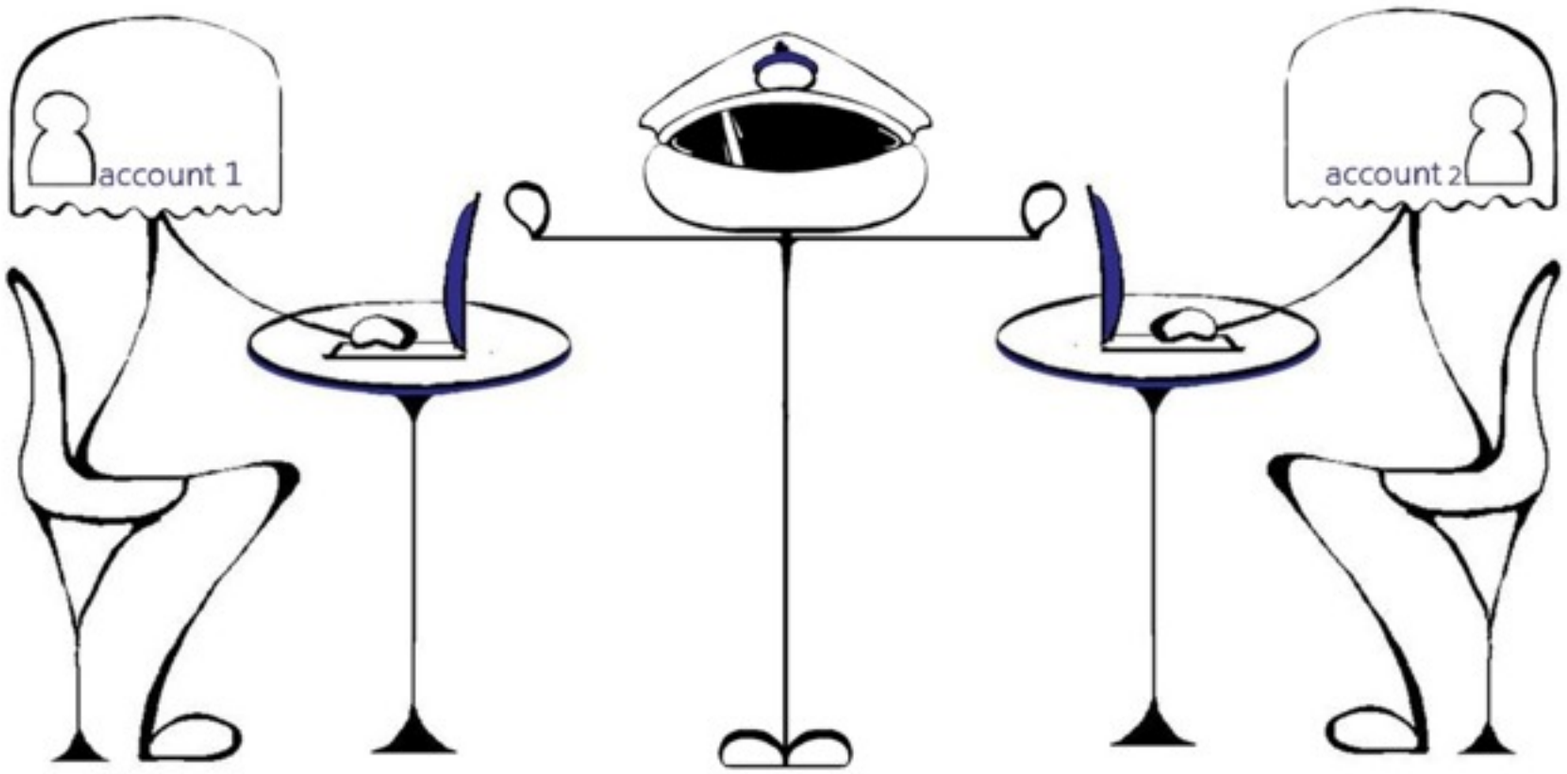


Il problema dei furti di identità nelle infrastrutture Cloud e possibili rimedi

Giuseppe “Gippa” Paterno’
SMAU, 19 Ottobre 2012

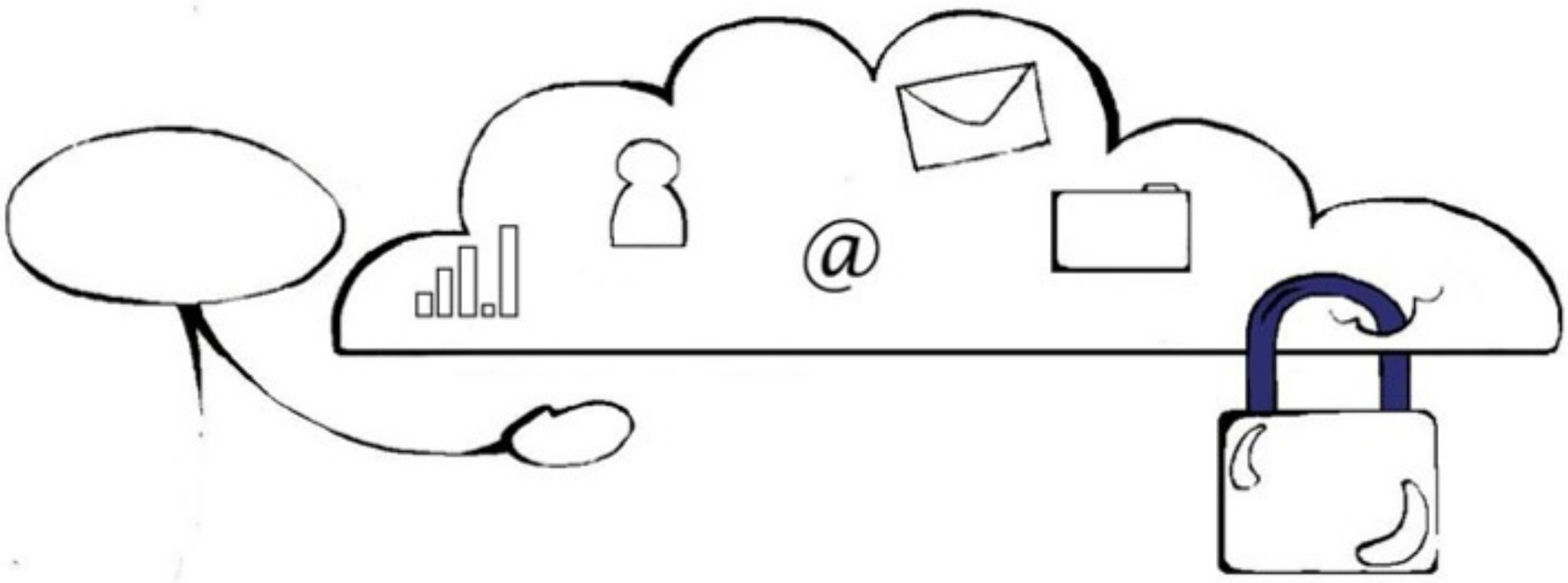
La mia identità: Giuseppe “Gippa” Paternò

- **Director Digital di GARL**, la Banca Svizzera dietro il servizio SecurePass
- **EMEA technical manager di Canonical**, la società dietro Ubuntu.
- Ricercatore di sicurezza e opensource, membro di sikurezza.org e appassionato del “Pinguino”
- Pilota “della domenica” di aerei
- Cuoco non professionista (Benedetta Parodi, ti sfido!!! :)
- Radioamatore con la passione per i “WiFi strani”: la mia associazione ha il “world record” di 304km in WiFi!!!

Il Cloud, questo sconosciuto!

IaaS

SaaS



PaaS

... e che CaaSino!

Cosa si intende per “Cloud”

Si intende un insieme di servizi, solitamente “affittati” da un service provider o interni (per grosse aziende) che diano:

- **Flessibilità**: la possibilità di espandere o contrarre la propria infrastruttura a seconda dei bisogni dell’IT.

- **Resilienza**: Alta affidabilità e disponibilità dei propri servizi IT, assicurando la continuita’ di servizio

- **Accessibilità**: Servizi fruibili da qualsiasi punto del pianeta con una semplice connessione ad Internet

- **Ottimizzazione dei costi**: si paga realmente quanto si usa la propria infrastruttura IT, evitando gli sprechi.

Il Cloud: IaaS

IaaS

=

Infrastructure as a Service

- L'affitto di una infrastruttura virtuale presso un service provider composta principalmente da server virtuali e reti virtuali
- Esempio: Amazon Web Services, Moresi.Com, ecc....
- Rischio di sicurezza: esposizione del pannello di controllo a Internet e controllo totale dell'infrastruttura da parte di un attaccante

Il Cloud: SaaS

SaaS

=

Software as a Service

- L'affitto di un applicativo qualsiasi, solitamente web-based, erogato in alta affidabilita' e accessibile dovunque
- Esempio: SalesForce.com, Office 360, ecc...
- Rischio di sicurezza: esposizione dei dati aziendali su Internet e data leaking da un potenziale attaccante o concorrente

Il Cloud: PaaS

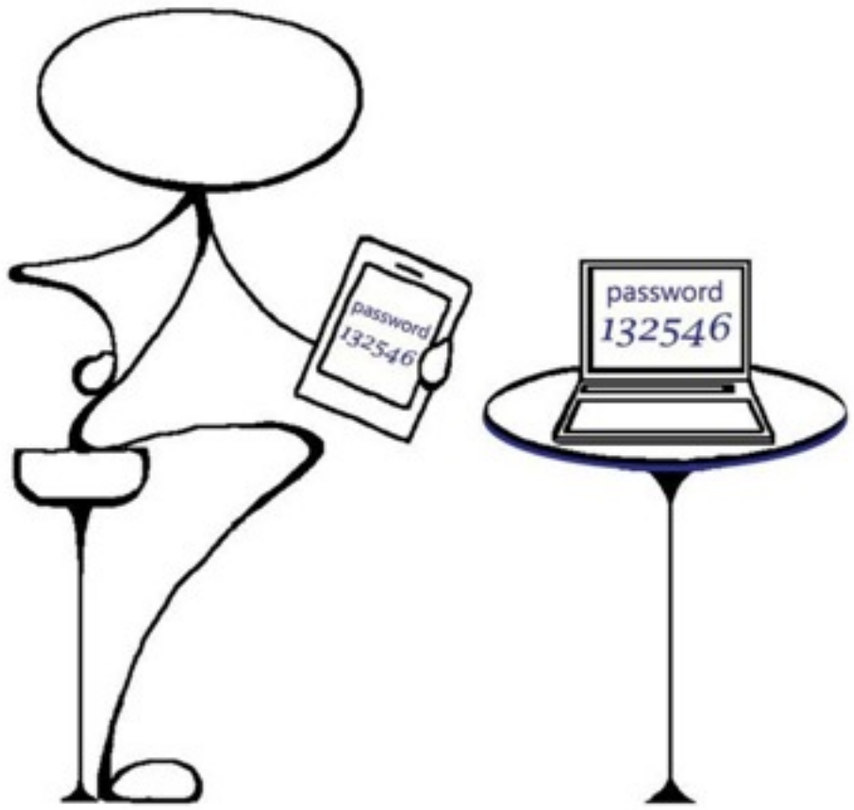
PaaS

=

Platform as a Service

- L'affitto di un ambiente operativo che ospita il PROPRIO applicativo. A differenza dello IaaS, il PaaS non si occupa del sistema operativo, ma di "operare" l'ambiente applicativo (linguaggi, framework, database, ecc...)
- Esempio: Microsoft Azure, Google App Engine, CloudFoundry, ecc....
- Rischio di sicurezza: esposizione del pannello di controllo a Internet, controllo totale dell'infrastruttura da parte di un attaccante, esposizione dei dati aziendali su Internet e data leaking da un potenziale attaccante o concorrente

Complicazione: BYOD



- Yet another marketing buzzword :)
- BYOD = Bring Your Own Device
- Usare il proprio device “consumer” all’interno della realta’ aziendale: iPad/iPhone/Android/....
- Rischio di sicurezza: la perdita del device comporta accesso a dati sensibili. Molte app per iOS/Android hanno una “chiave statica” che elimina la procedura di identificazione.

Le vittime famose del furto di identità

SAMSUNG

IEEE

LinkedIn

... e molti altri!

I furti di identità in cifre

10	milioni di vittime di furti di identità solamente negli USA nel 2008 (Javelin Strategy and Research, 2009)
221	miliardi di dollari all'anno la perdita economica mondiale relativa al furto di identità (Aberdeen Group)
5840	ore di lavoro per correggere i problemi relativi ai furti di identità, ovvero l'equivalente di due anni di lavoro di una persona (ITRC Aftermath Study, 2004).
35	milioni di dati compromessi tra le aziende e agenzie governative nel solo 2008 (ITRC)
2	miliardi di euro di danni alle aziende nella sola Italia nel 2009(Ricerca ABI)

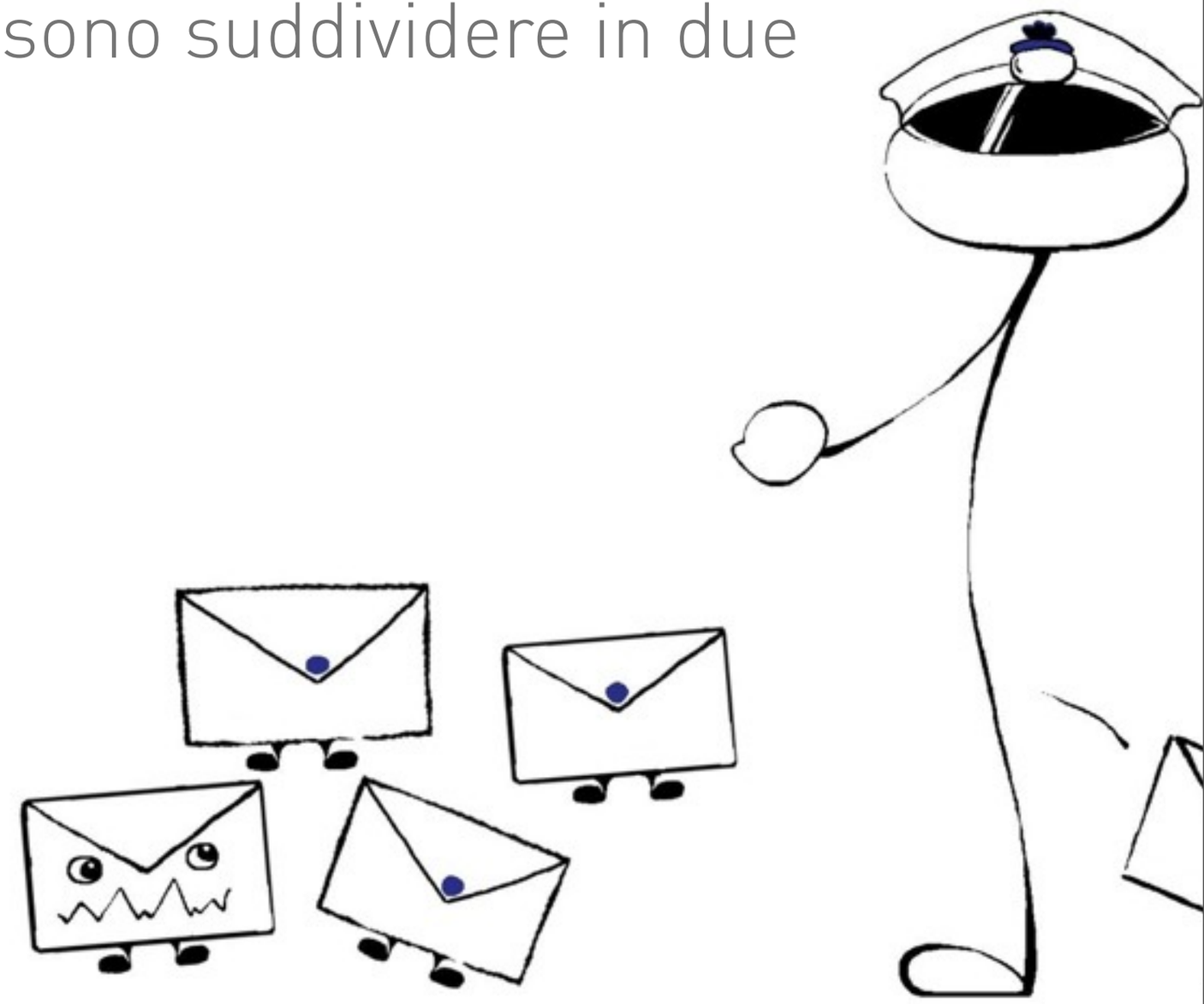
Il fattore umano, un esempio in aviazione

An organization can **minimize its vulnerability to human error and reduce its risks** by implementing human factors best practices [...] It contains guidance material which [...] should **help reduce the risks associated with human error and human factors**, and improve safety. It [...] concentrates upon risk and error management rather than risk and error elimination.

(EASA, JAR 145, Aviation Human Factors)

Il fattore umano nella sicurezza IT

- **Il fattore umano è la causa primaria delle intrusioni** da parte di hacker, governi stranieri o della concorrenza. Si possono suddividere in due problemi principali:
  - Password troppo facili
  - Social Engineering
- **Hope is not a strategy!**



Best practices, quando non funzionano

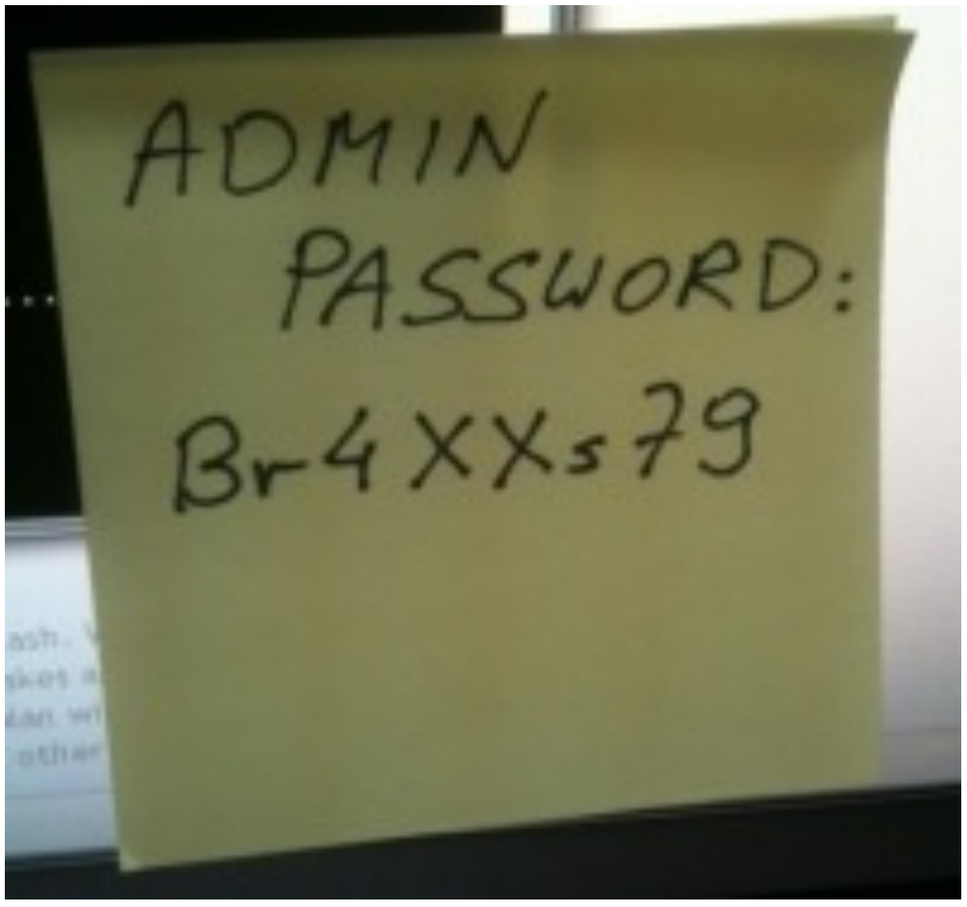
- La più quotata probabilmente è la BS/ISO 17799, divenuta ISO 27001
- Molte delle best practices coprono la parte di accesso fisico e accesso di rete:
  - non hanno più senso in un ambito Cloud
  - possono essere di aiuto per selezionare il fornitore
- **Ha senso la parte di controllo di accessi**:
  - identificazione sicura dell'utente (identity management)
  - necessario controllare chi sta facendo cosa (auditing)
  - permessi/diritti di accesso al singolo dato (policy management)

Rimedi ai furti di identità

Questo non è un rimedio!

:-)

Rimedi ai furti di identità



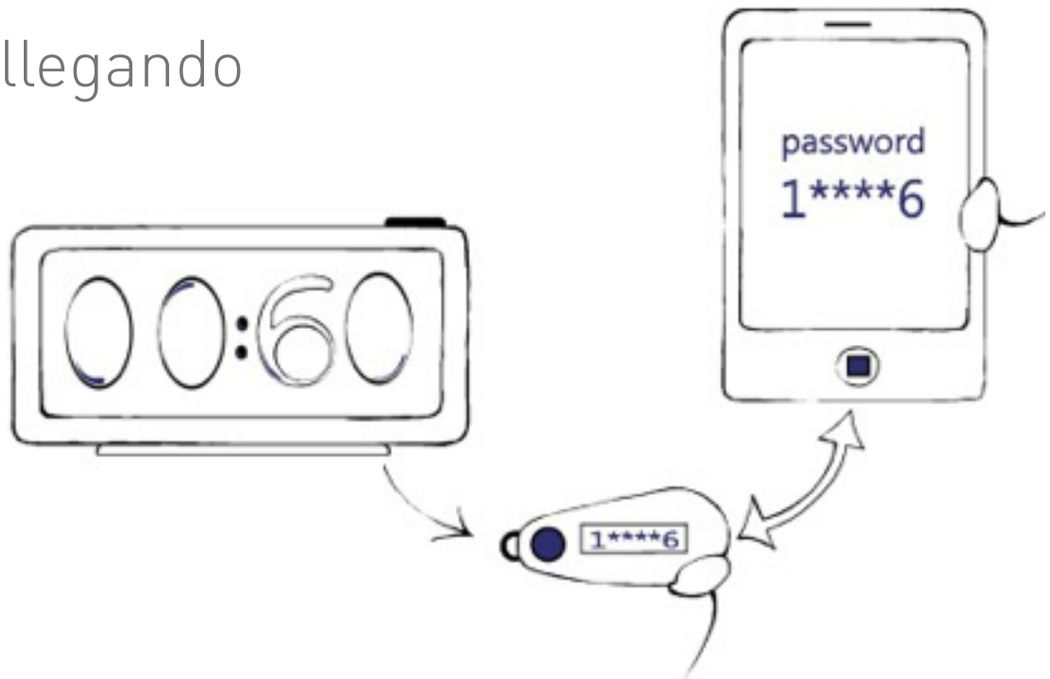
... e neanche questo

;-)

Rimedi ai furti di identità

La sicurezza deve essere semplice e trasparente, altrimenti nessuno le implementa!

- Autenticazione forte (strong autentication)
- Riconoscere da quali paesi l'utente si sta collegando (GeoIP)
- Patch, patch e patch!
- Programmazione sicura degli applicativi

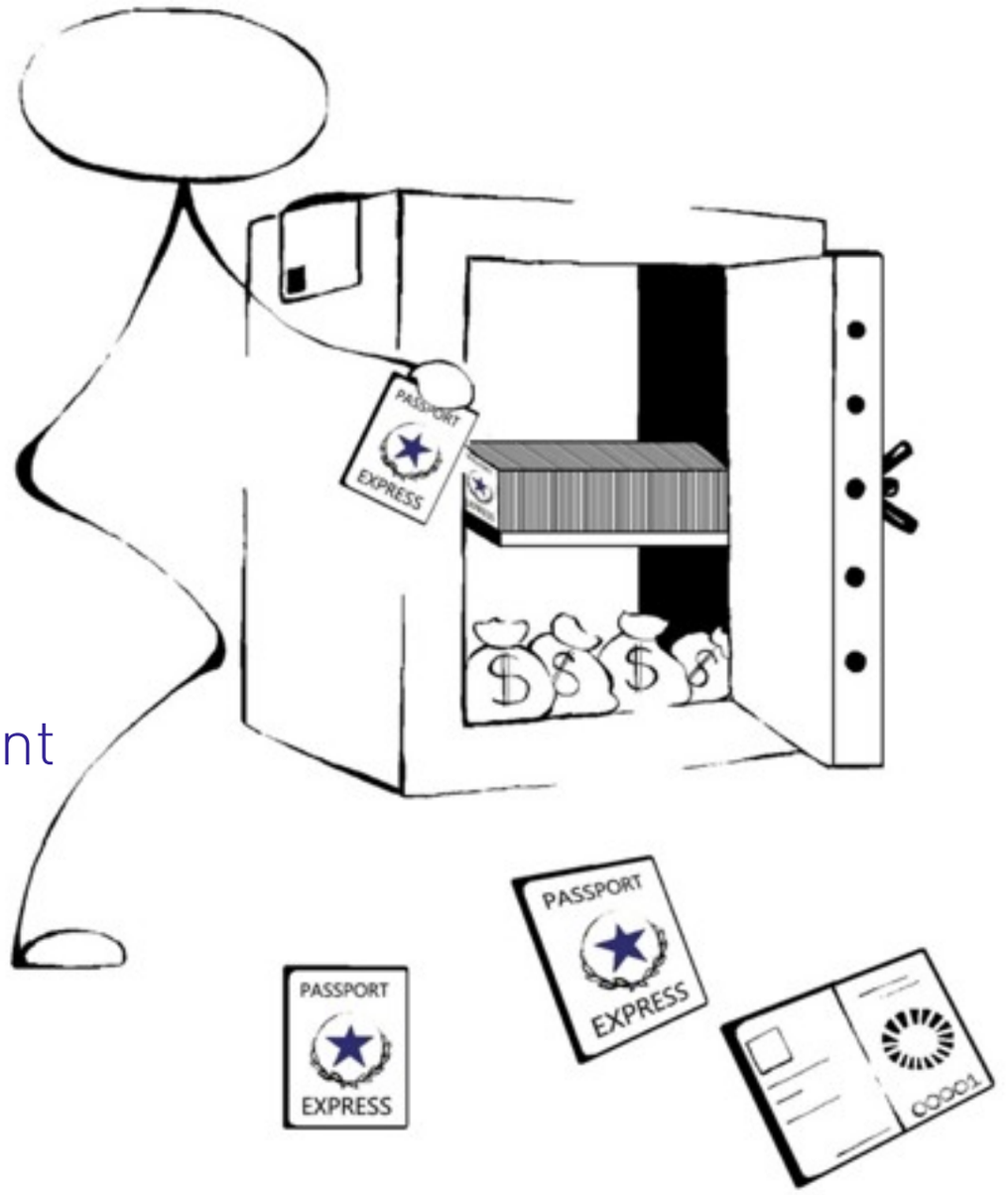


Intranet vs the Cloud and Trusted third party

- Nel mondo "tradizionale" il ruolo di identity management, auditing e policy è affidato tipicamente a Microsoft Active Directory

- AD non è stato ideato per un ambito Cloud distribuito "al di fuori dei confini" della propria azienda

- E' necessario un sistema di identity management distribuito con strong autentication che "funga" da Microsoft Active Directory per gli ambienti Cloud che sia in grado di ridurre gli "errori umani" tramite strong authentication e che sia affidato a una terza parte di fiducia



Un possibile rimedio: SECUREPASS™

- SecurePass è un sistema di Unified Secure Access per gli ambienti Cloud, web applications e devices di sicurezza

  - Strong authentication, tramite token hardware o su dispositivi mobili (iOS/Android/BlackBerry)

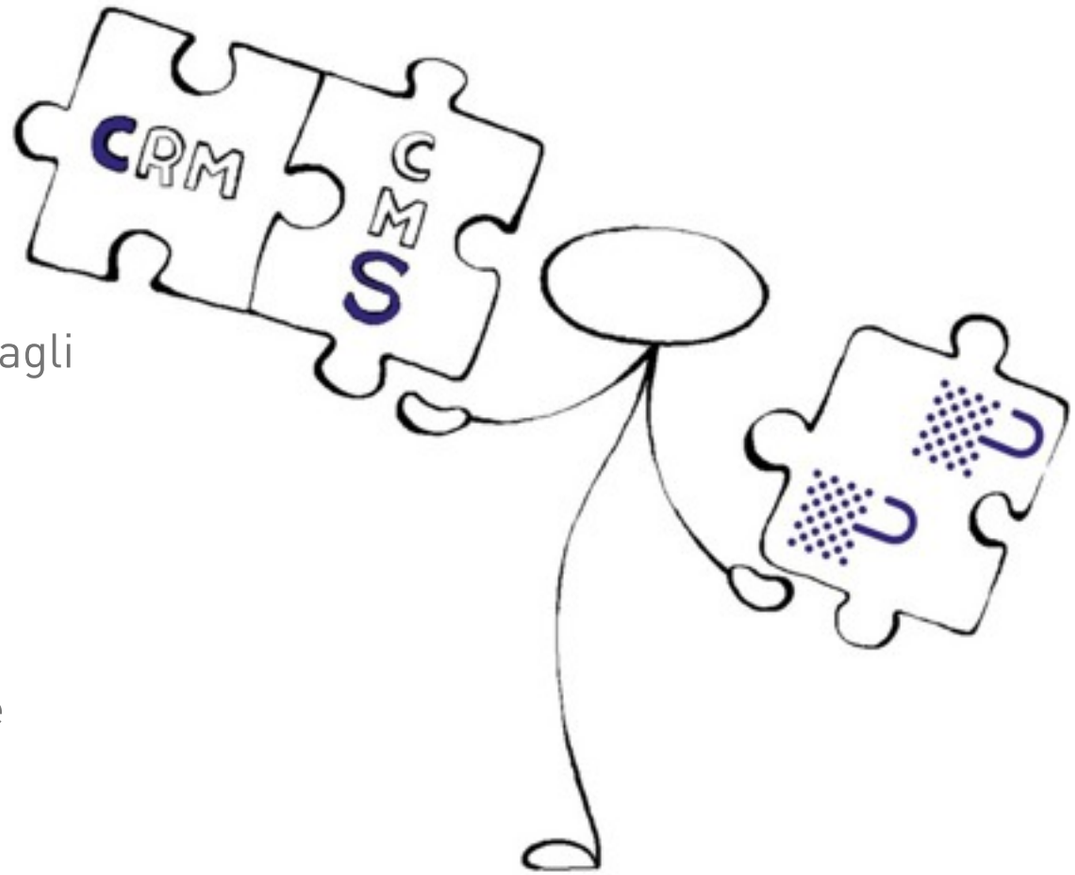
  - Identity Management, contiene informazioni sul proprio personale

  - Web seamless Single Sign-On, per semplificare l'accesso agli utenti

  - Basato su protocolli aperti: LDAP, RADIUS e CAS

  - Facile da integrare, in pochi minuti e' possibile proteggere infrastrutture e applicazioni

  - **Garantito da una Banca Svizzera**



Esempio: Moresi.com

- Hosting/housing provider Svizzero con due data centers in continua espansione. Sta spostando il focus da housing “tradizionale” a provider Cloud IaaS

- Clienti selezionati, tra le quali banche (DR) e grossi clienti internazionali

- Ogni cliente ha un accesso al proprio vDatacenter che puo’ orchestrare a piacimento

- **Obiettivo**: fornire un **accesso sicuro ai propri virtual datacenters**

vmware

User name:

Password:

Login

Moresi.Com SA

Sign up for an account
Forgot your password or user name?

Esempio: Assicurazione multinazionale

- La seconda piu' grande assicurazione mutinazionale, 48 aziende nel mondo, ognuna con il proprio consiglio di amministrazione e direttore generale

- Tutti i membri del consiglio di amministrazione accedono a documenti riservati attraverso vari dispositivi (laptop, tablet, smartphone) con alto rischio di furto di dati

- **Obiettivo**: fornire un accesso sicuro ai documenti riservati ai membri del consiglio di amministrazione ed evitare fughe i informazioni

Esempio: Azienda settore automobilistico

- Una delle prime 5 aziende del settore automobilistico con120.000 postazioni di lavoro

- Avevano bisogno di risolvere i problemi di sicurezza legati al BYOD (Bring Your Own Devices) da parte dei propri impiegati e direttori

- **Obiettivo**: fornire un accesso aziendale sicuro dai tablet e smartphone attraverso **SSL VPN e portali disegnati ad-hoc**

Q&A

Giuseppe Paternò

gpaterno@gpaterno.com
gpaterno@garl.ch

Web sites:
www.gpaterno.com
www.secure-pass.net

Twitter: @gpaterno