

Cybersecurity , Cloud e nuovi modelli di business

CesenaLab 22/11/18



CISE - AZIENDA SPECIALE
CAMERA DI COMMERCIO DELLA ROMAGNA
FORLÌ-CESENA E RIMINI

Mi presento

- Matteo Cecchini, nativo digitale nato troppo presto 😊
- Inizio a frequentare la Rete nel 1994
- 5 minuti dopo avevo già deciso quale sarebbe stato il mio percorso professionale
- Nel 1995 inizio ad lavorare come sistemista freelance
- Nel 2007 sono co-founder di T-Consulting, uno dei primissimi Managed Service Provider italiani
- Focus e passione costante su CyberSecurity e Business Continuity





CLOUD & NUOVI MODELLI DI BUSINESS



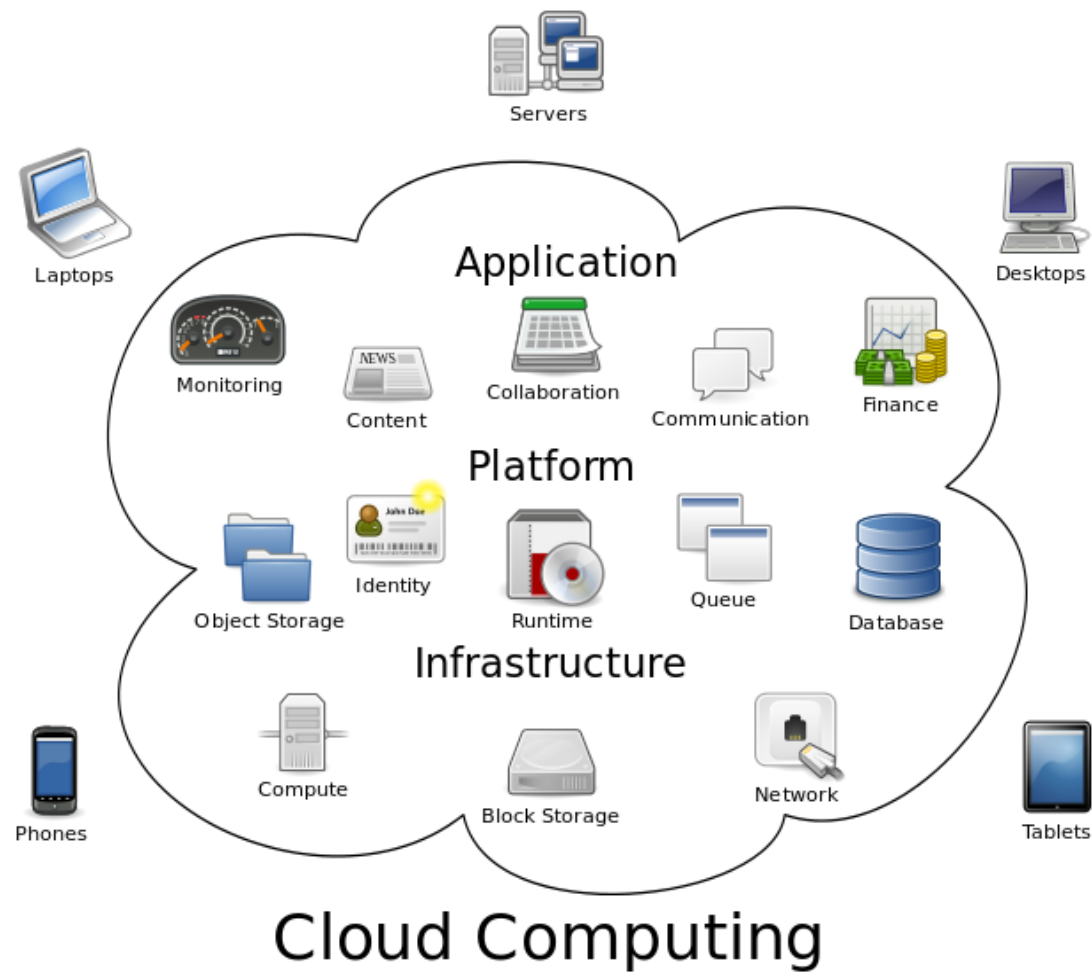
There is no cloud
it's just someone else's computer

Quindi???

Parliamo dell'accesso ad un servizio che mi consente di utilizzare applicazioni, piattaforme di sviluppo o infrastrutture IT (di qualcun altro) tramite Internet pagando solo l'effettivo consumo.



Le declinazioni del Cloud



Alcune applicazioni

- Archiviazione documenti
- Posta Elettronica
- CRM
- Applicazioni di Office Automation
- Backup
- Disaster Recovery
- Computing



Buy vs Rent - (Affittare o Acquistare ?)

- Per un'impresa, pensare di passare al Cloud, o di non passarci, è simile alla decisione di affittare od acquistare uno stabilimento produttivo
- Affittare una casa sarebbe come dire “housing-as-a-service”
- Nel lungo periodo l'affitto potrebbe essere più costoso dell'acquisto
- L'affitto non richiede grossi investimenti iniziali e permette un certo grado di flessibilità
- L'acquisto richiede un impegno ma permette all'utente di personalizzare a suo piacimento ogni aspetto

Impatto Economico

- ▶ La possibilità di usufruire di un prodotto, hardware o software in modalità as a service, consente di convertire i costi in conto capitale (CapEx) in costi operativi (OpEx)
- ▶ Questo permette di ridurre i costi di investimento iniziali e di operatività perché non avremo, nelle fasi iniziali, una spesa massiccia
- ▶ Soprattutto nell'ambito IT in cui è difficile calcolare il ROI è utile un approccio di "Pay-per-Use"

Cosa frena l'adozione del Cloud

- Timore della perdita di controllo su dati
- Ostilità culturale a portare all'esterno i dati maggiormente "core",
- Forti preoccupazioni sul fronte della sicurezza,
- Difficoltà non indifferenti sul tema dell'integrazione applicativa,
- Una certa confusione sui modelli di riferimento,
- Limitata diffusione della banda larga sul territorio nazionale.



Connettività: il primo passo

C'è bisogno di:

- Banda
- Bassa latenza
- Stabilità
- Tempi di intervento certi

Things I Need To Survive:

1. Coffee.
2. Tea.
3. Books.
4. More books.
5. Coffee.
6. More books.
7. Intelligent Conversation.
8. More tea.
9. A note book & pen.
10. More coffee.

Larghezza di banda

- Si intende la velocità della linea Internet
- Velocità Download = velocità con cui i dati arrivano dall'esterno verso la mia rete interna
- Velocità Upload= velocità con cui i dati transitano dalla mia rete verso l'esterno

Latenza

- E' la velocità di risposta di un sistema o di un collegamento di rete
- Deve essere BASSA
- Difficile da calcolare a priori
- Alcune tipologie di collegamento hanno una bassa latenza in ogni caso (es. fibra ottica)

Stabilità

- I servizi Cloud, per poter essere utilizzati in modo efficace, necessitano di stabilità nel collegamento alla Rete
- Alcune tipologie di connessioni sono instabili per loro natura

Tempi di intervento certi

- Tema spesso sottovalutato
- Se si verifica un problema di connettività DEVO avere la certezza del tempo di intervento
- LEGGERE i contratti 😊

Alcune delle domande da porsi prima di partire

- La propria infrastruttura è adeguata?
- La connessione Internet supporta il carico previsto?
- Quali possibilità ho in caso di fault locale per continuare a lavorare?
- Gli operatori della mia azienda sono adeguatamente formati?
- Quali modalità di ripristino in caso di fault del provider? (attacchi informatici, disastri naturali,...)

Clausole Contrattuali

- SLA, Service Level Agreement
- Gelocalizzazione dei dati
- Modalità di backup e disaster recovery
- Modalità di audit e di valutazione delle certificazioni
- Possibilità e supporto a migrazione ed interoperabilità (evitare il Lock-in)
- Distruzione dei dati dopo la cessazione del rapporto
- Penali per eventuali inadempienze?





CYBERSECURITY: NUOVI SCENARI LAVORATIVI, NUOVE MINACCE

Parliamo di dati...

Three main concerns

C

Confidentiality



I

Integrity

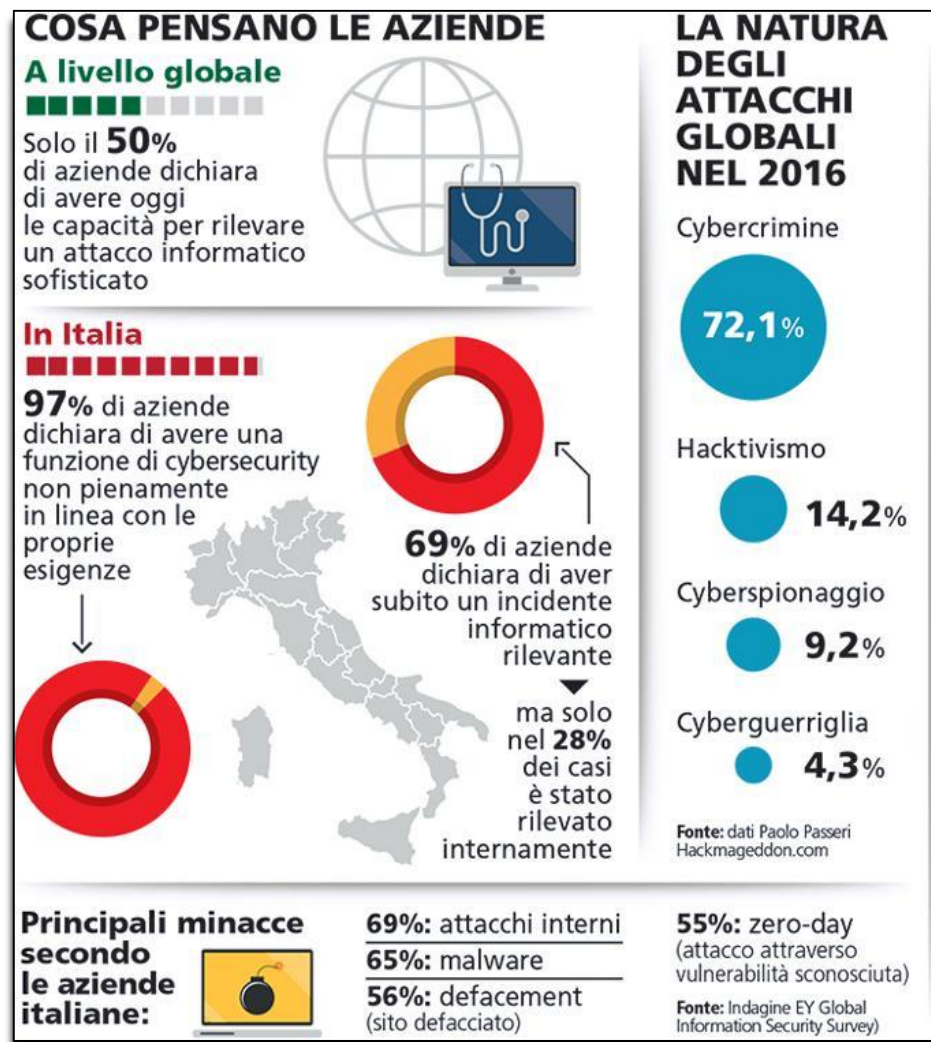


A

Availability

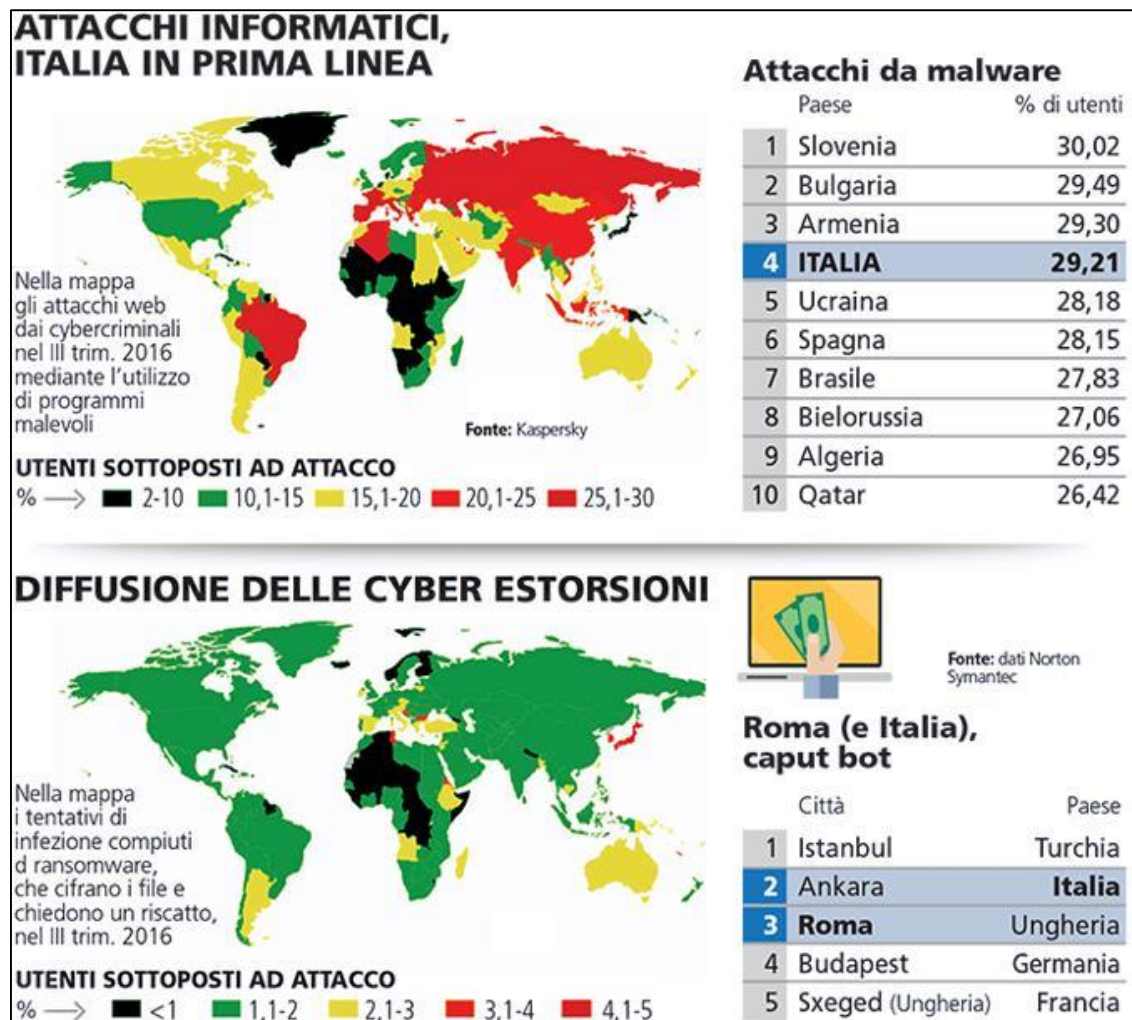


Stato dell'arte: security in Italia



- Il **97%** delle Aziende Italiane, contro il 50% di quelle globali, dichiara di non avere un Sistema di Sicurezza in grado di bloccare le minacce informatiche avanzate
- Il **69%** delle Aziende Italiane, dichiara di aver subito un attacco informatico rilevante

Stato dell'arte: security in Italia



Fonte: La Stampa 2017

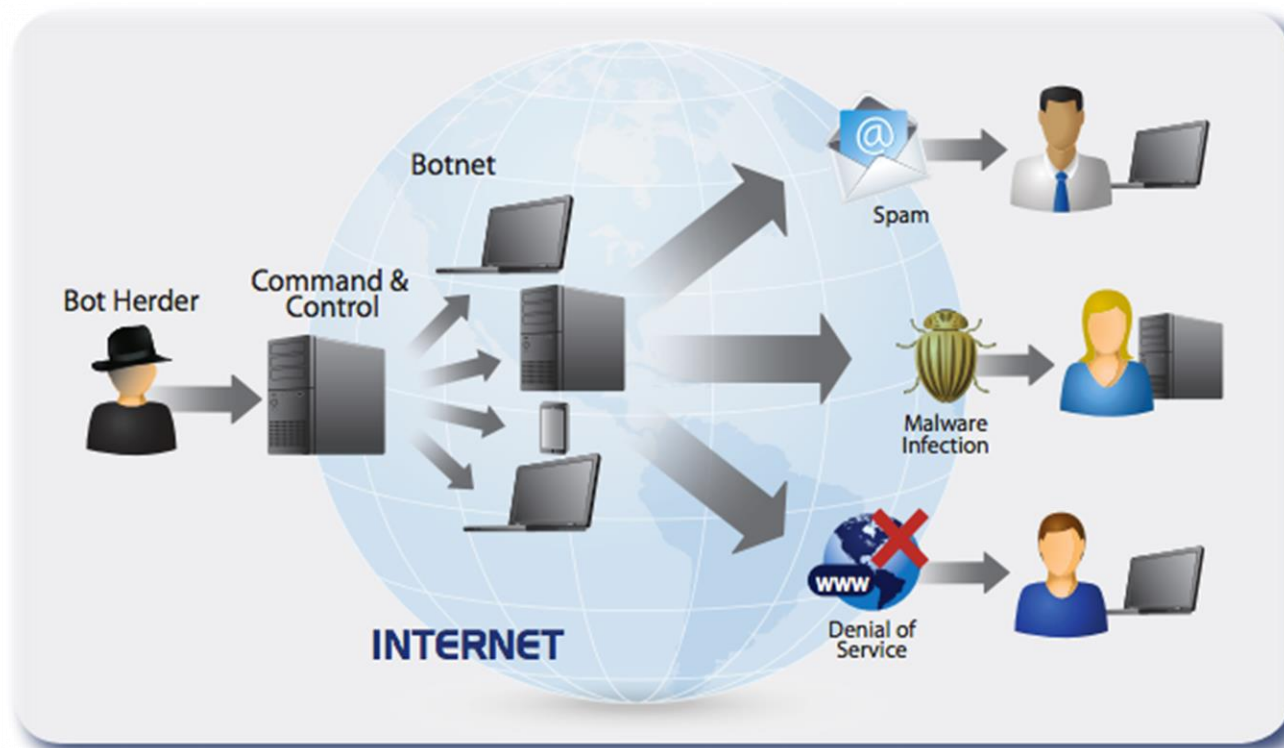
- Italia e' al 4' posto nel mondo come attacchi Malware, 29% utenti internet sono stati colpiti nel 2016
- Roma e' la 3 citta' nel mondo colpita da cyber estorsioni (ransomware ed affini)

... DAI PRIMI ATTACCHI



- Semplici nella loro esecuzione
- Basici: puntavano gli IP
- Brevi
- Unico fine: bypassare la barriera di sicurezza aziendale – hackerare un sito

... PASSANDO PER LE BOTNETS



- Attacchi piu' complessi
- Mirano alle applicazioni
- Intensi
- Fine principale: creare un disservizio, danneggiare le infrastrutture di rete

OFFRONO RESILIENZA ED ANONIMATO

PER ARRIVARE AD UNA NUOVA FRONTIERA DI ATTACCHI.... ... LE MINACCE AVANZATE PERSISTENTI

Un' APT (Advanced Persistent Threat) è un nuovo tipo di minaccia intelligente, ad alto valore tecnologico, pensata per avere un ritorno economico prolungato nel tempo e pieno controllo di uno specifico target



WHAT IS AN ADVANCED PERSISTENT THREAT?



Targeted

An individual organization, nation state or even specific technology is the focus. Infiltration is not accidental.



Advanced

An unknown, zero day attack that has malware payloads and uses kernel rootkits and evasion-detection technologies.



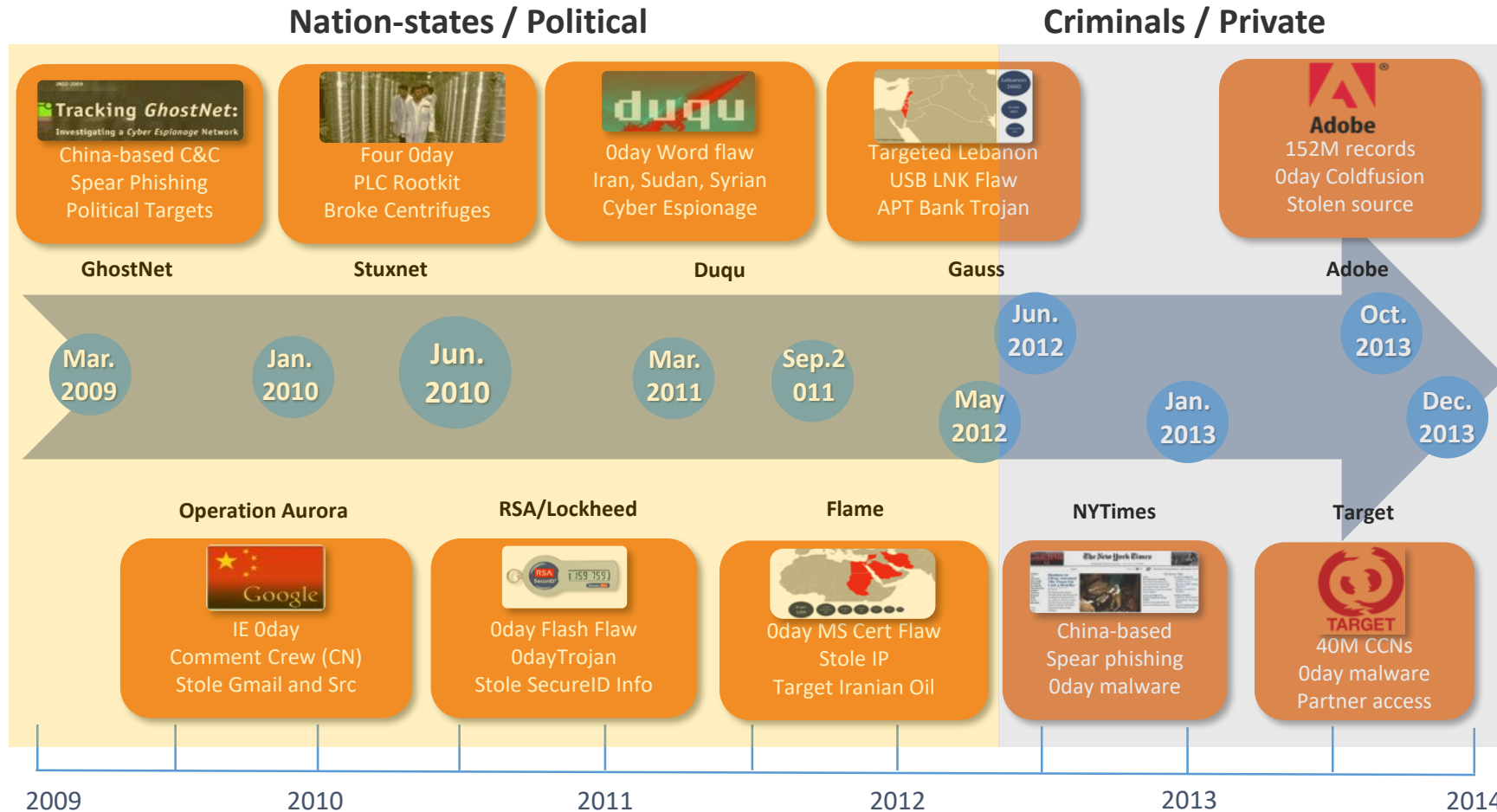
Persistent

It doesn't stop. It keeps phishing, plugging and probing until it finds a way in to serve malware.

Gli attributi che contraddistinguono una minaccia APT

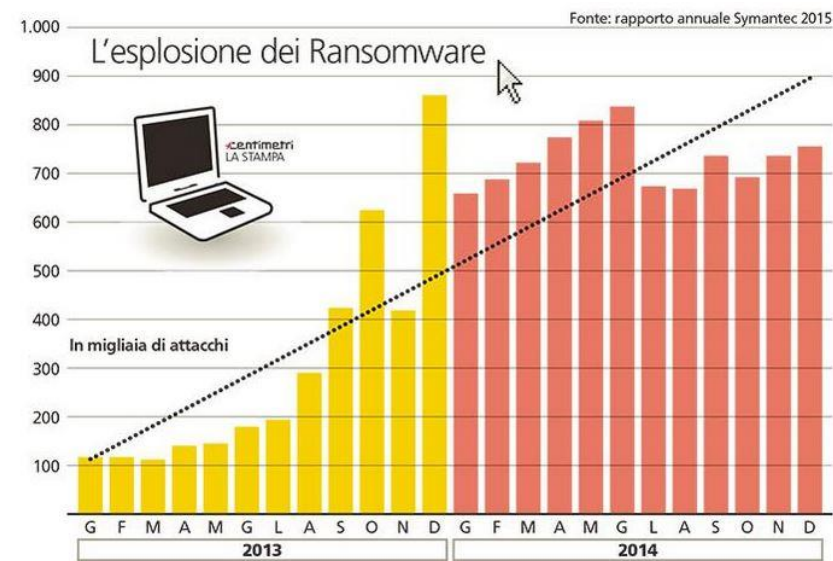
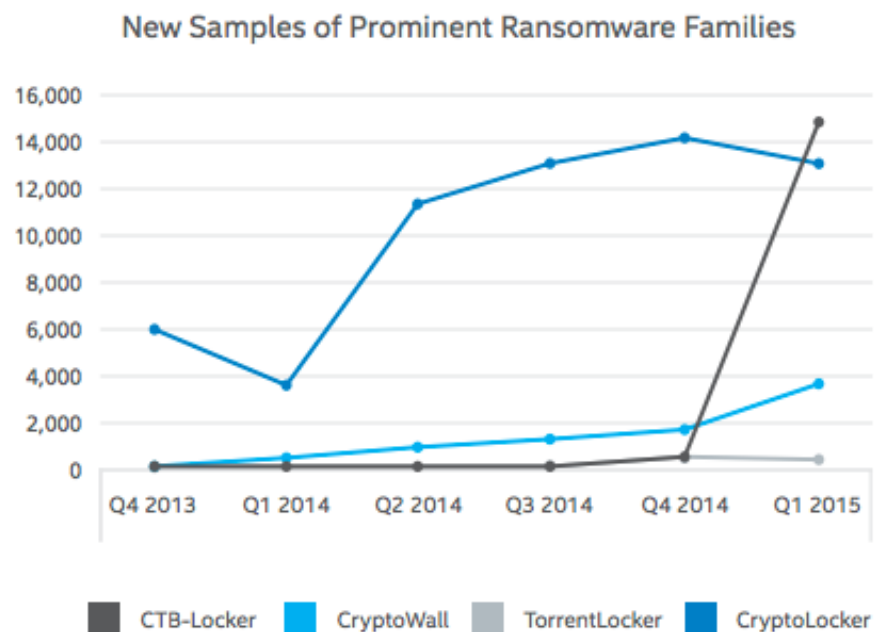
1. Avanzata
2. Persistente
3. Targettizzata

APT TIMELINE



RANSOMWARE: il protagonista del momento

Ransomware e' una forma di computer malware che blocca l'accesso al vostro computer o ai suoi file fino a quando non viene pagato un riscatto per riottenerne l'accesso.

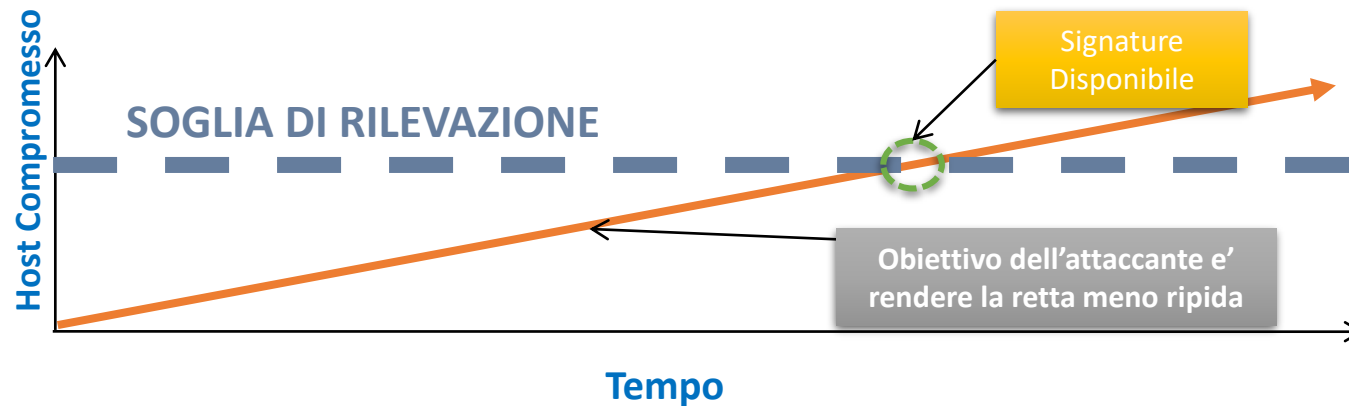


Source: McAfee 2015

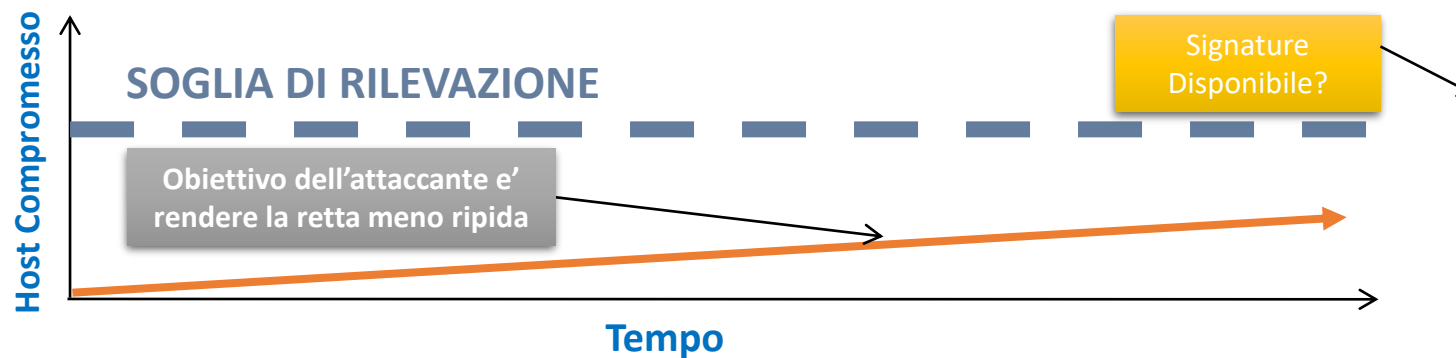
E L'ANTIVIRUS?

Gli antivirus sono la migliore protezione contro attacchi opportunistici non targettizzati offrendo una efficiente protezione seguente la creazione di una signature (impronta) descrivente la minaccia.
Tutto quanto sotto la soglia viene identificato come ZERO DAY

Opportunistico
Attacco



"Avanzato"
Attacco



I PIU' DIFFUSI RANSOMWARE

Cryptolocker, CTB-Locker, CryptoWall, Tesla Script, CryptorBit, KeyHolder, Operation Global, TorrentLocker, CryptoDefense, ZeroLocker, Ransom32

Colpiscono utenti Windows, Mac, Linux...



GENERATORE DI RANSOMWARE

The dashboard for 'Karmen' shows a 'Statistics Overview' with four key metrics: 1 Client, 0 Payments, 0 Earned, and 1284\$ Bitcoin Price. Below these are sections for 'Updates' (listing new designs, bug fixes, and version releases) and 'Infos' (current version 2.4, price to unlock, and contact info). A modal window titled 'Files encrypted' is overlaid, stating: 'All files are encrypted! Please follow the mind. In order to get the key to decrypt send this amount to our wallet Bitcoin. Decrypt files automatically. Interference with the program - can leave you without files.' It includes 'DEU' and 'ENG' language buttons and a progress bar at the bottom.

The 'Ransom32 - Stats' page displays the wallet address '1EnWWsdyrMiXPTU87bWtvW6zPL6ZczD61v' and a 75% payout ratio. Below are counters for Installs, Lockscreens, Paids, and Paid BTC, all currently at 0. The 'Client download' section allows configuring the ransomware's behavior: BTC amount to ask (0.1), checkboxes for 'Fully lock the computer', 'Low CPU usage', 'Show the lockscreen before encrypting', and 'Show a message box', and a 'Latent Timeout' section for days, hours, and minutes. A message box configuration shows options for Critical Error (Yellow Exclamation), Yellow Exclamation, and White Information. An error log entry reads: 'ERROR: main_gui_render.cc(237) Running without Renderer'. A 'Download client.scr' button is at the bottom, with a note: 'Don't worry if the download "hangs". While the download bar is shown, Tor is receiving the file. Just wait.'

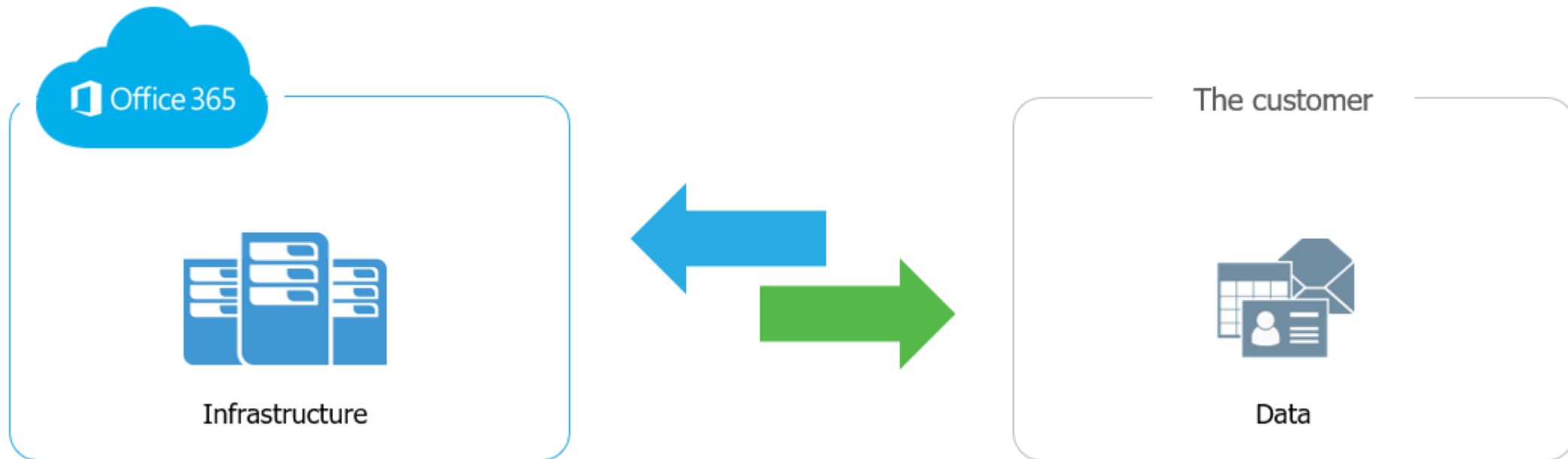
CyberSec & Cloud – Responsabilità condivisa

Questa è la percezione degli utilizzatori (l'esempio di Microsoft):



CyberSec & Cloud – Responsabilità condivisa

Questa è la realtà:



CyberSec & Cloud – Responsabilità condivisa

[Trust Center](#)[Privacy](#)[Prodotti](#)[Servizi](#)[Tutti i siti Microsoft](#)[Cerca](#)[Carrello](#) [Sign in](#)[Overview](#)[Sicurezza](#)[GDPR](#)

Overview

Sicurezza e privacy sono integrate nella piattaforma Microsoft Azure, a partire dal [Security Development Lifecycle \(SDL\)](#). Il Security Development Lifecycle gestisce la sicurezza in ogni fase di sviluppo e garantisce che Azure venga costantemente aggiornato per renderlo ancora più sicuro. [Operational Security Assurance \(OSA\)](#) è basato su informazioni e processi del Security Development Lifecycle per fornire un framework che garantisca operazioni sicure lungo l'intero ciclo di vita dei servizi basati sul cloud. Il [Centro sicurezza di Azure](#) rende Azure una piattaforma di cloud pubblico che offre monitoraggio continuo dello stato di sicurezza.

Per risorse tecniche sulla sicurezza di Azure, visita la pagina [Documentazione della sicurezza di Azure](#) >

Gestisci e controlla le identità e gli accessi degli utenti	Crittografa le comunicazioni e i processi operativi	Rafforza la sicurezza di reti e infrastrutture	Difenditi dalle minacce	Responsabilità condivisa
---	---	--	-------------------------	--------------------------

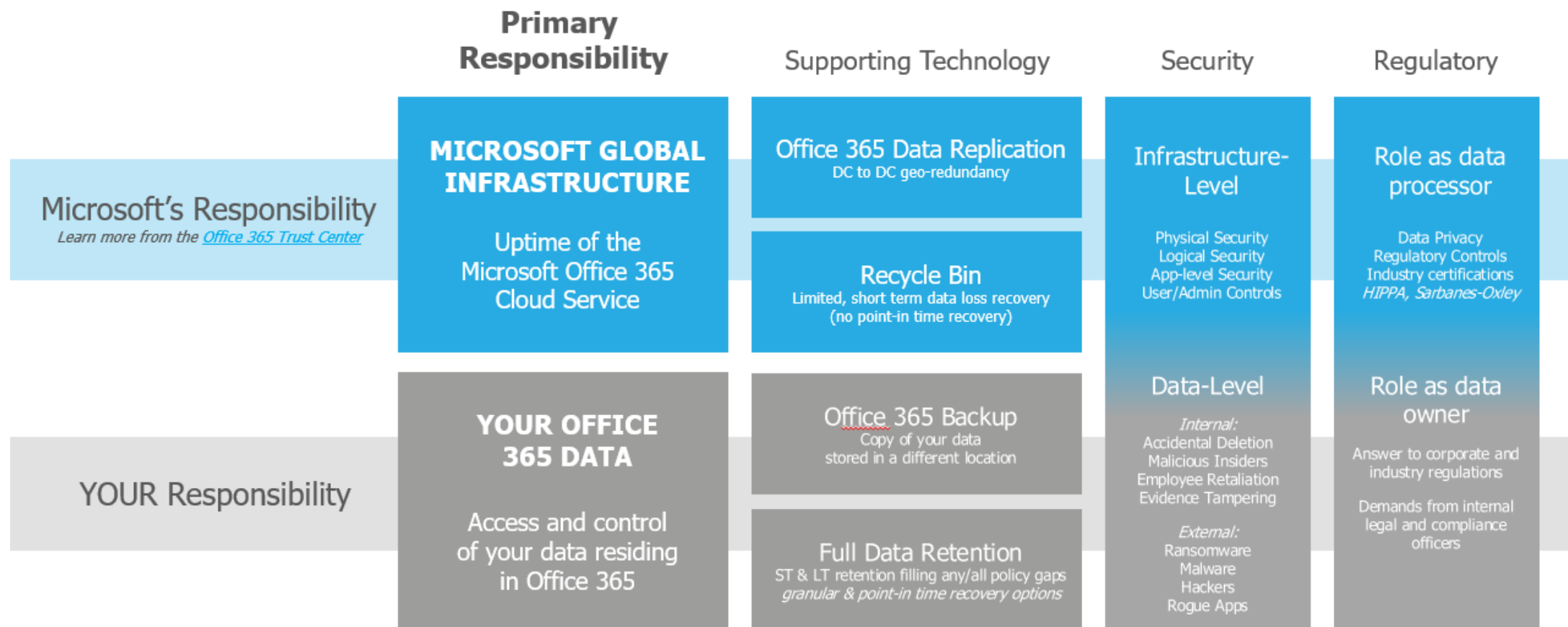
Nel considerare il cloud computing pubblico, alcune aziende credono erroneamente che dopo l'adozione del cloud il ruolo di protezione dei dati passi interamente al provider di servizi cloud (CSP). Non è così. Per definizione, i provider di servizi cloud garantiscono la sicurezza di determinati elementi, tra cui l'infrastruttura fisica e i componenti di rete, ma la sicurezza dei dati nel cloud comporta una responsabilità condivisa.

I clienti devono implementare procedure consigliate per la sicurezza e istruire gli utenti su come accedere ai servizi cloud in modo sicuro. Modelli di servizi cloud diversi usano modalità di gestione differenti.



CISE - AZIENDA SPECIALE
CAMERA DI COMMERCIO DELLA ROMAGNA
FORLÌ-CESENA E RIMINI

CyberSec & Cloud – Responsabilità condivisa



Backup dei dati Cloud: 6 ragioni per cui farlo



Accidental deletion



Retention policy confusion / gaps



Internal security threats
Malicious insiders / departing employees



External security threats
Ransomware / rogue apps



Legal and compliance requirements



Managing hybrid deployments and migrations

Un altro aspetto delicato: l'identità...digitale



Fiducia?



E sempre a proposito di fiducia

*I dilettanti attaccano i computer;
i professionisti prendono di mira le
persone*



Data:
lunedì 05.10.2015

www.italiaoggi.it
Italia Oggi
Sette

Estratto da Pagina:
16

In un report i numeri del fenomeno che non si dirige più solo all'industria finanziaria

Phishing, le aziende abboccano

Truffe via e-mail più diffuse. Ma difendersi è possibile

Facciamo una prova? ;-)

<https://haveibeenpwned.com/>

Da tenere BEN presente



Come posso difendermi?

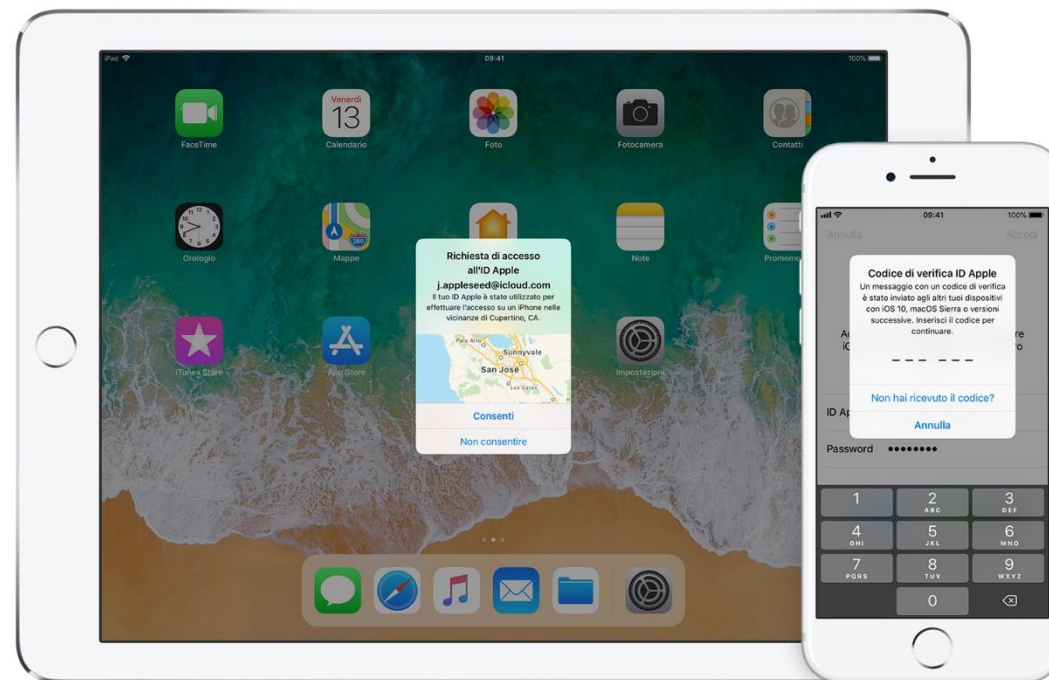
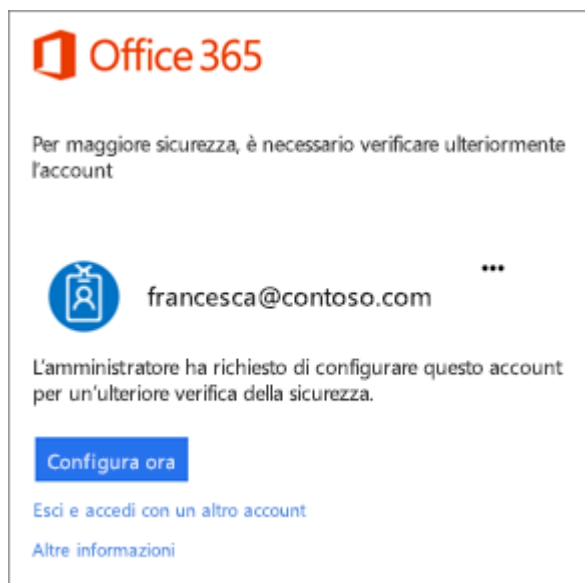
- Consapevolezza
- **Autenticazione a 2 fattori (MFA)**

Consapevolezza, un esempio

The screenshot displays the Office 365 Security and Compliance Center interface. The top navigation bar includes 'Office 365' and 'Sicurezza e conformità'. A left-hand sidebar lists various security and compliance tools: Home, Avvisi, Autorizzazioni, Classificazioni, Prevenzione della perdita dei dati, Governance dei dati, Gestione delle minacce, Ricerche e indagini, Report, and Garanzia del servizio. The main content area, titled 'Home', features several informational tiles. The 'Benvenuto in Centro sicurezza e conformità' tile includes a message about creating a resource for Office 365 security and compliance, with a 'Presentazione' button. The 'Gestione delle minacce' tile highlights the importance of data protection and offers links to 'Visualizza quarantena' and 'Nuovi criteri di filtro della posta indesiderata'. The 'Office 365 Secure Score' tile shows a score of 15 out of 364, with a description of the score's purpose and a 'Vai a Secure Score' link. The 'Governance dei dati' tile explains data ownership and provides links to 'Importa i dati in Office 365', 'Aggiungi criteri di conservazione', and 'Abilita spazio di archiviazione aggiuntivo'. Other tiles include 'Cerca utenti', 'Scelta consigliata', 'Cerca attività', 'Novità', and 'Importa i dati in Office 365'. The bottom of the dashboard includes a search bar for 'Ricerche e indagini' and a 'Garanzia del servizio' link.

Autenticazione a 2 fattori (MFA)

Autenticazione che si basa sull'utilizzo congiunto di due metodi di autenticazione individuale



Ricapitoliamo i vantaggi del Cloud..

- Riduzione dei costi per l'implementazione iniziale della infrastruttura
- Scalabilità garantita al crescere delle esigenze
- Indipendenza dalla locazione geografica dell'utente (Smart Working)
- Riduzione dei costi di gestione e manutenzione

E le criticità

- Potenziale minor controllo sui dati, essendo localizzati presso le strutture del provider (dove?)
- Dipendenza da terze parti (il provider)
- Sicurezza (sicurezza presso il provider, hijacking delle comunicazioni, sicurezza presso l'utente, affidabilità operatori, ...)
- Compliance normativa e contrattuale (GDPR)
- Contratto con il provider (gestione dei dati nel cloud, uptime e disponibilità, migrazione, assistenza, ...)
- Infrastruttura lato client (connessione sempre disponibile, veloce, affidabile, sicura)

Domande?



m.cecchini@t-consulting.it



@TeoCecchini / @TConsultingSrl



www.linkedin.com/in/matteo-cecchini