

DIRECTION

Reportec

LA DIGITAL ECONOMY AL SUPPORTO DEL BUSINESS



Cloud e Managed Service

Distribuito gratuitamente con "Il Sole 24 Ore"

OAD: Osservatorio Attacchi Digitali in Italia

L'OAD, Osservatorio Attacchi Digitali, è l'unica iniziativa in Italia per l'analisi sugli attacchi intenzionali ai sistemi informatici delle aziende e degli enti pubblici in Italia, basata sui dati raccolti attraverso un questionario compilabile anonimamente on line.

Obiettivo principale di OAD è fornire reali e concrete indicazioni sugli attacchi ai sistemi informatici che possano essere di riferimento nazionale, autorevole e indipendente, per la sicurezza ICT in Italia e per l'analisi dei rischi ICT. La disponibilità di un'indagine sugli attacchi digitali indipendente, autorevole e sistematicamente aggiornata (su base annuale) costituisce una indispensabile base per contestualizzare l'analisi dei rischi digitali, richiesta ora da numerose certificazioni e normative, ultima delle quali il nuovo regolamento europeo sulla privacy, GDPR.

La pubblicazione dei rapporti OAD aiutano in maniera concreta all'azione di sensibilizzazione sulla sicurezza digitale del personale a tutti i livelli, dai decisori di vertice agli utenti.

OAD è la continuazione del precedente OAI, Osservatorio Attacchi Informatici in Italia, che ha iniziato le indagini sugli attacchi digitali dal 2008. In occasione del decennale OAD, in termini di anni considerati nelle indagini sono state introdotte numerose innovazioni per l'iniziativa, che includono:

- sito ad hoc come punto di riferimento per OAD e come repository, anno per anno, di tutta la documentazione pubblicata sull'iniziativa OAD-OAI: <https://www.oadweb.it>
- visibilità di OAD nei principali social network: pagina facebook @OADweb, in LinkedIn il Gruppo OAD <https://www.linkedin.com/groups/3862308>
- realizzazione di webinar gratuiti sugli attacchi agli applicativi: il primo, sugli attacchi agli applicativi, è in <https://aipsi.thinkific.com/courses/attacchi-applicativi-italia>
- questionario OAD 2018 con chiara separazione tra che cosa si attacca rispetto alle tecniche di attacco, con nuove domande su attacchi a IoT, a sistemi di automazione industriale e a sistemi basati sulla block chain
- omaggio del numero di gennaio 2018 della rivista ISSA Journal e di un libro di Reportec sulla sicurezza digitale ai rispondenti al questionario OAD 2018
- ampliamento del bacino dei potenziali rispondenti al questionario con accordi di patrocinio con Associazioni ed Ordini di categoria, quali ad esempio il Consiglio Nazionale Forense con i vari Ordini degli Avvocati territoriali
- Reportec come nuovo Publisher e Media Partner
- collaborazione con Polizia Postale ed AgID.



4 Infrastrutture as a service e managed service guidano l'innovazione del business

7 La "magia" delle varie forme cloud rende flessibili le infrastrutture migliorando la governance aziendale

8 Il cloud pubblico è in crescita

9 Gartner: la metà delle offerte PaaS sono in cloud

10 I tre cloud a supporto del business

11 Il public cloud in Europa, una questione di spesa

12 Tutti pazzi per il cloud ibrido

14 Cloud First, not Cloud Only è la chiave per la trasformazione digitale

16 Libertà per la comunicazione aziendale col centralino cloud

18 Il cloud ibrido è la nuova frontiera dell'IT

20 Sogni tranquilli con i servizi gestiti

22 Cloud Managed Service Provider: soluzioni con un perché

24 Proteggere il cloud e il business aziendale

27 Cloud e sicurezza

28 La protezione dell'asset aziendale inizia dagli utenti privilegiati

Direttore responsabile: Gaetano Di Blasio
In redazione: Giuseppe Saccardi,
Gaetano Di Blasio, Paola Saccardi,
Edmondo Espa
Grafica: Airmone Bolliger
Le immagini delle copertine di questo numero sono di Irina Kharchenko ID 69725342 su Dreamstime.com

Redazione:
via Marco Aurelio, 8 - 20127 Milano
Tel 0236580441 - fax 0236580444

www.reportec.it
redazione@reportec.it

Stampa:
Media Print Srl, via Brenta 7,
37057, S.Giovanni Lupatoto (VR)

Editore: Reportec Srl, via Marco Aurelio 8,
20127 Milano

Il Sole 24 Ore non ha partecipato alla realizzazione di questo periodico e non ha responsabilità per il suo contenuto

Direction Reportec
anno XVI - numero 108

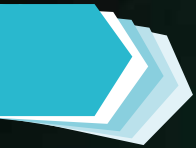
Presidente del C.d.A.: Giuseppe Saccardi
Iscrizione al tribunale di Milano
n° 212 del 31 marzo 2003
Diffusione (cartaceo ed elettronico)
50.000 copie
Tutti i diritti sono riservati;
Tutti i marchi sono registrati e di proprietà delle relative società.




**Infrastrutture as a service
e managed service
guidano l'innovazione
del business**



Applicazioni, software e servizi supportano le imprese nella trasformazione digitale, semplificando i processi aziendali e le operation





La "magia" delle varie forme cloud rende flessibili le infrastrutture migliorando la governance aziendale

Soluzioni as a service, sistemi software defined cambiano i modelli dell'ICT e aumentano la produttività

Il cloud pubblico è in crescita

Gartner prevede una crescita globale del Cloud Pubblico del 17,5% nel 2019. Entro la fine dell'anno oltre il 30% dei nuovi investimenti software dei fornitori di tecnologia passeranno dal 'cloud-first' a 'cloud-only'

Il mercato mondiale dei servizi cloud pubblici è previsto in crescita del 17,5% nel 2019 raggiungendo i 214,3 miliardi di dollari, contro i 182,4 miliardi del 2018, secondo le stime della società di analisi Gartner.

Il segmento di mercato in più rapida crescita sarà costituito dai servizi di infrastruttura del sistema cloud, o infrastruttura come servizio (IaaS), che si prevede aumenterà del 27,5% nel 2019 fino a raggiungere i 38,9 miliardi di dollari, da 30,5 miliardi di dollari nel 2018 (vedi Tabella 1). Il secondo tasso di crescita più alto pari al 21,8%

sarà raggiunto dai servizi di infrastruttura cloud applicativa o dal platform as a service (PaaS).

«I servizi cloud stanno decisamente scuotendo il settore - ha affermato Sid Nag, vicepresidente alla ricerca di Gartner -. In Gartner non conosciamo fornitori di servizi, oggi, i cui modelli di business e crescita dei ricavi non siano influenzati dalla crescente adozione di strategie 'cloud-first' nelle organizzazioni. Ciò che vediamo ora è solo l'inizio, però. Attraverso il 2022, Gartner prevede

una crescita del settore dei servizi cloud di quasi tre volte la crescita dei servizi IT complessivi. »

Secondo i recenti sondaggi di Gartner, più di un terzo delle organizzazioni considera gli investimenti nel cloud come una delle prime tre priorità di investimento, il che sta influenzando le offerte del mercato. Gartner prevede che entro la fine del 2019, oltre il 30% dei nuovi investimenti software dei fornitori di tecnologia passeranno dal 'cloud-first' a 'cloud-only'. Ciò significa che il consumo di software basato su licenze sarà ulteriormente ridotto, mentre SaaS e modelli di consumo di cloud basati su abbonamento continueranno a crescere.

«Le organizzazioni hanno bisogno di servizi legati al cloud per entrare a bordo di cloud pubblici e trasformare le loro operazioni mentre adottano servizi cloud pubblici», ha affermato Nag. Attualmente quasi il 19% dei budget sul cloud viene speso per servizi relativi al cloud, come consulenza cloud, implementazione, migrazione e servizi gestiti, e Gartner prevede che questa percentuale aumenterà fino al 28% entro il 2022.

«Finchè il cloud resta una tendenza principale nella maggior parte delle organizzazioni, i manager di prodotti

PREVISIONE DI RICAVI DEI SERVIZI DI PUBLIC CLOUD A LIVELLO GLOBALE (IN MILIARDI DI DOLLARI)
(fonte: Gartner Agosto 2018)

	2018	2019	2020	2021	2022
Cloud Business Process Services (Business Process as a Service)	45.8	49.3	53.1	57.0	61.1
Cloud Application Infrastructure Services (Platform as a Service)	15.6	19.0	23.0	27.5	31.8
Cloud Application Services (Software as a Service)	80.0	94.8	110.5	126.7	143.7
Cloud Management and Security Services	10.5	12.2	14.1	16.0	17.9
Cloud System Infrastructure Services (IaaS)	30.5	38.9	49.1	61.9	76.6
Total Market	182.4	214.3	249.8	289.1	331.2

Gartner: la metà delle offerte PaaS sono in cloud

Secondo la società americana di analisi quasi il 50% delle offerte PaaS sono cloud-only. Si prevede un spostamento degli investimenti strategici in questo settore

Secundo la società di ricerca Gartner, quasi la metà delle attuali offerte platform as a service (PaaS) sarebbero in cloud. Attualmente, ci sono più di 360 fornitori in 21 segmenti di mercato, che offrono più di 550 offerte PaaS. Il 48% percento di queste offerte sono 'cloud-only', come spiega Gartner. Nessun venditore ha un punto d'appoggio in tutti i 21 segmenti, il 90% di essi, invece, opera solo all'interno di un singolo segmento di mercato PaaS.

«I leader aziendali e tecnologici stanno spostando gli investimenti strategici nel cloud computing - ha affermato Yefim Natis, vicepresidente alla ricerca e analista di Gartner -. Il cloud computing è una delle principali forze dirompenti nei mercati IT che sta conquistando la fiducia principale. Sebbene molte organizzazioni

prevedano un ammortamento a lungo termine dell'infrastruttura on-premise, i fornitori di quasi la metà delle piattaforme cloud scommettono sulla crescita di quest'ultimo e scelgono il delivering solo in cloud» ha commentato Natis.

Pertanto Gartner prevede che

la spesa IT delle aziende per le offerte basate su cloud supererà la spesa per le offerte non in cloud entro il 2022. Si prevede che il fatturato totale del mercato PaaS raggiungerà i 20 miliardi di dollari nel 2019 e supererà i 34 miliardi di dollari nel 2022, secondo stime comunicate da Gartner.

In questo passaggio al cloud, i servizi di database e application platform rappresentano i segmenti di mercato più grandi, con blockchain, esperienza digitale, servizi di platform serverless e di intelligenza artificiale/machine learning (AI/ML) che si posizionano come i più innovativi.

Gli analisti di Gartner approfondiranno il tema dei servizi Cloud Platform e Key Cloud Computing in occasione dell'evento Gartner Enterprise Architecture & Technology Innovation Summit 2019, che si terrà il prossimo 3-4 giugno a Londra.

PASSAGGIO AL CLOUD PER CATEGORIA

(fonte: Gartner Agosto 2018)

	2018	2019	2020	2021	2022
System infrastructure	11%	13%	16%	19%	22%
Infrastructure software	13%	15%	17%	18%	20%
Application software	34%	36%	38%	39%	40%
Business process outsourcing	27%	28%	29%	29%	30%
TOTAL	19%	21%	24%	26%	28%



tecnologici per i servizi correlati al cloud dovranno concentrarsi sulla fornitura di soluzioni che combinino esperienza ed esecuzione con le offerte dei provider hypersclae», ha affermato Nag. «Questo approccio complementare guiderà sia la trasformazione che l'ottimizzazione dell'infrastruttura e delle operazioni di un'organizzazione».



I tre cloud a supporto del business

di
Gaetano
Di Blasio

In molti decidono di utilizzare le diverse tipologie di cloud, non sempre comprendendo le differenze che riguardano soprattutto la governance dei sistemi e la sicurezza

Fino a pochi anni fa era impensabile rinunciare a controllare la propria infrastruttura, se non scegliendo un fornitore in outsourcing, che ne prendeva la completa responsabilità.

Con il ricorso al public cloud, invece, quello che era il cuore del sistema informativo, cioè il centro dati, diventa un concetto sempre più astratto e composto da un'architettura eterogenea.

L'uso del cloud pubblico si è andato affermando, perché trasforma in opex, con un modello pay per use, il tradizionale acquisto di nuove infrastrutture, che impongono investimenti in capex.

La nuova flessibilità, comporta vantaggi, come la scalabilità e il time to market, reso possibile dalla flessibilità e dal modello

as a service o a noleggio. Nasconde tuttavia anche dei rischi. In particolare la scelta del provider deve garantire la riservatezza dei dati che girano su strutture condivise, senza penalizzare la scalabilità e gli altri vantaggi.

Il cloud privato rappresenta il "vecchio" modello on premise, cioè il mantenimento di una propria infrastruttura, che, rispetto al passato, risulta molto più flessibile, grazie alla virtualizzazione: le recenti tecnologie che consentono di astrarre l'uso delle infrastrutture dall'hardware, per gestire tutto molto più facilmente attraverso il software.

Tornando al tema della riservatezza e quindi della sicurezza dei dati, questo approccio

deve fare i conti con le soluzioni tipicamente di Software-Defined Networking (SDN), per la sicurezza della rete. Ci sono diverse soluzioni disponibili e occorrerà scegliere quella più idonea per il proprio caso. In generale la soluzione per la sicurezza che si sceglie, può essere distribuita facilmente in un ambiente cloud.

A questa si aggiunge la sicurezza che deve essere fornita dal provider, cioè le capacità di protezione delle strutture messe a disposizione dal fornitore dei servizi cloud.

Nella maggior parte dei casi quest'ultimo dispone di risorse maggiori rispetto a quelle della singola azienda.

Stiamo parlando delle cinque principali piattaforme di cloud pubblico, quali: AWS, Azure, Google, IBM e Oracle, ma lo stesso vale per altre come OVH e Aruba, senza poterle citare tutte. Si devono controllare le certificazioni, ovviamente, ma anche ricordare che i fornitori di servizi non sono tenuti a garantire la protezione di default: occorre fare molta attenzione agli SLA (Service Level Agreement), che ciascun provider propone di volta in volta. ❄



Il public cloud in Europa, una questione di spesa

di
Tito
Labanchi

Esperienze e aspettative con opportunità per l'Italia

Il cloud è subito stato visto come una panacea a tutti i mali dell'informatica aziendale, costretta da vincoli importanti che rallentavano l'innovazione per salvaguardare investimenti pregressi. La logica del "pay per use" ha rapidamente attecchito con la promessa di trasformare capex in opex.

L'uso "smodato" del cloud pubblico, però ha mostrato alcuni limiti, almeno stando alle conclusioni di una indagine svolta a livello Emea da Vanson Bourne.

Gli analisti hanno osservato che la maggior parte delle aziende a livello globale fatica a controllare la spesa nel cloud pubblico.

Fortunatamente, l'Italia risulta più virtuosa mediamente: il 36% degli intervistati a livello globale e il 40% degli intervistati

Emea hanno segnalato che le distribuzioni di servizi cloud pubblici superano i budget IT, anche se la limitata penetrazione del public cloud, potrebbe spiegare la differenza, peraltro è probabile che la cautela abbia prevalso come in passato. Si tratterà di trovare l'equilibrio tra spesa e innovazione.

Esaminando quanto i servizi di cloud pubblico abbiano soddisfatto le aspettative degli utenti, gli analisti di Vanson hanno concluso che le esperienze

in Italia sono in linea con quelle della regione Emea e delle grandi aziende in generale. Il 41% afferma, infatti, che i servizi di cloud pubblico hanno "completamente" soddisfatto le aspettative.

I vantaggi considerati più importanti riguardano specificatamente sicurezza e conformità, questo sia a livello globale, sia nelle diverse aree comprese nell'indagine.

In Emea è stata segnalata anche la scalabilità tra i massimi vantaggi. In Italia, inoltre, gli intervistati hanno classificato la sicurezza dei dati e la conformità come i principali vantaggi offerti dai servizi di cloud pubblico, aggiungendo al secondo posto il TCO come principale beneficio, tutto sommato in media con il resto del mondo

I maggiori benefici del cloud pubblico

Sorprende un po' che le imprese europee, soggette al GDPR, siano differiscano in merito all'importanza di sicurezza e conformità. Solo l'8% delle aziende dei Paesi Bassi e il 13% della Spagna hanno classificato la sicurezza al primo posto, rispetto al 27% in Italia e al 28% nel Regno Unito. Disparità

I maggiori benefici del cloud pubblico

Beneficio	Media globale	Emea	Italia
Sicurezza e conformità dei dati	21%	20%	27%
TCO ridotto	19%	16%	20%
Prestazioni	17%	17%	15%
Agilità	11%	13%	14%
Scalabilità	8%	20%	7%
Semplicità di gestione	7%	16%	7%
Flessibilità on-demand	6%	7%	1%

simili sono risultate evidenti anche in area APAC e Giappone, indicando che le imprese potrebbero non aver ben chiaro se la sicurezza e la conformità migliorino o peggiorino con il passaggio al cloud pubblico.

Cloud pubblico o cloud privato: come scegliere

I dipartimenti IT aziendali utilizzano svariati parametri per decidere quale infrastruttura utilizzare per le loro differenti applicazioni. Quando è stato chiesto alle aziende di elencare in base a quale fattore scelgano dove far girare le applicazioni, conformità e sicurezza sono risultati i fattori più citati a livello globale, in Emea e in Italia, seguiti dal costo. Gli intervistati italiani ritengono che l'agilità sia un elemento di scelta leggermente più determinante rispetto alle proprie controparti in Emea, in media, e un fattore nettamente più determinante rispetto alla media globale. ❁

Tutti pazzi per il cloud ibrido

di
Gaetano
Di Blasio

Secondo gli analisti di Vanson Bourne il modello IT che combina infrastrutture pubbliche e private è preferito dal 91% delle imprese

Una ricerca realizzata da Vanson Bourne ha determinato che l'infrastruttura cloud ideale per le imprese è quella ibrida, mentre il solo cloud pubblico non è in grado di garantire tutte le esigenze.

L'indagine, commissionata da Nutanix, ha coinvolto circa 2300 "technical decision maker", distribuiti in aziende d'ogni dimensione, presso aziende di diverse dimensioni e operanti in vari mercati in America, Europa, Medio Oriente, Africa, area Asia-Pacifico e Giappone.

Il rapporto ha esaminato i progetti relativi all'adozione del cloud privato, pubblico e ibrido, arrivando a sancire che le aziende prevedono di incrementare l'utilizzo del cloud ibrido nella misura del 91% (90% in Italia).

Al momento, secondo gli analisti, solo il 18% (24% in Italia) ha già adottato tale modello, ma la mobilità delle applicazioni su qualsiasi cloud risulta essere una priorità per il 97% (96% in Italia) degli intervistati e l'88% dei manager coinvolti, (86% in Italia) è convinto che il multcloud permetterebbe, almeno in parte, a risolvere molti dei problemi attuali.

Più in dettaglio, l'indagine rivela che il cloud pubblico non è una panacea, ma secondo gli intervistati la possibilità di utilizzare l'ambiente cloud corretto, per le varie applicazioni, è fondamentale. In particolare, il 35% (18% in Italia) delle aziende, che utilizza il cloud pubblico, ha speso più del budget annuale assegnato. Inoltre, l'importanza del cloud ibrido è stata così classificata:

1 l'interoperabilità tra diversi tipi di cloud (23% a livello globale, 29% in Italia);
2 la possibilità di spostare le applicazioni tra diversi cloud (16% globalmente, 10% in Italia);

3 il costo (6% sia a livello globale sia in Italia);
4 la sicurezza (5% globalmente, 9% in Italia).

Il cloud ibrido appare rispondere meglio alle esigenze aziendali rispetto al solo cloud pubblico, incluso il prezzo: l'87% (77% in Italia) degli intervistati ha affermato che il cloud ibrido, come trend IT, sta avendo effetti positivi sulle proprie aziende, mentre il 49% (42% in Italia) di quelli che usano cloud ibrido riportano che tutte le esigenze sono state soddisfatte rispetto al 37% degli utenti di un unico cloud pubblico.



Inoltre, le aziende che utilizzano il cloud pubblico spendono il 26% (24% in Italia) del loro budget IT annuale sul cloud pubblico.

Sorprende gli analisti che solo il 6% delle aziende le quali che utilizzano il cloud pubblico ha rispettato il budget, mentre il 35%, cioè quasi sei volte di più, l'ha superato. Come vedremo più avanti, per quanto riguarda i carichi di lavoro, la sicurezza rappresenta la priorità in quanto gli intervistati identificano la sicurezza dei dati e la conformità con le normative come i fattori principali per stabilire dove posizionare i propri carichi di lavoro.

Agilità e trasformazione

Uomini e donne dell'IT sanno che agilità e trasformazione digitale sono più che un concetto astratto, soprattutto perché gli ambienti di runtime dedicati alle applicazioni enterprise vivono un costante cambiamento.

Non è una sorpresa, dunque, che gli intervistati abbiano individuato la necessità di una maggiore orchestrazione e mobilità delle applicazioni in tutti gli ambienti cloud.

Infatti i team IT cercano la flessibilità per spostare le app sul cloud "giusto" in una maniera dinamica. Inoltre, sono consapevoli dei rischi della "shadow IT". Cosiddetta perché identifica le ombre rappresentate dalle pratiche IT non autorizzate, come, per esempio la sottoscrizione di un'applicazione as a service che espone i dati aziendali a una possibile perdita di riservatezza.

Gli analisti hanno rilevato che oltre la metà degli intervistati (57%) segnala uno o più incidenti legati alla shadow IT.

Le imprese italiane e il cloud del futuro

Sempre in base alle risposte raccolte dagli analisti di Vanson Bourne, le imprese italiane attualmente gestiscono meno carichi di lavoro nei data center tradizionali (24%) rispetto ai loro omologhi a livello globale (41%) ed EMEA (40%), inoltre sono anche coloro che impiegano più spesso i cloud privati e ibridi con una penetrazione rispettivamente del 49% (38% EMEA) e del 24% (17% EMEA).

Nei prossimi 12 o 24 mesi, le aziende italiane dovrebbero mantenere le attuali abitudini nell'utilizzo del cloud, cosicché l'impiego di data center tradizionali, sarà, con ogni probabilità, destinato a scendere ben al di sotto delle medie, a favore dell'utilizzo di servizi di cloud ibrido, privato e molteplici cloud pubblici. Più precisamente, gli analisti si attendono la seguente penetrazione dei diversi tipo di cloud presso le imprese del nostro Paese (risposte multiple): 48% ibrido, 20% privato, 20% pubblico. In questo mostrandosi in linea con le altre aree geografiche.

Attenzione alla sicurezza e alle competenze

Si è già notato che la sicurezza non è la priorità quando si parla di cloud ibrido. Anche gli incidenti, cui si è accennato relativamente allo shadow IT, lasciano intendere una scarsa attenzione

alla sicurezza informatica. Lo dimostrano pure le prassi per la realizzazione delle applicazioni. Infatti, stando all'indagine, il 57% degli sviluppatori elude l'IT (in Italia, fortunatamente solo il 30%).

Per contro, la sicurezza è l'elemento principale per stabilire i carichi di lavoro: il 71% (75% in Italia) degli intervistati riconosce la sicurezza dei dati e la conformità con le normative quali i fattori principali per stabilire dove posizionare i propri carichi di lavoro. Seguono le prestazioni con il 62% (stesso dato Italia), la semplicità di gestione al 53% e il costo al 52%.

Un'altra questione per la sicurezza è quella di trovare professionisti del settore. Più in generale sussiste la difficoltà nel reperire le competenze necessarie nella gestione dell'IT, anche a livello di esperti cloud manager. Gli analisti di Vanson Bourne segnalano che gli intervistati lamentano la fatica nel trovare personale qualificato per il modello IT ibrido: gli intervistati ritengono che la scarsità di esperti è un problema, con il 54% (34% in Italia) dei rispondenti che indica nella la fidelizzazione di tali professionisti esperti una componente del problema.

È un aspetto preoccupante, considerato che le previsioni degli analisti riportano una crescita delle esigenze.

In particolare, in EMEA l'adozione del cloud ibrido sarà superiore a quella delle Americhe, che sono partite prima, ma saranno sorpassate in Europa (+43%) e in Italia ancor di più, con un incremento previsto pari a 48%.



Cloud First, not Cloud Only è la chiave per la trasformazione digitale

La piattaforma cloud di Vem Sistemi raccoglie i parametri di produzione, calcola efficienza, OEE di produzione del singolo lotto, velocità, qualità, le cause di fermo e verifica la corrispondenza al piano impresa 4.0

Cloud e innovazione hanno molto in comune. Nella nuvola il ritmo con cui vengono ideati, sviluppati e rilasciati nuovi servizi è mozzafiato. Il tasso di innovazione interno alle principali organizzazioni che forniscono servizi di cloud pubblico è elevatissimo e questa onda di innovazione ne genera un'altra: quella di tutte le organizzazioni che, attraverso le tecnologie digitali, stanno cercando nuove strade per aumentare la propria competitività, cambiare il modello di business oppure individuare orizzonti completamente nuovi.

Queste aziende sempre di più trovano nel cloud la loro "cassetta degli attrezzi dell'innovazione". Semilavorati innovativi che abilitano nuovi servizi altrettanto innovativi. Innovazione che abilita innovazione.

È sfruttando queste leve che il gruppo Vem all'inizio del 2017 ha cominciato un percorso di Open Innovation che ha portato la società ad affrontare progetti digitali in una modalità del tutto nuova rispetto al passato.

Vem Sistemi è una società fondata a Forlì nel 1986 che si è sempre occupata di progettare e realizzare infrastrutture ICT come reti di comunicazione, data center, sistemi di sicurezza informatica.

Puntando su qualità e avanzati servizi di gestione delle soluzioni realizzate, Vem ha consolidato la sua posizione di mercato diventando un gruppo che oggi genera circa 50M di euro di fatturato, 250 dipendenti e sei sedi operative dislocate in tutto il centro e nord Italia.

La caratteristica di operare su infrastrutture come la rete o i sistemi computazionali, non aveva portato Vem a realizzare soluzioni ICT direttamente connesse al processo di business dei propri clienti fino al 2017, quando il neonato team di innovazione ha cominciato un percorso nuovo. Sposando i concetti della Open Innovation sono stati avviati una serie di progetti di esplorazione mettendo al centro il cliente, le sue esigenze ed il suo processo di business per comprendere come le tecnologie digitali potessero effettivamente aprire nuove opportunità.



Marco Bubani, direttore
innovazione di VEM
sistemi

Di seguito due esempi concreti di innovazione cloud illustrati da Marco Bubani, direttore innovazione di VEM sistemi.

Il cloud per la filiera alimentare

Un primo progetto è stato realizzato nella filiera alimentare, in particolare con un produttore di carni avicole e ci si è concentrati sull'area zoo-mangimistica, oggi scarsamente digitalizzata.

Dopo una serie di workshop condotti con tutti gli stakeholder del processo di allevamento sono stati individuati una serie di parametri fondamentali da monitorare per il benessere animale, che oggi vengono gestiti in maniera empirica dal singolo allevatore. L'obiettivo che ci si è posti è stato quello di raccogliere questi parametri in modo strutturato per poterli storicizzare, confrontare, ed analizzare in modo molto più profondo al fine di migliorare il processo di allevamento.

Fornire quindi a tutti gli attori che orbitano attorno al processo di allevamento uno strumento molto più flessibile e completo che li supporti e li agevoli nelle decisioni.

Il cloud è stato il veicolo per riuscire a realizzare una piattaforma IIoT in tempi brevi che potesse rispondere alle esigenze emerse dai workshop. Il team di Vem sfruttando tool e servizi resi disponibile dal public cloud ha creato una piattaforma composta sostanzialmente da due macro componenti: un modulo edge software di raccolta e prima elaborazione dati dal campo (da sensori e automazioni presenti o aggiunte in allevamento) e una componente cloud che riceve in modo sicuro dalla componente edge i dati raccolti e li archivia in modo nativo. La piattaforma consente quindi l'applicazione di algoritmi per l'individuazione di situazioni anomale o migliorative per il processo e la generazione di allarmi singoli

o correlati fra più grandezze. Il tutto è restituito agli stakeholder mediante dashboard web e app utilizzabili da smartphone.

È stato possibile realizzare questa piattaforma in tempi rapidi e con costi relativamente contenuti grazie al cloud. E sempre grazie al cloud, se il progetto si amplierà, sarà possibile scalare senza nessuna frizione e sarà possibile attingere a funzionalità di gestione ed elaborazione dati più avanzate come algoritmi di machine learning o computer vision in modo estremamente rapido ed efficace.

Il cloud per il packaging

Mutuando l'esperienza fatta con gli allevamenti e replicando la logica edge-cloud utilizzata, in un distretto industriale completamente diverso, è stata realizzata una piattaforma di raccolta dati delle macchine automatiche per un Machine Builder del settore packaging. Con questa piattaforma cloud il gruppo Vem attraverso la consociata MyDev, è in grado di raccogliere tutti i parametri di produzione generati dalla macchina, associarli al lotto di produzione e alla ricetta di macchina, e calcolare parametri di efficienza l'OEE di produzione del singolo lotto, la velocità e la qualità di produzione, le cause di fermo e molto altro, agevolando così la compatibilità della macchina al piano impresa 4.0.

Questi, ha osservato Bubani, sono solo due esempi di come il cloud è ormai elemento fondamentale per supportare e accelerare la trasformazione digitale. Cloud First, not Cloud Only, è la chiave. *

Chi è VEM sistemi

Da 33 anni VEM sistemi è uno degli ICT player italiani più innovativi e attento a intercettare le nuove tendenze del settore, rendendole funzionali alle esigenze dei clienti. Dalle sei sedi dislocate nei poli manifatturieri dove il "made in Italy" ha le sue radici - Forlì, Milano, Modena, Padova, Roma e Senigallia - offre servizi di integrazione delle tecnologie di networking basate su IP, con una visione olistica che va dalla cybersecurity, alla mobility, dalla collaboration, al data center, fino all'automazione dell'edificio e al custom application development del software, per consentire ai propri clienti di cogliere il meglio dalla tecnologia in completa sicurezza. <http://vem.com/>



Libertà per la comunicazione aziendale col centralino cloud

NFON propone una tariffa unica per utente che comprende tutti i servizi di centralino professionale anytime, anydevice e anywhere in Europa, sfruttando le moderne logiche cloud

NFON sbarca in Italia portando un approccio dirompente nel mercato della telefonia in cloud, superando il concetto di centralino o PBX e proponendo un modello economico lineare: una singola tariffa per utente (8,80 euro mese) con un numero unico sempre disponibile fino a nove dispositivi, fissi o mobili. Il modello cloud, in linea con le logiche as a service e pay per use, porta a una modernizzazione del vecchio sistema telefonico e, soprattutto, un significativo abbattimento del costo di possesso, evidenzia Marco Pasculli, Managing Director di NFON in Italia.

Si eliminano tutti i costi di manutenzione, che NFON gestisce in cloud, e si ottiene la flessibilità dei sistemi virtualizzati.

Altra semplificazione economica riguarda la tariffazione unica e stesse condizioni in tutta Europa. Per questo NFON si considera l'unico fornitore "paneuropeo".

L'azienda. Nata nel 2007, arriva nel nostro paese dopo una storia di successi, culminati con la quotazione presso la borsa di Francoforte nel listino Prime Standard avvenuta nel 2018, che ha permesso l'espansione e il lancio del nuovo prodotto di punta: Cloudya. L'ultimo anno ha portato i risultati attesi dagli investitori e si è concluso, rivela il Ceo Hans Szymanski, con un 21% di ricavi in più, un 27% di clienti in più e una crescita del 25% dei ricavi ricorrenti (su base mensile) che rappresentano circa l'80% dei ricavi totali. Il tutto per un fatturato di 43 milioni di euro.



Marco Pasculli, Managing Director di
NFON in Italia

Le soluzioni Premium

Pasculli evidenzia la vision strategica: «Vogliamo la libertà della comunicazione cioè: una sola tariffa, lo stesso piano per tutte le imprese europee, tutti i servizi inclusi e la possibilità di rescindere il contratto ogni mese».

Il cloud abilita questo modello, grazie a due data center in

Europa, geo-ridondanti e conformi alle normative internazionali, GDPR incluso.

Un modello di per sé aggressivo, cui si aggiunge la strategia di NFON che «non si limita alla vendita di telefonia a una qualsiasi azienda italiana, ma sviluppa soluzioni che svolgono un ruolo essenziale nella modernizzazione delle esigenze di comunicazione all'interno di interi comparti industriali», spiega Pasculli.

Nhospitality e Ncontactcenter e Neorecording sono alcune delle innovative soluzioni offerte da NFON; tre soluzioni definite "Premium", che rispondono direttamente alle esigenze di molte aziende italiane. Più in dettaglio, Nhospitality è pensata per soddisfare le esigenze di comunicazione delle strutture alberghiere: circa 33mila hotel e 22mila agriturismi in Italia, evidenzia il manager italiano. Strutture che devono rinnovarsi integrando nuovi servizi da "hotel 5 stelle", il tutto abbattendo i costi di gestione e manutenzione dei vecchi centralini per scegliere sistemi as a service semplici da utilizzare. Il risultato è una comunicazione aziendale moderna e flessibile, grazie alla quale ottimizzare i processi e ridurre i costi al minimo, sottolinea Pasculli.

Ncontactcenter, invece, permette alle tante imprese che raggiungono la clientela attraverso il telefono, di configurare le risorse in maniera dinamica, fronteggiando la scalabilità con un semplice clic per aumentare o diminuire il numero di operatori in base alle necessità e ai picchi di carico richiesti

in specifici periodi dell'anno. Neorecording, infine, soddisfa le esigenze delle aziende che vendono servizi e contratti al telefono attraverso la registrazione vocale del contratto.

Il servizio è conforme alle stringenti normative, sia tecniche sia legali, per la registrazione, fornendo capacità d'indicizzazione e archiviazione permanente in storage protetti.

Le opportunità della Unified Communication in cloud

Le potenzialità per NFON sono elevate in generale: secondo la società di ricerca MZA, i numeri di telefono in cloud erano 13 milioni nel 2017 e raddoppieranno entro il 2022. Inoltre, Marcus Kramer, Vice President of Product, New Business & M&A di NFON, sottolinea: «In Europa ci sono 439 milioni di abitanti, 135 milioni di telefoni fissi, 143 milioni di dipendenti nelle piccole e medie imprese e altri 67 milioni nelle medie e grandi aziende. Numeri impressionanti che si abbinano a un momento di trasformazione del mercato che va in direzione del cloud, mentre il tasso di adozione del centralino in cloud in Italia è ancora molto basso». Szymanski, inoltre, sottolinea quanto il modello cloud, molto diffuso in Germania, si stia affermando come strumento d'innovazione, che permette, in particolare, di adottare un'architettura innovativa.

Più in dettaglio, il modello di NFON prevede l'assegnazione di un numero d'interno a ciascun utente, ma non c'è la connessione fisica

al centralino, poiché il Cloud PBX virtualizza il collegamento. Il numero è una sorta di identificativo, al quale possono essere abbinati, come accennato, fino a 9 nove dispositivi, attivabili dall'utente. Per esempio, spiega Szymanski, «posso indirizzare le chiamate che arrivano al fisso sulla scrivania in ufficio verso il cellulare, quando sono in vacanza e nessuno potrà accorgersi che non sto rispondendo dall'ufficio, ...ammesso, che sia una buona idea "portarsi" il telefono aziendale in vacanza».

Cloudya: anytime, anywhere, any device

La soluzione plug and play Cloudya adotta il tipico approccio delle applicazioni in cloud: semplicità tipo plug and play, in qualsiasi luogo, momento e con ogni dispositivo, che sia facile da gestire, affidabile e sicura, come precisa Kramer: «Sono queste le caratteristiche che il cloud PBX deve garantire, permettendo di scalare senza problemi: per esempio aggiungendo linee con un semplice clic on demand per fronteggiare le attività di picco, per poi eliminare i numeri aggiunti appena terminano di servire». Il provisioning è automatico, il che consente un'installazione immediata, evidenzia ancora Kramer, che ci mostra, in una demo, il rapido accesso alle funzioni di Unified Communication e il facile utilizzo di Cloudya.

Questa, tra l'altro, permette di configurare softphone per Android, Windows e Apple, su browser Google Chrome, Safari, Mozilla Firefox.



Il cloud ibrido è la nuova frontiera dell'IT

di
Giuseppe
Saccardi

Le soluzioni Nutanix per il cloud ibrido facilitano il passaggio al cloud, rimuovono gli ostacoli per la gestione, abilitano la mobilità e migliorano i costi aziendali

Che lo si ami o lo si detesti, il cloud sta avendo un grande impatto sull'IT in azienda. Questa è la sensazione, ma per rendersene pienamente conto di quanto sia forte il suo effetto basta analizzare i risultati di una ricerca su ciò che sta accadendo nel mercato dell'enterprise cloud.

Condotto da Vanson Bourne per conto di Nutanix, lo studio ha raccolto dati molto interessanti da circa 2.300 aziende di tutto il mondo. I risultati sono espliciti: oltre un terzo (36%) dei workload aziendali è già in cloud e la maggior parte delle aziende intervistate si aspetta che questo dato cresca rapidamente per arrivare ad oltre la metà dei workload in cloud entro l'ormai prossimo 2020.

L'approccio ragionato al cloud ibrido

Le aziende stanno sperimentando i benefici del cloud pubblico (scalabilità on-demand, risparmio grazie a un approccio pay per use e così via) e, allo stesso tempo, sono consapevoli del fatto che non tutti i cloud sono uguali. Di conseguenza, scelgono il luogo migliore per ogni applicazione che distribuiscono, sia esso un cloud pubblico o privato, invece che uniformarsi a un unico cloud e adattarvi le applicazioni.



Alberto Filisetti, Country Manager di Nutanix Italia

Purtroppo, evidenzia Alberto Filisetti, Country Manager di Nutanix Italia, si è ben lontani dall'essere in grado di trasformare l'aspirazione ad una libera circolazione delle applicazioni.

Innanzitutto perché non tutti i cloud sono uguali e a questa constatazione se ne aggiunge un'altra emersa dallo studio condotto da Vanson Bourne: una reale mancanza di personale con le competenze necessarie per concretizzare tale ambizione.

Il risultato è una mancanza di visibilità nel momento in cui le applicazioni vengono distribuite su un mix ibrido di cloud. E se a tale mix si aggiunge un'infrastruttura tradizionale on-premise, diventa ancora più difficile avere visibilità su cosa stia succedendo non solo in termini di

prestazioni e disponibilità, ma anche di sicurezza e conformità.

Gestire il cloud ibrido

È evidente che qualcosa andava fatto e, in questo senso, ci sono tecnologie e soluzioni in fase di sviluppo in grado di fornire l'auspicata visibilità tra i cloud. Tre funzionalità, osserva Filisetti, sono particolarmente utili:

- Strumenti di analisi avanzata in grado di comprendere le peculiarità tecniche, finanziarie e di governance dei cloud pubblici per permettere ai team IT di scegliere la "sistemazione" migliore per le proprie applicazioni.
- Servizi di disaster recovery (DR) in cloud per proteggere le applicazioni e i dati aziendali critici.
- Strumenti e tecnologie di rete cross-cloud in grado di gestire la connessione tra applicazioni attraverso cloud, istanze di servizi e prodotti di vendor diversi, nonché di identificare colli di bottiglia e potenziali vulnerabilità e avviare iniziative correttive.

«La distribuzione di questi e altri strumenti di gestione del cloud ibrido sarà tutt'altro che semplice e richiederà una maggiore cooperazione tra i vendor cloud e i service provider. Tuttavia, a fronte di un crescente numero di aziende che sta passando a un modello ibrido, è nell'interesse di tutti lavorare in sinergia. E' giunto il momento di unificare i cloud e fornire la visibilità, le tecnologie e gli strumenti necessari per sfruttare al meglio questa interessante modalità di fornire e gestire l'IT enterprise» ha osservato Filisetti.

La situazione del cloud in Italia

Se quella descritta è la situazione emersa in EMEA su un campione di 900 aziende in 9 nazioni, come si presenta il cloud in Italia? Tutto sommato mostra un concreto dinamismo in quanto l'Italia ha superato la media su un certo numero di punti, in particolare per quanto riguarda l'ubicazione della maggior parte dei carichi di lavoro, che sono oggi molto inferiori nei data center tradizionali rispetto alla maggior parte degli altri Paesi e molto di più in cloud privati e ibridi.

Rispetto ai suoi omologhi a livello globale e regionale in EMEA, l'Italia gestisce attualmente un numero significativamente inferiore di carichi di lavoro nei data center tradizionali (24%), significativamente maggiore nei cloud privati (49%) e ibridi (24%), e notevolmente inferiore in molteplici cloud pubblici (3%).

Se poi le aziende italiane seguiranno i piani indicati, il loro utilizzo dei data center tradizionali scenderà ben al di sotto delle medie, mentre il loro utilizzo di servizi di cloud ibrido, privato e pubblici supererà moderatamente le medie.

Dall'analisi emerge poi che si assisterà ad un marcato spostamento dell'Italia dai tradizionali data center in 12 - 24 mesi, quando l'utilizzo diminuirà di tre volte.

I cloud ibridi e l'utilizzo di più cloud pubblici prenderanno il sopravvento, dato che l'uso del cloud ibrido in Italia raddoppierà e l'utilizzo del multicloud aumenterà più di sette volte nello stesso periodo.



Questo a scapito del ricorso al cloud privato e di un singolo cloud, che diminuirà della metà o più.

L'esigenza di ecosistemi per il cloud ibrido

La complessità nell'approntare una soluzione ibrida che soddisfi le varie esigenze, da quelle economiche a quelle applicative, non può che essere affrontata con un forte connubio, osserva Filisetti, tra le aziende fornitrici di soluzioni cloud.

Un esempio è quello tra Nutanix e Hewlett Packard Enterprise (HPE), che hanno dato il via a una collaborazione globale volta a fornire una soluzione integrata di cloud ibrido as a Service (aaS).

La soluzione si basa sul software Nutanix Enterprise Cloud OS e il suo hypervisor AHV integrato e gratuito, reso disponibile tramite HPE GreenLake.

L'approccio permette alle aziende di poter disporre di un cloud ibrido che può essere gestito in toto da HPE, ridurre in modo significativo il TCO e assicurare un time to value più rapido.



A woman in a white, ethereal dress is shown floating in a dark space filled with stars and nebulae. The scene is dreamlike and serene, with the woman's body appearing to be in a state of peaceful suspension. The background is a deep blue and black, dotted with numerous small white stars and larger, glowing blue nebulae.

Sogni tranquilli con i servizi gestiti

Affidarsi a professionisti esperti specializzati permette di concentrarsi sul proprio core business, creando una partnership con il fornitore



Cloud Managed Service Provider: soluzioni con un perché

Achab propone servizi che consentono agli MSP di applicare un approccio progettuale focalizzato sul business del cliente

Si parla ormai moltissimo di servizi cloud. Per un managed service provider (MSP) si tratta semplicemente di una modalità di delivery di un servizio gestito con un canone ricorrente. La scelta di utilizzare il cloud dipende da una serie di condizioni inevitabilmente legate all'esigenza del cliente. L'MSP dovrà fissare una metrica per valutare che il grado di servizio erogato rientri negli obblighi contrattuali. «All'utente finale non deve interessare se sarà utilizzato il cloud o meno», sottolinea Andrea Veca, amministratore delegato di Achab.

All'inizio, ricorda l'AD, c'è stata molta confusione in merito a ciò che il cloud avrebbe determinato e, complice la scarsa conoscenza, l'atteggiamento attorno a questa innovazione era stato di diffidenza. In seguito si sono compresi i vantaggi, ed il cloud è stato percepito come la panacea per tutte le criticità dell'informatica, ovvero come uno strumento di semplificazione totale delle attività che quasi rendeva inutile il fornitore di servizi. Attualmente siamo giunti alla presa d'atto che una gestione del servizio da parte di un fornitore competente è necessaria. Anche sul fronte infrastrutturale si è passati dalla diffidenza all'euforia, ma la realtà è che occorre valutare le necessità aziendali nel loro complesso.

Per esempio, ci sono molte applicazioni che possono essere fruite as a service sul cloud, come la posta elettronica, ma per garantire la sicurezza e un servizio affidabile non basta fidarsi della singola applicazione.

Un approccio progettuale

Per esempio, afferma il Ceo di Achab: «Nessuno si preoccupa di effettuare il backup della posta, fin quando non emerge un problema. Allo stesso modo nessuno aggiorna gli antivirus o altre soluzioni di sicurezza se non dopo che si verifica una violazione.

In sintesi, Veca sottolinea che, a prescindere dalla modalità di messa in esercizio di un servizio, questo deve essere gestito in maniera oculata e completa, sia on premise o in cloud sia gestito internamente o da un fornitore.

Ovviamente gli oneri possono essere demandati o condivisi (come nel caso di un'applicazione fornita as a service, da un cloud provider che si prende carico



Andrea Veca, Ceo di Achab

degli aggiornamenti e del costantemente corretto funzionamento). Al contrario un sito realizzato con Wordpress da un neofita, il quale non esegue i continui aggiornamenti è pericolosamente insicuro. Potrebbe essere necessario, dunque prevedere un processo di gestione delle applicazioni, anche in cloud, oppure è necessario affidarsi a un cloud managed service provider che inserisce l'aggiornamento delle vulnerabilità nell'insieme di tutte quelle operazioni che servono per garantire il funzionamento di ogni applicazione. In questo contesto, chiediamo a Veca di illustrarci quali problematiche vanno affrontate per prime: «L'attenzione maggiore deve concentrarsi sulla "governance dell'intero sistema". Ci sono diversi tipi di cloud e una porzione di risorse che restano on premise, quindi sia le imprese sia i loro fornitori, in pratica tutti coloro che garantiscono il funzionamento dell'infrastruttura, devono applicare un approccio progettuale focalizzato sul business del cliente.

Dopo di che vanno gestite conseguenze operative, come la sicurezza, la conformità alle normative, la protezione dei dati eccetera. Il tutto avendo chiaro qual è l'esigenza del cliente.

La prassi, purtroppo, è occuparsi delle singole attività. In sostanza facendo manutenzione, senza una visione olistica. Manca una regia da parte di qualcuno che abbia ben chiaro gli obiettivi del business e abbia un portafoglio da investire. Il regista potrebbe essere il CIO, che magari siede anche

nel consiglio d'amministrazione. Potrebbe anche essere un facente funzioni, non necessariamente tecnico, se ben supportato da partner e fornitori.

Achab propone un portfolio di prodotti coerenti per realizzare un insieme di servizi da offrire alle imprese. «Prodotti che hanno un perché», chiosa Veca, presentando tre soluzioni innovative.

Datto SaaS Protection: La posta al sicuro

Datto SaaS Protection è una soluzione di backup cloud to cloud. Necessaria, per esempio, per proteggere la posta con il backup. Infatti, il servizio e-mail, che ormai la maggioranza delle imprese ha in cloud, non fornisce il backup: «né Microsoft né Google lo fanno», afferma Veca, mentre Datto SaaS prende i dati relativi alla e-mail che sono presso il provider di posta e li salva su un proprio spazio cloud, in genere gestito da un fornitore o direttamente dall'utente finale. Quest'ultimo, sgravato dall'onere di gestire l'applicazione, si può concentrare sulla protezione dei dati relativi alla posta o su quelli di altri servizi di cui è opportuno avere il backup.

Beachhead: la crittografia senza pensieri

Un'altra soluzione che ha un perché serve a crittografare i dati che si trovano sui dispositivi mobili. Di fatto un pc portatile, un tablet o uno smartphone sono un libro aperto per un esperto informatico. Perdere un device, mette a rischio tutte le informazioni sui propri

clienti che un avvocato, un medico o un altro professionista possiede. I produttori dei dispositivi non forniscono una soluzione per la complessità nella manutenzione delle chiavi di cifratura.

Grazie alla soluzione di crittografia sicura Beachhead, i fornitori che supportano le aziende possono facilmente realizzare un servizio gestito, perché Beachhead, disponibile as a service, amministra in cloud lo scambio delle chiavi e mette a disposizione delle aziende di supporto informatico, uno strumento per erogare un servizio gestito.

La rete sotto controllo

Infine, un'altra soluzione che consente di semplificare le complessità per realizzare servizi gestiti e accrescere affidabilità e sicurezza delle infrastrutture, sempre con lo scopo di supportare il business, è Auvik.

Si tratta di una soluzione per il monitoraggio e la gestione della rete. La connettività è data per scontata, ma non bisogna mai dimenticare che si tratta dell'elemento fondante di tutto il sistema, eppure la sua manutenzione è trascurata, salvo quando si presentano problemi e la rete si blocca o fornisce prestazioni ridotte. Il tutto mentre, con la crescita dell'Internet delle cose e dell'industry 4.0, il traffico aumenta vertiginosamente.

Quando si sottoscrive un servizio gestito, l'impresa si aspetta che funzioni, ma se il problema è nella rete? Auvik permette ai MSP di far funzionare la rete senza mal di testa.





Proteggere il cloud e il business aziendale

La sicurezza dei dati e degli
accessi è critica nell'era della
connettività pervasiva





Questa volta
siamo noi
a chiedere aiuto
a voi.

Fai un'offerta per una nuova ambulanza.

Servizio emergenza/urgenza 118 - auto medica - trasporto ammalati - trasporto organi - corsi di formazione di primo soccorso per aziende e per la popolazione - stazionamento ad eventi di massa - spettacoli e manifestazioni sportive - 37 sezioni in tutta la Lombardia - 100 anni storia.
Questo è quello che possiamo offrirti, tutti i giorni 365 giorni all'anno. Adesso tocca a te.

DONACI IL TUO 5 x mille: C.F. 03428670156, oppure puoi fare una donazione detraibile
(IBAN It43u0326801603000866949890)

Visita www.crocebianca.org e scoprirai come poterci aiutare.

Cloud e sicurezza

di
Gaetano
Di Blasio

Un divario da colmare grazie a fiducia e assunzione di responsabilità

La cultura della sicurezza è ancora troppo poco diffusa, nonostante si senta parlare di attacchi informatici in televisione e sui media con regolare frequenza.

Il trend registrato dagli esperti del Clusit, presentato con l'annuale Rapporto mostra una curva di crescita senza sosta degli attacchi considerati significativi (tra quelli noti). Nel 2018, in particolare, si è manifestato un picco di attacchi con un più 38%.

Addirittura gli attacchi considerati gravi sono saliti del 99%. Tra i settori più colpiti la sanità.

Il fattore gravità è ovviamente elevato per i potenziali rischi alla salute dei pazienti, ancor più che per le possibili violazioni a dati riservati e sensibili quali quelli trattati in questo settore.

La crescita dell'IoT e, più in generale il diffondersi di sistemi connessi in ogni ambito, dalle imprese alle case e così via, solleva il timore di poter arrivare a causare incidenti che passano dal piano virtuale del dark Web a quello fisico della vita reale in cui si espande l'uso del digitale.

Il Cybercrime resta la principale causa di attacchi gravi: il 79% di questi è stato infatti



compiuto allo estorcere denaro alle vittime, o per sottrarre informazioni da rivendere e ricavarne denaro (+44% rispetto ai dodici mesi precedenti).

Aumenta l'attività di spionaggio cyber, comprese azioni di spionaggio indirizzate alla politica o all'industria, che hanno registrato un più 57% nel loro complesso, comprendendo anche il furto di proprietà intellettuale.

La sfida, considerando la crescita dell'intelligenza artificiale consiste nel realizzare progetti, soluzioni, sistemi che siano "trustworthy", cioè sicuri e affidabili. Il problema, però, è che non è semplice definire cosa sia affidabile.

Per questo anche nel cloud occorre indicare un percorso di controllo che parta dalla consapevolezza che il cloud è in continuo divenire.

Daniele Cateddu, CTO della Cloud Security Alliance pone la questione "fiducia", che, sostiene l'esperto deve basarsi sulle "prove". In altre parole, ciascuno ha una propria percezione di fiducia, ma deve applicare le regole predefinite per verificare che ci siano i presupposti perché il sistema sia "trusted", però, la fiducia è necessaria, ma ancor di più lo è l'accountability: l'assunzione di responsabilità da parte di ciascun attore nella catena del valore in un modello condiviso. ❁

La protezione dell'asset aziendale inizia dagli utenti privilegiati

Le soluzioni di CyberArk per la sicurezza degli accessi privilegiati garantiscono l'individuazione e la protezione continua dai rischi nel cloud

CyperArk, società leader a livello mondiale nello sviluppo di soluzioni per la sicurezza degli accessi privilegiati degli utenti umani e non-umani, ha annunciato l'espansione delle sue soluzioni con nuove funzionalità volte a semplificare l'individuazione dei rischi e ad assicurare in ambienti cloud la protezione continua degli accessi privilegiati.

In particolare, l'ultima release (la v10.8) della soluzione "Privileged Access Security" di CyberArk, evidenzia la società, è la prima nel suo genere per quanto concerne l'automazione del processo di individuazione di rischi, di alert e di risposta ai rischi per account Amazon Web Services (AWS) non gestiti e potenzialmente a rischio.

La versione dispone in particolare di nuove funzionalità Just-in-time che sono volte a garantire un accesso flessibile per l'utente ai sistemi Windows, sia che questi siano basati su cloud sia di tipo on-premise.

In pratica, con la nuova release di Privileged Access Security Solution, l'azienda si è proposta di definire un vero e proprio nuovo standard e di abilitare un approccio ampiamente esaustivo e al top del settore per quanto concerne la sicurezza e l'efficienza operativa che deve essere garantita nel cloud.

L'obiettivo postosi da CyberArk è stato perseguito tramite funzionalità che permettono:

- **Identificazione continua degli account privilegiati:** identifica gli account privilegiati in AWS, come gli utenti IAM (Identity and Access Management) non gestiti, e le istanze e gli account EC2. Le organizzazioni possono, in pratica, tracciare le credenziali di AWS ovunque siano create e indipendentemente da come sono create, e accelerare il processo di on-boarding degli account non gestiti.
- **Rilevazione e risposta automatica agli exploit:** permette di inviare avvisi prioritari inerenti comportamenti potenzialmente rischiosi, quali per esempio attività che bypassano il vaulting, il furto della chiave di accesso o un'inadeguata gestione. La soluzione di CyberArk è anche in grado di assumere il controllo su questi account e attivare una nuova chiave di accesso o una sua rotazione automatica per mitigare il rischio.



- **Installazione semplificata in ambienti AWS:** estende le funzionalità già esistenti per la protezione dell'infrastruttura cloud. Diventa possibile, per esempio, semplificare l'implementazione di CyberArk Privileged Access Security Solution in AWS con AMI per tutti i componenti principali, inclusi il vaulting, la gestione delle sessioni e l'analisi delle minacce.
- **Accesso just-in-time con opzioni di provisioning flessibili:** permette all'amministratore di configurare la durata concessa

per l'accesso ai sistemi Windows, sia che si tratti di cloud sia di apparati on-premise. L'obiettivo è di consentire alle organizzazioni di ridurre in modo significativo la problematica operativa per gli end-user e mitigare il rischio costituito da un accesso privilegiato senza restrizioni. La nuova versione estende, ha spiegato CyberArk, la propria leadership tecnologica con una gamma molto ampia di opzioni utili nell'implementare e nel rafforzare i controlli sugli accessi privilegiati, dagli account protetti tramite

accesso Just-in-time a quelli completamente gestiti tramite audit, sia on-premise sia nel cloud.

Le soluzioni CyberArk posizionate al top dagli analisti

La conferma più diretta che le soluzioni di CyberArk rispondono a reali e sempre più diffuse esigenze aziendali viene dalle società di ricerca e analisi di mercato presso gli utenti finali. La società è stata di recente nominata leader assoluto per la gestione degli accessi privilegiati per il

quarto anno consecutivo da parte di KuppingerCole Analysts nel suo rapporto per il 2019 “Leadership Compass: Privileged Access Management”.

Il rapporto della società di analisi indipendente fornisce un’analisi dettagliata del mercato relativa alla gestione degli accessi privilegiati e si propone di essere di ausilio per i responsabili della sicurezza e dell’Identity & Access Management (IAM) nell’identificare le soluzioni che hanno il maggiore impatto positivo sui loro programmi di sicurezza informatica. CyberArk risulta essere il fornitore preferito per le organizzazioni globali che cercano una soluzione di gestione degli accessi privilegiati e leader del mercato per requisiti complessi.

Delle 20 società valutate nel report, solo CyberArk, ha notato la società, è stata riconosciuta come leader in tutti i segmenti a motivo del suo “focus sulla costante

innovazione” ed è stata identificata come “il più importante fornitore” sul mercato.

In particolare, tra le venti società analizzate, la soluzione per la sicurezza degli accessi privilegiati di CyberArk ha ricevuto il punteggio più alto possibile in tutte le categorie di valutazione del prodotto ed è stata riconosciuta per la qualità della sua progettazione per quanto concerne l’intuitività e la robustezza dell’interfaccia utente; l’efficacia del supporto DevOps e l’ampio supporto per quanto riguarda applicazioni e infrastrutture cloud.

CyberArk è stata posizionata tra i leader nel Privileged Identity Management anche in una ricerca indipendente realizzata dalla società di analisi Forrester Research nel suo “The Forrester Wave: Privileged Identity Management, Q4 2018”, un report che ha analizzato gli 11 fornitori più quotati del settore, tra i quali, ha evidenziato la

società, CyberArk è stata riconosciuta leader.

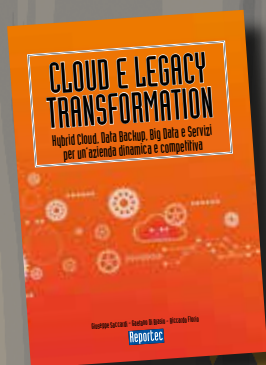
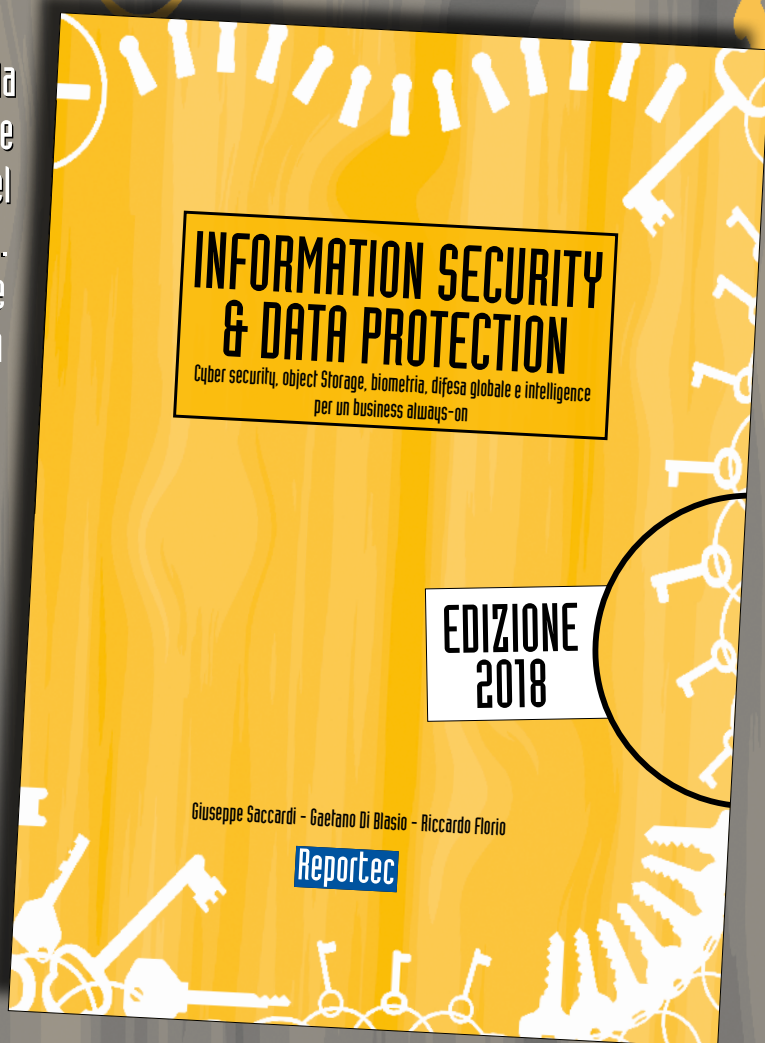
Il report è di alto valore per le organizzazioni globali che necessitano di una guida che li aiuti nel decidere cosa acquistare e le supporti nel definire la loro strategia per quanto concerne gli account privilegiati on premise o nel cloud. L’importanza della scelta della corretta strategia e dei relativi prodotti è strettamente dipendente dal fatto che a seguito dei crescenti investimenti effettuati nella migrazione al cloud, nel DevOps e nell’Internet of Things (IoT), nonché in altre aree emergenti a livello industriale come la automazione basata su processi robotici, la superficie di attacco si sta espandendo esponenzialmente.

In questo complesso e variegato processo di digitalizzazione, la gestione oculata e sicura delle identità privilegiate, mette in guardia CyberArk, diventa cruciale al fine di rafforzare la postura aziendale e organizzativa per la sicurezza e migliorare la gestione del rischio. Secondo il report, CyberArk dispone di una gestione delle password sicura, di gestione delle sessioni, di analitiche privilegiate dei rischi, nonché del più ampio supporto DevOps di qualsiasi altro dei produttori valutati da Forrester Wave. In particolare, osserva l’azienda, CyberArk si posiziona al top nelle categorie quali il portfolio di soluzioni e la presenza sul mercato e ha ottenuto il massimo punteggio possibile, tra altre voci, per quanto concerne la customer satisfaction, il cloud, il supporto DevOps e dei Container. ❁



È disponibile il nuovo libro **SICUREZZA E PROTEZIONE DEI DATI**

In oltre 200 pagine il punto sulla situazione della cybersecurity e sulle dinamiche aziendali nella protezione del dato e della continuità del business. Una tematica sempre più vitale per le imprese, le quali devono mettere in conto che saranno attaccate. Ormai esistono sistemi automatici e pressioni da parte dei cybercriminali, tali per cui nessuno può sentirsi al sicuro: chi non è ancora stato attaccato lo sarà e, se non subirà danni gravi, sarà solo perché chi l'ha assalito cercava qualcos'altro.



È disponibili anche
CLOUD E LEGACY TRANSFORMATION

Il libro è acquistabile al prezzo di 30 euro (IVA inclusa) richiedendolo a
info@reportec.it - tel 02 36580441 - fax 02 36580444

Fujitsu consiglia Windows 10 Pro.

FUJITSU

shaping tomorrow with you

Affidabile,
potente
e leggero

FUJITSU Notebook
LIFEBOOK U938



Sottile e ultra-mobile.
Il notebook Fujitsu LIFEBOOK U938 è per i
professionisti che desiderano il meglio, ovunque.

Windows 10 Pro | Intel® Core™ i7-8650U | 20 GB RAM

Info: www.fujitsu.com/it/ultrabook | Numero verde: 800 466 820
customerinfo.point@ts.fujitsu.com | blog.it.fujitsu.com

© Copyright 2019 Fujitsu Technology Solutions GmbH

Fujitsu, il logo Fujitsu e i marchi Fujitsu sono marchi di fabbrica o marchi registrati di Fujitsu Limited in Giappone e in altri paesi. Altri nomi di società, prodotti e servizi possono essere marchi di fabbrica o marchi registrati dei rispettivi proprietari e il loro uso da parte di terzi per scopi propri può violare i diritti di detti proprietari. I dati tecnici sono soggetti a modifica e la consegna è soggetta a disponibilità. Si esclude qualsiasi responsabilità sulla completezza, l'attualità o la correttezza di dati e illustrazioni. Le denominazioni possono essere marchi e / o diritti d'autore del rispettivo produttore, e il loro utilizzo da parte di terzi per scopi propri può violare i diritti di detto proprietario. Schermate simulate, soggette a modifica. App Windows Store vendute separatamente. La disponibilità di app e l'esperienza possono variare in base al mercato.

 Windows 10

Windows 10 Pro è sinonimo di business.