Cloud & Business

n.68
Febbraio 2018

LA RIVISTA PER IL MANAGER CHE DEVE OTTIMIZZARE COSTI E PROCESSI

IN QUESTO NUMERO

PAG 01-03
- Con OVH l'era del Cloud ibrido e aperto diventa realtà

PAG 05-12
- Il data center cambia e va nel cloud

PAG 13
-Veeam Backup for Microsoft Office 365 sempre più richiesto

PAG 14
- Con A10 Networks una protezione DDoS basata su cloud

PAG 15
- Da Canon una gestione documentale in cloud e sicura

PAG 17
- Cloud Platform semplifica lo sviluppo di app e accelera l'innovazione

PAG 18
- Con Vertiv l'energia per la rete diventa un servizio ESaaS

PAG 19
- Red Hat al top dei gradimenti per il cloud pubblico

PAG 20-21
- Si afferma sempre più la digital transformation

PAG 22-23
- Il GDPR è alle porte, ultimi avvisi

COVER STORY

CON OVH L'ERA DEL CLOUD IBRIDO E APERTO DIVENTA REALTÀ

Una rete di data center mondiale e connessioni ad alta capacità permettono di realizzare un cloud ibrido aperto per un IT sicuro e compliant con il GDPR

Con il cloud si è quasi universalmente affermato il paradigma di fruizione dell'IT come servizio, esternalizzandone la complessità affidandola a un service provider.

Dal cloud pubblico o privato si è approdati al cloud ibrido, un approccio che permette alle aziende di mantenere il controllo diretto di risorse e applicazioni critiche continuando a fruire del cloud pubblico per quanto concerne un'ampia porzione delle proprie applicazioni ed esigenze infrastrutturali.

Accettato ormai come concetto, per trasformarsi da idea a realtà concreta un cloud ibrido richiede un partner che possa rispondere a esigenze di globalizzazione, ampiezza di servizi, sicurezza, presenza territoriale e capacità di integrazio-

Dionigi Faccenda di OVH

Reportec Cloud&Business - Numero 68 - Febbraio 2018 - Registrazione al tribunale n°574 del 5 Novembre 2010 - Tutti i marchi sono di proprietà delle relative società- Editore: Reportec Srl (www.reportec.it) - Direttore responsabile: Giuseppe Saccardi - In redazione: Gaetano Di Blasio - Grafica: Paola Saccardi - Immagini: Dreamstime.com

ne che abilitino una digital transformation flessibile, sicura e in grado di adattarsi rapidamente alle esigenze di business.
Lo sviluppo di un portfolio di servizi che concretizzano e rendono facile e sicura l'evoluzione verso il cloud ibrido è quello che ha fatto di OVHun gruppo che gestisce attualmente 27 data center distribuiti in 12 siti in 4 diversi continenti, spiega Dionigi Faccenda, Direttore Sales di OVH in Italia e Spagna. L'azienda dispone di una propria rete mondiale in fibra ottica a larga banda che le permette di gestire direttamente l'intera catena dell'hosting, e non solo.
Alle aziende che intendono passare in modo sicuro al cloud ibrido, infatti, OVH propone la tecnologia HCX, che permette di migrare le proprie macchine virtuali a caldo senza interruzione di servizio da un data center a un altro o a partire dalla propria infrastruttura.

Con vRack servizi cloud affidabili e sicuri

vRack è una tecnologia sviluppata da OVH che permette di mettere in comunicazione in modo sicuro server e servizi distribuiti sul territorio e di interconnettere i servizi OVH all'interno di una o più reti private sicure. In pratica, le aziende possono creare infrastrutture private complesse grazie a un'architettura distribuita in modalità multi-datacenter.
Permette altresì di isolare i server principali e creare di fatto fino a 4.000 vLAN private, facendo in modo che le comunicazioni tra i server non passino sulla rete pubblica in modo da garantire livelli elevati di performance e affidabilità dei collegamenti.
Con lo sviluppo di vRack, OVH si è posta l'obiettivo di dare una risposta concreta alle esigenze di flessibilità che quando ci si rivolge al cloud diventa un aspetto chiave nell'individuare il provider di riferimento.
Elemento chiave è che si tratta di una soluzione estremamente flessibile che permette di scegliere tra numerosi servizi di OVH per quanto concerne infrastruttura, Storage, Big Data, Private e Public Cloud.
La tecnologia vRack è operativa tra i diversi data center proprietari di OVH distribuiti nel mondo, tra Europa, America del Nord e area Asia-Pacifico. Consente alle aziende di estendere le proprie infrastrutture on premise ai datacenter di OVH e creare una propria rete privata collegando le diverse soluzioni OVH di cui dispongono, in modalità ridondante o distribuita.
Tra gli elementi salienti di vRack, ha evidenziato Dionigi Faccenda, vanno annoverate sicurezza e velocità. Per quanto concerne la sicurezza, che continua ad essere una delle principali preoccupazioni delle aziende che prendono in considerazione il passaggio al cloud, e ne rappresenta il freno principale per il 40% secondo l'Osservatorio Cloud & ICT as a Service, le policy di security avanzate disponibili permettono di garantire alla vLAN il medesimo livello di sicurezza delle reti locali interne.
La tecnologia vRack garantisce anche elevate velocità trasmissive, un fattore essenziale nel collegamento di data center e nelle attività di disaster recovery con RTO e RPO molto severi. Grazie a interconnessioni in fibra ottica implementate e gestite con l'utilizzo di dispostivi DWDM, la rete OVH permette di raggiungere prestazioni di primissimo piano, con collegamenti tra i vari data center multipli, con percorsi automatici alternativi e una banda di 13 Tbps in espansione.

Un 2018 denso di novità, tra migrazione al Cloud e il GDPR

Se il 2017 è stato per OVH un anno ricco di soddisfazioni, tale si prospetta anche il 2018. Per l'anno in corso, il progetto "Next Level", contri-

La rete mondiale dei data center OVH

buirà a rafforzare la posizione della società tra i principali attori mondiali del Cloud. Il progetto prevede l'evoluzione dell'offerta di OVH verso tre nuovi universi:

- OVHcloud, infrastrutture altamente scalabili per operazioni critiche;
- OVHspirit, server dedicati ad elevate prestazioni con un mirato rapporto qualità/prezzo;
- OVHmarket, soluzioni di hosting, domini, servizi email e, in alcuni Paesi, di telecomunicazione raggruppati sotto un unico brand.

Il progetto Next Level segue di pochi mesi l'acquisizione di vCloud Air di VMware, volta a permettere al Gruppo di accelerare l'insediamento negli Stati Uniti e soprattutto di dotarsi della tecnologia HCX (Hybrid Cloud eXchange) per offrire servizi di migrazione di infrastrutture inter-data center senza interruzioni di servizio.

Il 2018 sarà anche l'anno dell'applicazione del GDPR, importante normativa sul trattamento dei dati, cui tutte le aziende europee si dovranno conformare.

Per facilitarne il rispetto, OVH ha integrato nella sua infrastruttura i criteri previsti dal GDPR per la protezione dei dati personali dei clienti, come la trasparenza in merito alla localizzazione dei dati e il rifiuto di ricorrere a un subappalto che implichi l'accesso ai dati archiviati dall'utente. Inglobate nella sua offerta sono anche le linee guida dettate dal Codice di condotta CISPE (Cloud Infrastructure Providers in Europe), uno dei primi a nascere sotto l'impulso del GDPR con l'obiettivo di fornire un quadro di riferimento per l'applicazione della normativa presso i provider e i loro clienti e favorire così la nascita di un mercato europeo digitale unico.

L'impegno OVH per un Cloud sempre più aperto

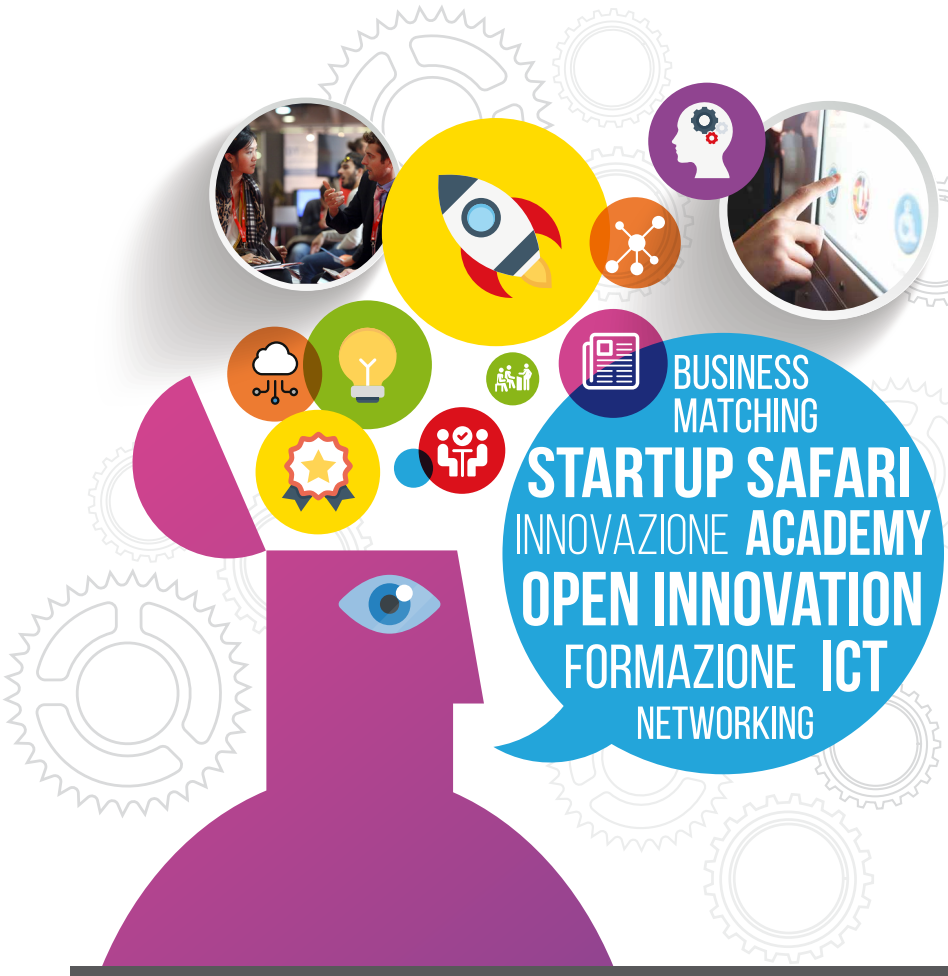
Tra le iniziative che vedono impegnata OVH vi è anche la sfida per un cloud sempre più aperto che permetta il massimo di indipendenza alle aziende che lo adottano.

Per perseguire questo obiettivo OVH è parte attiva dell'Open Cloud Foundation, un'iniziativa che riunisce i principali attori del settore IT (fornitori, utenti, centri di ricerca, organismi pubblici, e costituita per garantire soluzioni aperte e alternative alle politiche di chiusura presenti sul mercato.

Open Cloud Foundation, che annovera già oltre venti sostenitori del Cloud aperto, ha la missione di promuovere gli standard tecnologici - e sviluppare quelli mancanti- partecipare a un dialogo pubblico sulle regolamentazioni e certificare i fornitori conformi ai valori dell'Open Cloud.

Quattro i valori fondanti:

- La reversibilità dei dati, in modo che le aziende abbiano la libertà di scegliere e cambiare in qualsiasi momento il provider di infrastrutture senza alcun impatto sui propri dati.
- L'interoperabilità per rendere i dati compatibili con il maggior numero possibile di soluzioni sul mercato.
- La protezione dei dati da un punto di vista legislativo, in base al Paese in cui sono localizzati.
- La proprietà intellettuale degli algoritmi sviluppati da un cliente sulle infrastrutture di un provider.
- L'Open Cloud Foundation contribuirà anche, evidenzia OVH, a migliorare le practice esistenti e, se necessario, ad accompagnare l'evoluzione normativa dei servizi Cloud.



DOVE TROVI L'INNOVAZIONE PER LA TUA AZIENDA

Smau è l'appuntamento di riferimento per l'ecosistema italiano dell'Innovazione. Alla tre giorni di Milano da diversi anni si affianca un Roadshow che porta l'innovazione nei territori per approdare a Berlino e da quest'anno anche a Londra, dove le startup e imprese del nostro Paese avranno la possibilità di misurarsi direttamente con investitori e imprese del mercato tedesco e britannico.

Un percorso che ogni anno vede la partecipazione di **50mila imprese**, che scelgono Smau per trovare nuove "ispirazioni" e **orientarsi nel complesso e ricchissimo panorama dell'ecosistema dell'innovazione italiana**. Il modello di riferimento è quello dell'Open Innovation: innovare da soli non conviene più, mentre è dall'incontro fra **mondo corporate** e la **galassia delle startup** che spesso nascono le innovazioni destinate a disegnare il futuro. Ma la proposta di Smau non si esaurisce con il calendario del Roadshow: alle tappe sul territorio si affianca la **piattaforma online gratuita** di formazione permanente **Smau Academy**.

SMAU IN PILLOLE (dati 2017)

- **50.000** VISITATORI
- **1.000** ESPOSITORI
- **2.200** OPERATORI MEDIA
- **700** WORKSHOP ED EVENTI
- **500** CASI DI SUCCESSO

UN ROADSHOW PER ACCELERARE L'INNOVAZIONE ITALIANA

SMAU PADOVA 22-23 Marzo
SMAU LONDRA 2-3-4 Maggio *new*
SMAU BOLOGNA 7-8 Giugno
SMAU BERLINO 13-14-15 Giugno
SMAU MILANO 23-24-25 Ottobre
SMAU NAPOLI 13-14 Dicembre

+39.02.283131 | INFO@SMAU.IT | WWW.SMAU.IT

IL DATA CENTER CAMBIA E VA NEL CLOUD

Il Data center sta mutando forma per far fronte alle esigenze di sicurezza e di business. L'iperconvergenza si sta affermando con concreti benefici

In un modo che è stato inizialmente strisciante ma con un processo che tende a velocizzarsi è in atto la trasformazione dei data center. A dare il via sono state le esigenze degli utilizzatori e del contesto di business in cui si muovono e , subito a seguire, chi li gestisce, e cioè il personale IT alle prese con una trasformazione digitale che in pochi anni ha proiettato il data center in uno scenario di utilizzo e un contesto architetturale del tutto nuovo.

Svariati sono i fattori che hanno portato a questo cambiamento, alcuni di natura economica e sociale, altri di natura prettamente tecnologica ed organizzativa .

Tra i primi va annoverata l'esigenza da parte delle aziende di concentrarsi sul core business e di ottimizzare Capex e Opex, il che, detto in altre parole, contenere il costo delle infrastrutture o perlomeno parametrarle ai ritorni in termine di fatturato e allo stesso tempo ottimizzare, alias ridurre, il personale preposto. Il processo di virtualizzazione dell'IT è stato in pratica un modo per contenere il Capex ed utilizzare al meglio il data center.

Tra i secondi la proiezione verso l'esterno dell'azienda, la crescita tumultuosa della Mobility, l'esigenza di rispondere rapidamente alle richieste del mercato.

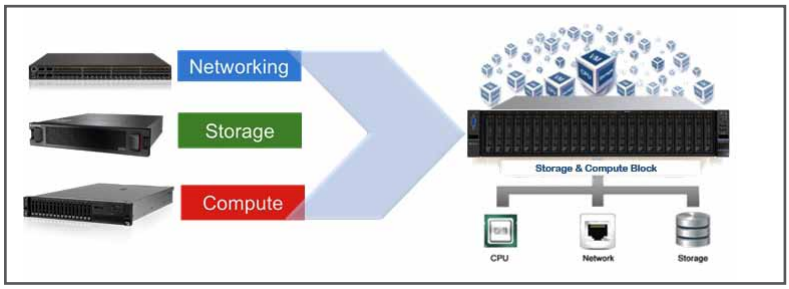
Il successo del Cloud e dell'IT visto come servizio e come modo per esternalizzare la sua complessità deriva in definitiva dal fondersi di quanto sopra detto.

L'iperconvergenza è un ulteriore passo in questa direzione volta a semplificare la complessità dell'IT e in qualche modo permettere anche alle PMI e alle aziende e agli enti pubblici in generale di poter trarre beneficio dai processi che sino ad ora hanno interessato e favorito i service provider o i fornitori mondiali di servizi cloud, senza che si debbano far carico degli oneri di una complessa gestione.

Da convergenza a iperconvergenza

Ma cosa si intende per iperconvergenza, che segue quella che a questo punto si può definire come step intermedio nel processo evolutivo dell'IT, della convergenza?

In sostanza, pur con varianti minori, consiste nel rendere disponibili soluzioni chiavi in mano che racchiudono capacità di calcolo, di storage e di rete, il tutto in un fattore di forma compatto e predisposto per l'espansione sia locale che geografica. Un ruolo importante in questa evoluzione lo gioca il software e in particolare quello di



Esempio di soluzione iperconvergente (fonte Lenovo)

orchestrazione e di gestione.

Poiché l'obiettivo primario di un tale approccio è quello della semplificazione, e cioè del poter disporre di quello che a parte le dimensioni di scala si configura come un vero e proprio data center senza però doverne supportare i costi di gestione, è subito evidente che il software di gestione e orchestrazione delle risorse deve risultare molto user friendly e farsi carico di tutte quelle operazioni che in un data center convenzionale è competenza di personale specializzato che va a influire in modo massiccio sui costi di esercizio e sull'Opex.

I benefici del diffondersi di soluzioni iperconvergenti sono molteplici. Innanzitutto si apre la possibilità anche per medie o piccole aziende di disporre di soluzioni resilienti e con prestazioni facilmente espandibili, sia per uso locale che per realizzare infrastrutture di backup o di disaster recovery a costi di realizzazione e di esercizio molto contenuti. Va osservato che però nel caso di soluzione per il disaster recovery un ruolo importante è assunto da parametri quali RPO e RTO, ovverossia il punto da recuperare e il tempo in cui lo si vuole realizzare per ritornare operativi. Tempo che naturalmente dipende dalla velocità della linea di interconnessione e che può avere un costo anche fortemente variabile. Importante è quindi anche definire una scala di priorità tra le applicazioni per stabilire quelle che devono essere recuperate e rimesse in produzione per prime, dati compresi.

Un secondo beneficio è che diventa più facile evolvere a livello di applicazioni e di elaborazione e gestione verso il cloud. Si può in tale scelta strategica spostare sul cloud attività non critiche per quanto concerne la riservatezza, così come adottare il cloud per la fase di test e sviluppo di nuove applicazioni mantenendo però una gestione e un controllo locale delle applicazioni e relativi dati aventi carattere sensibili che non potrebbero essere trasferiti sul cloud, sia in base a scelte strategiche che a regolamenti nazionali e sovranazionali.

Un terzo punto coinvolge il canale, perché anche aziende o system integrator di medie dimensioni possono dare servizi con un data center che può essere rapidamente attivato anche in sedi distaccate prossime ai clienti e fatto crescere in funzione del numero e delle esigenze dei clienti.

Soluzioni adatte per tutte le esigenze

L'adozione di data center di nuova concezione e in particolare iperconvergenti e con caratteristiche centrate sul sofwtare, in aderenza a quanto viene riferito come "Software Defined Data Center", ha affrontato una ulteriore evoluzione: quella dei moduli o mattoncini di base a disposizione degli utenti.

Una prima fase di sviluppo di questo nuovo approccio, con soluzioni a rack o stand alone di configurazione fissa ha mostrato delle criticità a causa della rigidità e ha subito un adattamento progressivo per andare incontro a esigenze specifiche per quel che riguarda il solo calcolo o il solo storage.

Le prime soluzioni, peraltro abbastanza recenti, presentavano infatti il problema che se si voleva espandere il sistema perché lo spazio storage (o il tipo di storage) era esaurito o la capacità di calcolo non più in grado di gestire il crescente workload, si doveva comperare un nuovo modulo di cui poi si finiva con l'usare solo una delle

componenti.
Ciò ha portato i produttori, pur mantenendo invariato l'approccio generale, a sviluppare moduli dedicati al solo storage (anche con caratteristiche diverse in termini dii capacità e tipologia) o al solo calcolo.
In sostanza, quello che è possibile fare stante l'attuale situazione dell'offerta, è dotarsi di una soluzione iniziale costituita da un paio di moduli con capacità di calcolo, storage e rete per disporre in ogni caso di un sistema ridondato e poi aggiungere moduli analoghi se storage e capacità elaborativa vanno come esigenze di pari passo o aggiungere solo moduli storage o di calcolo .
I benefici sono consistenti e non solo per gli utenti finali ma anche per il Canale. Come evidenziato, per quest'ultimi si apre non solo la strada verso la fornitura di servizi in modalità del tutto simile (salvo la scala) al Cloud messo in campo da colossi del mercato in modo proporzionale al business, ma diventa possibile farlo concentrandosi sulla gestione dei servizi erogati e sulla gestione e il supporto del cliente.


Alberto Filisetti - Nutanix Italia

Data center a misura di esigenza

Con un processo che tende a velocizzarsi, è in atto la trasformazione dei data center evidenziata nei paragrafi precedenti. A dare il via sono state le esigenze degli utilizzatori e del contesto di business in cui si muovono e, subito a seguire, di chi li gestisce, e cioè il personale IT alle prese con una trasformazione digitale che in pochi anni ha proiettato il data center in uno scenario di utilizzo e un contesto architetturale del tutto nuovo.
Svariati sono i fattori che hanno portato a questo cambiamento, alcuni di natura economica e sociale, altri di natura prettamente tecnologica ed organizzativa .
Tra i primi va annoverata l'esigenza da parte delle aziende di concentrarsi sul core business e di ottimizzare Capex e Opex, il che, detto in altre parole, contenere il costo delle infrastrutture o perlomeno parametrarle ai ritorni in termine di fatturato e allo stesso tempo ottimizzare, alias ridurre, il personale preposto. Il processo di virtualizzazione dell'IT è stato in pratica un modo per contenere il Capex ed utilizzare al meglio il data center. Tra i secondi la proiezione verso l'esterno dell'azienda, la crescita tumultuosa della Mobility, l'esigenza di rispondere rapidamente alle richieste del mercato.
Il successo del Cloud e dell'IT visto come servizio e come modo per esternalizzare la sua complessità deriva in definitiva dal fondersi di quanto sopra detto.
L'iperconvergenza, ha osservato Alberto Filisetti, Country Manager di Nutanix Italia, è un ulteriore passo in questa direzione, volta a semplificare la complessità dell'IT e in questo modo permettere anche alle PMI e alle aziende e agli enti pubblici in generale di poter trarre beneficio dai processi che sino ad ora hanno interessato e favorito i service provider o i fornitori mondiali di servizi cloud, senza che si debbano però far carico degli oneri di una complessa gestione e di parimenti elevati investimenti.

Dalla convergenza all'iperconvergenza

Ma cosa si intende per iperconvergenza? In sostanza, pur con varianti minori, consiste nel rendere disponibili soluzioni chiavi in mano che racchiudono capacità di calcolo, di storage e di rete, il tutto in un fattore di forma compatto e predisposto per l'espansione sia locale che geografica. Un ruolo importante in questa evoluzione lo gioca il software e in particolare quello di orchestrazione e di gestione.

Poiché l'obiettivo primario di un tale approccio è quello della semplificazione, e cioè del poter disporre di quello che a parte le dimensioni di scala si configura come un vero e proprio data center senza però doverne supportare i costi di gestione, è subito evidente, osserva Filisetti, che il software di gestione e orchestrazione delle risorse deve risultare molto user friendly e farsi carico di tutte quelle operazioni (o quasi) che in un data center convenzionale è competenza di personale specializzato che va a influire in modo massiccio sui costi di esercizio e sull'Opex.

I benefici del diffondersi di soluzioni iperconvergenti sono molteplici. Innanzitutto si apre la possibilità anche per medie o piccole aziende di disporre di soluzioni resilienti e con prestazioni facilmente espandibili, sia per uso locale che per realizzare infrastrutture di backup o di disaster recovery a costi di realizzazione e di esercizio molto contenuti.

Va osservato che però nel caso di soluzione per il disaster recovery un ruolo importante è assunto da parametri quali RPO e RTO, ovverossia il punto da recuperare e il tempo in cui lo si vuole realizzare per ritornare operativi. Tempo che naturalmente dipende dalla velocità della linea di interconnessione e che può avere un costo anche fortemente variabile. Importante è quindi anche definire una scala di priorità tra le applicazioni per stabilire quelle che devono essere recuperate e rimesse in produzione per prime, dati compresi.

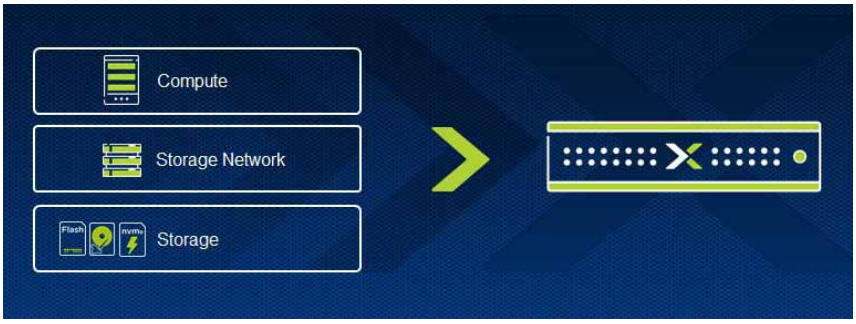
Un secondo beneficio è che diventa più facile evolvere a livello di applicazioni e di elaborazione e gestione verso il cloud. Si può in tale scelta strategica spostare sul cloud attività non critiche per quanto concerne la riservatezza, così come adottare il cloud per la fase di test e sviluppo di nuove applicazioni mantenendo però una gestione e un controllo locale delle applicazioni e relativi dati aventi carattere sensibili che non potrebbero essere trasferiti sul cloud, sia in base a scelte strategiche che a regolamenti nazionali e sovranazionali.

Un terzo punto coinvolge il canale, perché anche aziende o system integrator di medie dimensioni possono dare servizi con un data center che può essere rapidamente attivato anche in sedi distaccate prossime ai clienti e fatto crescere in funzione del numero e delle esigenze dei clienti.

L'approccio di Nutanix all'iperconvergenza

L'approcci Nutanix alla iperconvergenza si basa nella sua essenza su uno stack che integra i layer di una soluzione IT complessa e su moduli di base su cui lo stack di applicazioni e servizi, cloud privato o ibrido compreso, opera.

Lo stack comprende a livello fisico o logico lo strato di rete che connette i moduli di calcolo e di storage, sia locali che distribuiti, e su cui agisce un software di virtualizzazione nativa che viene fornito gratuitamente assieme all'infrastruttura. Aperta è comunque la possibilità di adottare il software di virtualizzazione disponibile sul mercato preferito.



L'approccio Nutanix all'iperconvergenza: rete, server, storage tutto in uno

Sullo strato di virtualizzazione si calano poi le applicazioni per la gestione, l'automazione delle operation e quanto serve per una gestione nel cloud, proprie-

tario o ibrido.
Per quanto concerne il cloud, ha illustrato Filisetti, è possibile ad esempio procedere alla attivazione e alla gestione delle applicazioni e disporre della visibilità e del controllo esaustivo dell'uso che si fa delle risorse pubbliche.
Ampia la scelta di soluzioni cloud pubbliche disponibili, che comprende Google Cloud Platform, AWS e Microsoft Azure.
Ampia anche la scelta di moduli di base, disponibili sia come elementi dotati di capacità di calcolo e di storage e anche come moduli dedicati con solo capacità di calcolo o solo capacità di storage, quest'ultima anche con caratteristiche e dimensioni atte a soddisfare sia workload normali che workload che richiedono elevate prestazioni in termini di velocità di I/O o di resilienza del media.
Non ultime, atte a soddisfare le più svariate esigenze anche le architetture realizzabili. Comprendono sia una connettività locale a livello di rack o di rete per espandere il sistema in modalità scale out, che la possibilità di remotizzazione geografica dei diversi elementi fisici per far fronte a esigenze distribuite o per realizzare architetture ad elevata resilienza dotate di capacità di disaster recovery, con sistemi che possono essere connessi sia con modalità sincrona che asincrona in funzione delle distanze e delle esigenze di recovery.

Roberto Vicenzi - Centro Computer

Cloud, data center e sicurezza a fattore comune

Un aspetto che solleva sempre dubbi è la sicurezza di una soluzione centrata su cloud e sul grado di disponibilità dei data Center su cui si appoggia.
A rimuovere del tutto o perlomeno ad attenuare fortemente i dubbi ci ha pensato Centro Computer, società di consulenza specializzata in prodotti, servizi e soluzioni IT per le aziende, che ha consolidato la partnership con ReeVo Cloud, Service Provider italiano specializzato in soluzioni e servizi di Cloud Computing e con Veeam Software, fornitore di soluzioni di Availability for the Always-On Enterprise.
La partnership ha avuto l'obiettivo di fornire soluzioni di Backup e Disaster Recovery alle imprese che permettano di ridurre sensibilmente i costi di gestione garantire un funzionamento ininterrotto di piattaforme e applicazioni.
L'accordo prende il via dalla considerazione, del tutto condivisibile, che anche il data center oggi si sviluppa sempre più in ottica Cloud e che da un punto di vista tecnologico buona parte delle resistenze nei confronti del Cloud sono state superate, come testimoniano i tassi di crescita a doppia cifra che si verificano da qualche anno anche in Italia.
Restano però da risolvere alcuni aspetti, osserva Centro Computer : il primo è legato al fatto che il cloud è considerato competenza solo dei grandi player americani, il secondo è l'idea che il mondo dei partner resti tagliato fuori dal nuovo business.
Due pensieri che però non corrispondono più alla realtà, come dimostrato dalla alleanza che da un paio anni è stata siglata tra ReeVo e Centro Computer, con una serie di iniziative e di investimenti importanti, accelerati in particolare negli ultimi mesi.
La collaborazione della società con Veeam Software invece risale al 2010, da quando è attiva la filiale italiana, perché le soluzioni di backup & replication di Veeam si sono rivelate come le più adatte, osserva l'azienda, alle dimensioni delle infrastrutture aziendali dei clienti e compliant ai requisiti richiesti.
«Il Cloud sta diventando sempre più l'elemento centrale delle nostre strategie di sviluppo, indi-

rizzando anche le scelte di carattere tecnologico messe in atto e programmate per il futuro. I data center più innovativi e all'avanguardia e le soluzioni che assicurano la massima affidabilità e protezione dati, sono un punto di forza della nostra offerta Cloud, ecco perché ci affidiamo a partner di fiducia come ReeVo e Veeam che garantiscono alte performance, virtualizzazione e massima sicurezza ai dati dei nostri clienti, facendo leva su un data center totalmente italiano», ha commentato Roberto Vicenzi, Vice Presidente di Centro Computer.

Ampia l'offerta sviluppata da Centro Computer nel cloud, che spazia dagli ambienti privati, a quelli pubblici e ibridi e in particolare per il Backup e il Disaster Recovery, che hanno il beneficio di costi variabili tramite un canone fisso predeterminato, l'eliminazione degli investimenti infrastrutturali e delle attività di gestione dei sistemi server, la riduzione dei consumi energetici e del TCO del parco macchine utenti.

«Grazie alla forte alleanza con Centro Computer caratterizzata dalla loro esperienza e grandi competenze, riusciamo ad offrire soluzioni innovative e sicure che rendono unica la nostra offerta. In ReeVo, assicuriamo un ambiente Cloud efficiente, scalabile, ed ai massimi livelli di sicurezza garantiti tramite i propri data center, in conformità alle norme e certificazioni più rigorose (ISO9001, ISO27001, ANSI 942, TIER4). Inoltre, la nostra proposta basata su tecnologia Veeam Cloud offre una soluzione completamente integrata, veloce e sicura per l'esecuzione di backup, repliche e ripristini dal Cloud», ha evidenziato Salvatore Giannetto, Presidente di ReeVo.

Data center e infrastruttura di rete

La ridefinizione del data center in chiave cloud o multicloud oltre alla sicurezza fa emergere il problema della rete e delle sue prestazioni. È un problema che ha affrontato Juniper Networks, società che sviluppa prodotti, soluzioni e servizi che abilitino la trasformazione in chiave digitale delle aziende e l'economia ad essa legata, che ha ampliato il proprio portfolio di soluzioni per permettere alle aziende di costruire ambienti multicloud automatizzati e sicuri.

In pratica, e a integrazione del suo portfolio di soluzioni di networking per data center, campus, sedi periferiche e cloud, con l'espansione si è proposta di fornire alle aziende anche quelle soluzioni infrastrutturali di cui le organizzazioni necessitano per diventare multicloud-ready e affrontare i cambianti richiesti da una smart economy.

L'espansione del portfolio in chiave multicloud deriva, ha osservato, dalla presa d'atto che le aziende spostano sempre più dati e applicazioni negli ambienti cloud in quanto forniscono una maggiore agilità e flessibilità. In proposito, da un recente studio condotto da PwC emerge che la maggior parte del workload che attualmente le aziende gestiscono in locale verrà migrato al cloud pubblico nel giro di 1-3 anni. Quello che ci si aspetta è che di conseguenza le aziende adottino sempre più strategie multicloud più articolate in modo da gestire workload distribuiti su diversi ambienti IT, dall'on-premise al cloud ibrido e al multicloud.

«La promessa del multicloud è l'offerta di un'infrastruttura sicura, ubiquitaria, affidabile e fungibile e in cui la migrazione dei workload sia un processo semplice e intuitivo. Affinché l'IT possa affrontare con successo questa transizione, è essenziale che le aziende considerino non solo i data center e il cloud pubblico ma anche le reti di campus e quelle delle filiali distaccate. In caso contrario, e dato che i confini di rete impediscono controllo e visibilità end to end, si troveranno a dover affrontare problemi legati a sicurezza e operazioni frammentate», ha osservato Bikash Koley, CTO di Juniper Networks.

Non si tratta però di un'evoluzione che possa avvenire da un giorno all'altro e, al fine di ri-

muovere gli ostacoli che potrebbero impedire di ottenere i benefici attesi dal multicloud, l'automazione e la sicurezza end-to-end dovranno essere integrate in tutti i punti della rete. Il problema è che le aziende si trovano in fasi diverse del percorso di avvicinamento a un'architettura multicloud che sia sicura e automatizzata, ed è questo differenziale che con la sua offerta espansa Juniper si è data l'obiettivo di colmare sia per quanto concerne le infrastrutture data center, che di campus, di sedi periferiche e in cloud.

Specificatamente per le organizzazioni che stanno aggiornando, ampliando o consolidando i data center per preparare l'ambiente IT al multicloud sicuro e automatizzato, Juniper sta introducendo nuove soluzioni:

Una è rappresentata dallo switch QFX10002-60C, un dispositivo di rete che può essere usato come dispositivo spine o edge per l'interconnessione tra data center. L'apparato equipaggia 60 interfacce a standard 100 Gigabit Ethernet deep buffer. Oltre a questo le novità comprendono anche il QFX5210-64C, uno switch con 64 porte 100GbE, e il QFX5200-48Y, equipaggiato con 48 interfacce 25GbE native.

Una seconda soluzione è rappresentata dallo switch QFX MACsec, un dispositivo che si aggiunge agli switch modulari QFX10000 del portfolio della società e che fornisce una connettività con 30 porte 100GbE per il traffico crittografato all'interno e tra i data center.

Switch Jumiper QFX10002-60C

Data center e cloud lock-in: il ruolo dei comitati

Il 25 maggio 2018 è la data di scadenza ufficiale - uguale per tutti i paesi dell'Unione Europea - per la piena applicazione del General Data Protection Regulation (GDPR), il regolamento che mette al centro le persone, ne riconosce il diritto all'oblio e le informa in modo trasparente, leale e dinamico sul trattamento delle proprie informazioni. Non si tratta soltanto della principale evoluzione della normativa comunitaria fin dall'introduzione della Direttiva dell'Unione Europea sulla protezione dei dati, ma anche di un cambiamento di consapevolezza grazie al quale "difendere i dati" diventa difendere le persone, la loro identità.

Il GDPR nasce, quindi, osserva Stefano Sordi, Chief Marketing Officer di Aruba, con l'intento di armonizzare le direttive a livello europeo, fissando delle regole chiare e precise su come mantenere e conservare i dati e, addirittura, prevede di creare una nuova figura aziendale con il ruolo di Data Protection Officer, specificatamente adibito a queste dinamiche. Parallelamente, sono diverse le associazioni ed organizzazioni di service provider che hanno cercato di anticipare la regolamentazione in termini di sicurezza e protezione dei dati.

Il ruolo del CISPE

Tra le prime, trova posto il CISPE, una coalizione nata nel 2016 che oggi raccoglie oltre 20 tra i maggiori provider di infrastrutture cloud attive in 15 Paesi europei. Il CISPE ha dato vita ad un Codice di Condotta (CoC) che precede l'entrata in vigore del GDPR, poiché, allineandosi ai suoi requisiti, ne condivide l'obiettivo principale: ridare ai cittadini il controllo dei propri dati personali, sapere dove questi dati si trovano e semplificare il contesto normativo per il commercio internazionale, unificando la regolamenta-

zione all'interno dell'UE.
Ai sensi del codice di condotta CISPE, infatti, i provider di infrastrutture cloud non possono effettuare data mining o tracciare i profili dei clienti per attività di marketing, pubblicità o simili, per scopi personali o per la rivendita a terzi.
Nel caso del CISPE, i servizi cloud dichiarati a norma del codice di condotta CISPE sono identificati da un particolare marchio di garanzia - 'CISPE service-declared' - che offre ai clienti dei servizi che lo espongono, la tranquillità di sapere che i dati ospitati presso le loro infrastrutture si trovano all'interno di data center localizzati entro i confini dell'Unione Europea e che sono conformi, già oggi, a determinati requisiti in termini di protezione e sicurezza delle informazioni.


Stefano Sordi - Aruba

Non c'è bisogno di attendere il 25 maggio 2018 - dunque - chiarisce Sordi, per iniziare a corazzarsi, è essenziale arrivarci preparati e non aspettare la fatidica data a braccia conserte: questo termine è da considerarsi come un'opportunità per favorire la sicurezza e la crescita aziendale - velocizzandola - creare posti di lavoro e, finalmente, beneficiare di un mercato digitale che potrebbe essere paragonato a quello statunitense o a quello cinese.

Il problema del data lock-in e la Open Cloud Foundation

Un altro tema di respiro internazionale su cui Sordi mette in guardia, che rappresenta un aspetto importante di valutazione quando si inizia ad usare un servizio cloud, è il "data lock-in", ossia la difficoltà che si può incontrare qualora si decida di spostare i propri dati da un cloud provider ad un altro.
OCF, Open Cloud Foundation, è un'associazione di aziende tecnologiche che nasce con l'obiettivo di elaborare un framework che assicuri l'apertura del cloud, facendo convergere su questo obiettivo fornitori di tecnologie e servizi, cloud provider, aziende clienti, società di ricerca ed entità 'regolatorie'. Lo scopo è quello di preservare e garantire la libertà di scelta delle aziende clienti nel disegno dei loro business e di evitare il pericolo del lock-in che può essere esercitato da fornitori poco trasparenti.
In uno scenario cloud in forte accelerazione come quello attuale, molto presto ogni livello tecnologico dell'offerta ICT sarà a disposizione in modalità as a service. Questo porterà le aziende clienti a poter fare affidamento su molti più servizi di outsourcing e a valore aggiunto offerti attraverso il cloud. Diventerà, quindi, essenziale evitare, da un lato, la nascita di nuovi sistemi a silos, dall'altro, che operatori cloud di prima grandezza possano imporre al mercato degli "standard" che si caratterizzerebbero inevitabilmente come chiusi e limiterebbero la dinamicità del mercato.
Per assicurare una crescita stabile per qualsiasi business, oggi, e sempre più in futuro, sarà necessario tutelare il concetto di cloud aperto: permettere ai clienti di cambiare con facilità il proprio fornitore e consentire l'accesso a degli stack cloud eterogenei manterrà attiva la competizione e spingerà gli operatori a sviluppare e offrire importanti innovazioni.
Grazie a questo tipo di iniziative - tra cui CISPE e OCF - è già possibile individuare i provider che si stanno attivando in tal senso, anche in anticipo rispetto all'evoluzione normativa, compiendo una serie di passaggi che garantiscono un sistema più attento alla sicurezza e alla trasparenza dei servizi in cloud.

VEEAM BACKUP FOR MICROSOFT OFFICE 365 SEMPRE PIÙ RICHIESTO

Albert Zammar - Veeam

Continua a crescere il numero delle aziende e degli utenti che ricorrono al backup di Veeam per rendere sicura la migrazione dei dati aziendali sul cloud

Veeam Software, società che sviluppa soluzioni per l'Availability for the Always-On Enterprise, ha confermato che cresce la richiesta di Veeam Backup for Microsoft Office 365 e che già .oltre 25.000 aziende hanno scaricato il software, numero che equivale in pratica a oltre 2,3 milioni di utenti Microsoft Office 365.

Nel solo trimestre fiscale più recente l'incremento delle vendite, ha illustrato l'azienda, grazie al rilascio di Veeam Backup for Microsoft Office 365 v1.5, è stata pari al 327%.

«Questi dati positivi, oltre a registrare 4 trimestri di crescita consecutivi, consentono a Veeam di porsi come leader di mercato nella protezione dati Office 365» ha commentato Albert Zammar, Regional Vice President della Southern EMEA Region di Veeam.

Il successo sul mercato si spiega con il fatto che Veeam Backup for Microsoft Office 365 fornisce alle aziende varie opzioni aggiuntive per proteggere i loro dati, oltre alla replica automatica dei dati che Microsoft fornisce nei suoi data center e ai controlli nativi di resilienza disponibili in Office 365. E una combinazione che consente in pratica alle aziende di mantenere un controllo completo dei propri dati e garantirne la disponibilità ai propri utenti.

Il nuovo rilascio di Veeam Backup for Microsoft Office 365 v1.5 ha portato ad una sua massiccia adozione da parte del mercato Enterprise grazie ai numerosi miglioramenti di scalabilità, guidati dalla nuova architettura multi-repository e multi-tenant che consente di proteggere le implementazioni Office 365 di grandi aziende con un'unica installazione.

Vodafone Espana, la Metropolitan Transportation Authority della Contea di Los Angeles, Fresno County Sheriff Department IT team, College Success Foundation e la città di Mairie de Versailles sono solo alcune delle grandi società., osserva Veeam, che sfruttano già la scalabilità e l'affidabilità della soluzione Veeam.

Ma l'interesse per il prodotto non è limitato alle aziende. «La nuova release dà la possibilità ai partner Veeam Cloud & Service Provider (VCSP) di offrire servizi di backup per Office 365 consentendo ai loro clienti di proteggere i dati critici delle e-mail in caso di attacco, errore umano o interruzione di servizio», ha commentato Lara del Pin , channel manager per l'Italia.

Veeam sta inoltre assistendo ad un uso intensivo di infrastrutture e-mail ibride. Per questo consente alle aziende di eseguire il backup dei dati e-mail sia di Office 365 sia di Exchange on-premises con la stessa soluzione. I clienti hanno la possibilità di memorizzare i dati nella loro posizione preferita, sia in un cloud pubblico come Microsoft Azure oppure on-premises.

CON A10 NETWORKS UNA PROTEZIONE DDOS BASATA SU CLOUD

La nuova soluzione DDoS Protection Cloud e l'appliance A10 Thunder 1040 TPS con scrubbing a spettro completo forniscono una protezione DDoS ibrida avanzata

Thunder 1040 TPS

A10 Networks, azienda specializzata in Application Visibility Performance and Security, ha annunciato la disponibilità di A10 DDoS Protection Cloud, una soluzione ottimizzata da Verisign, e l'appliance di sicurezza avanzata A10 Thunder 1040 TPS.

A10 DDoS è una soluzione, ha illustrato Alberto Crivelli, Regional Sales Manager per l'Italia, che tramite recenti soluzioni di sicurezza che incorpora fornisce una protezione aziendale a spettro completo per rilevare e mitigare gli attacchi denial of service distribuiti (DDoS).

Punto chiave della soluzione, ha spiegato il manager che da due mesi ha assunto la responsabilità per l'Italia, è la combinazione di un approccio nella difesa dai DDoS allo stesso tempo flessibile ed olistico che coniuga la protezione on-premise allo scrubbing cloud orchestrato, il tutto disponibile con fattori di forma e modelli di sottoscrizione del servizio di protezione a costi contenuti.

Si paga solo in base al traffico effettivo

Chiaro il modello di erogazione del servizio volto a proteggere gli investimenti e rendere semplice il suo upgrade al crescere del traffico. Il contratto non prevede infatti diverse configurazioni funzionali del servizio ma un insieme già completo di funzionalità. Quello che cambia, ha illustrato il manager, è un corrispettivo diverso in base alla banda fruita da analizzare e quindi si presta a seguire in modo lineare come Opex l'andamento del traffico e del business.

A rafforzamento di questo approccio volto a tutelare il cliente, ilservizio A10 DDoS Protection Cloud, assicurato da DDoS Protection Service cloud-based di Verisign, si basa sull'effettivo traffico legittimo, cosa che evita di dover pagare il volume di traffico conseguente agli attacchi subiti.

Le oscillazioni di traffico sul servizio cloud sono poi ottimizzate dalle appliance on-premise Thunder TPS, che utilizzano il machine learning, la profilazione del traffico e l'uso intelligente delle policy per ridurre le interruzioni on-premise e avvisare A10 qualora fosse necessario un reindirizzamento al cloud. «A10 mette a disposizione un'unica soluzione avanzata per proteggere le aziende da attacchi DDoS on-premise e con scrubbing cloud, supportata dal nostro team DDoS SIRT», ha commentato Chris White, Executive VP of Worldwide Sales di A10 Networks. «La precisione chirurgica e l'approccio ibrido a spettro completo di questa soluzione permettono alle aziende di essere resilienti agli attacchi DDoS in modo efficace e con investimenti contenuti».

A10 DDoS Protection Cloud, ottimizzata da Verisign e l'appliance A10 Thunder 1040 TPS, con un'opzione per il bypass hardware, sono già disponibili tramite il canale, costituito da Symbolic come distributore unico per l'Italia e da una rete di partner di canale qualificati e certificati che copre l'intero territorio nazionale.

DA CANON UNA GESTIONE DOCUMENTALE IN CLOUD E SICURA

Canon ha annunciato espansioni del proprio portfolio di stampanti che mettono a disposizione funzioni documentali su cloud e sicure

ImageRUNNER ADVANCED 8500

Canon ha annunciato una nuova serie di prodotti imageRUNNER ADVANCE che si basa sulla piattaforma Unified Firmware Platform (UFP). Le stampanti della nuova generazioni sono state progettata, ha evidenziato l'azienda, per collegare le tecnologie office al cloud e farlo in modo sicuro tramite la funzione di Universal Login Manager per una autenticazione basata sul dispositivo. A livello operativo la connettività cloud consente di abbinare ai dispositivi specifici requisiti di workflow documentale.

Come accennato, la sicurezza è uno degli aspetti chiave della nuova serie. Il login per l'autenticazione dell'utente presente sul dispositivo fa ad esempio sì che anche i lavori inviati dai dispositivi mobili possano essere conservati in modo sicuro sino al momento del rilascio.

Per impedire la distribuzione non autorizzata di informazioni riservate, è possibile disabilitare alcune delle funzioni del dispositivo per utenti specifici; notifiche acustico-visive segnalano invece se sono stati lasciati nel dispositivo gli originali scansionati.

Ampie le funzioni della console, tramite la quale gli . gli utenti possono controllare da remoto lo stato della periferica e dei materiali di consumo. I dipendenti hanno anche la possibilità di acquisire o stampare documenti in modo sicuro mentre sono in viaggio e collegare i propri dispositivi mobile direttamente all'interno dei flussi di lavoro aziendali.

Svariate le modalità di connessione per i dispositivi smart, che comprende il QR Code standard, la Connettività NFC (opzionale) e il Bluetooth (opzionale).

Per quanto riguarda la disponibilità la nuova serie di stampanti imageRUNNER ADVANCE sarà disponibile a partire da febbraio 2018.

«Noi di Canon prendiamo molto seriamente le esigenze di sicurezza dei nostri clienti e siamo fermamente convinti che le aziende possano disporre di solide misure di sicurezza che non ostacolano l'efficienza, ma piuttosto, la migliorano. Il nostro impegno nel portare innovazione è strettamente collegato al saper ascoltare le esigenze dei nostri clienti e fornire loro una pronta risposta per sviluppare le migliori soluzioni possibili per le loro attività», ha commentato l'annuncio Daniel Woodstock, Product Marketing Manager di Canon Europe.

SECURITY 10 ANNI
TECHNOLOGIES
MANAGEMENT COMPLIANCE
SUMMIT

Atahotel Expo Fiera

Via Giovanni Keplero 12
20016 Pero (Mi)

13-14-15 marzo

Security Summit è la manifestazione dedicata alla sicurezza delle informazioni, delle reti e dei sistemi informatici che, da anni, appassiona i partecipanti con contenuti e approfondimenti sull'evoluzione tecnologica del mercato.
Giunto alla X edizione il Security Summit si è imposto, ed è riconosciuto dal mercato, come l'Evento di eccellenza nel panorama italiano grazie all'alta qualità dei relatori e alla numerosa partecipazione di pubblico sempre più qualificato.
Anche nel 2018 si confermano questi valori: una struttura articolata in sessioni plenarie, percorsi formativi, atelier tecnologici, tavole rotonde e seminari tecnici.
Certificata dalla folta schiera di relatori (più di 500 sono intervenuti nelle scorse edizioni) provenienti dal mondo della ricerca, dell'Università, delle Associazioni, della consulenza, delle Istituzioni e delle imprese, la manifestazione è stata frequentata da oltre 15.000 partecipanti, e sono stati rilasciati circa 10.000 attestati validi per l'attribuzione di oltre 16.000 crediti formativi (CPE).

La manifestazione vede impegnati in prima persona gli esperti del Clusit per la parte dei contenuti e Astrea sul fronte organizzativo per le quattro tappe annuali: quest'anno si parte dalla tre giorni di **Milano**, in programma presso l'Atahotel Expo Fiera il 13, 14 e 15 marzo con un'agenda articolata in sessioni plenarie, percorsi formativi, atelier tecnologici, tavole rotonde e seminari tecnici, a partire dalla presentazione del **Rapporto Clusit 2018 sulla sicurezza ICT in Italia e nel mondo.**

La partecipazione a Security Summit è gratuita, previa registrazione al sito securitysummit.it, dove sarà a breve disponibile il programma della tre giorni milanese.

Security Summit ha il patrocinio della Commissione Europea e di ENISA, l'Agenzia dell'Unione Europea per la sicurezza delle informazione e della rete.

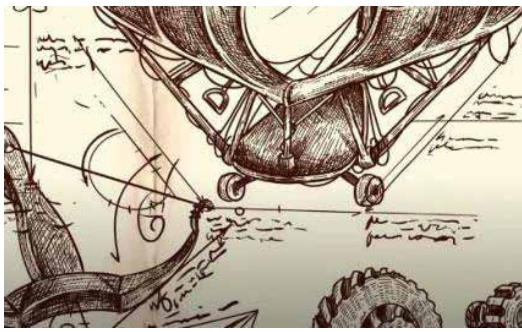
Organizzato da

Clusit
Associazione Italiana per la Sicurezza Informatica

ASTREA Advanced Security, Training Research, Events Agency

www.securitysummit.it

CLOUD PLATFORM SEMPLIFICA LO SVILUPPO DI APP E ACCELERA L'INNOVAZIONE



Gli aggiornamenti di SAP alla piattaforma cloud comprendono funzionalità mobile per aiutare le organizzazioni a diventare "aziende Smart"

SAP ha annunciato la disponibilità di un nuovo modello commerciale a consumo per permettere alle aziende di acquisire e lavorare con SAP Cloud Platform. I nuovi aggiornamenti includono un Software Development Kit di SAP Cloud Platform per iOS con cui l'azienda si è proposta di consentire di estendere applicazioni e processi enterprise ai dispositivi mobili.

SAP Leonardo, il sistema digitale per l'innovazione di SAP, si fonda su SAP Cloud Platform. Insieme permettono di trasformare le proprie organizzazioni in "aziende intelligenti," pronte per il ventunesimo secolo.

«Il nuovo modello commerciale a consumo di SAP Cloud Platform rende ancora più semplice per i nostri clienti e partner lo sviluppo e l'estensione di soluzioni innovative utilizzando il nostro portfolio di servizi per la piattaforma e il business in continua crescita», ha commentato Björn Goerke, president e chief technology officer SAP Cloud Platform. «Le innovazioni per il mobile, grazie alle esperienze di tipo consumer rese possibili dal nostro nuovo SDK di SAP Cloud Platform per iOS, forniscono alle organizzazioni maggiore libertà e flessibilità per creare e re-inventare il proprio business».

Il nuovo modello commerciale a consumo di SAP Cloud Platform si prefigge in particolare di abilitare una customer experience più semplice nel configurare e usare i servizi di SAP Cloud Platform. I benefici del Cloud sono immediati, e i servizi disponibili in SAP Cloud Platform, ha spiegato l'azienda, possono essere attivati velocemente secondo le specifiche esigenze e tempistiche. Inoltre, il nuovo modello commerciale, ha aggiunto, offre alle aziende una elevata trasparenza sull'uso di ogni servizio fruito mediante reporting e analytics, comprensivi di dati sul consumo in cloud e del residuo disponible per permettere di aggiustare i servizi di cui necessitano.

La migliorata versione di SAP Cloud Platform SDK per iOS supporta anche il consumo dei servizi di SAP Leonardo come ad esempio il riconoscimento delle immagini da un'app mobile.

SAP ha rilasciato anche ntrodotto due nuove app mobile per iOS. SAP Insurance Sales Assistant permette all'agente assicurativo di gestire le attività di vendita fornendo dati sui clienti con una vista a 360 gradi sulla posizione del singolo individuo e una sguardo sui principali indicatori di performance. SAP Asset Manager sfrutta il digital core di SAP S/4HANA e SAP Cloud Platform come la piattaforma per l'Internet of Things per gestire gli ordini di lavoro, le notifiche, il controllo delle condizioni e il consumo dei materiali, la gestione dei tempi e l'analisi dei guasti.

CON VERTIV L'ENERGIA PER LA RETE DIVENTA UN SERVIZIO ESAAS

Il colosso delle telecomunicazioni collaborerà con Vertiv per aumentare l'efficienza e sostenere l'innovazione

Giordano Albertazzi - Vertiv

Al Mobile World Congress, Vertiv e Telefónica hanno annunciato una partnership globale a lungo termine che promuoverà il risparmio energetico con le più adeguate soluzioni di infrastruttura. Secondo l'accordo, Vertiv fornirà Energy Savings as a Service (ESaaS, risparmio energetico come servizio) ai siti di rete core e di accesso di Telefónica presenti in Europa e in America, gestendo tutti gli aspetti, dalla valutazione iniziale del sito fino ai servizi di manutenzione completa per i prossimi dieci anni.

L'accordo prevede inoltre che gli esperti Vertiv conducano audit energetici e forniscano un'ampia gamma di report di valutazione contenenti previsioni sugli indicatori chiave di prestazione (KPI) e sul risparmio energetico di ciascun sito.

Includeranno anche una serie di raccomandazioni per ottimizzare le prestazioni, la capacità, la disponibilità e l'efficienza di infrastrutture critiche, al fine di aumentare il risparmio energetico. Vertiv garantirà un servizio di assistenza a 360°, dalla consulenza alla realizzazione di servizi di manutenzione e di monitoraggio 24 ore su 24, 7 giorni su 7, attività che non richiederanno alcuna spesa capitale (CAPEX) da parte del cliente. Vertiv sarà responsabile del finanziamento del progetto nell'ambito del contratto ESaaS.

«Telefónica è tra i più grandi fornitori di telefonia a livello mondiale e un'azienda Fortune 500, ed è anche uno degli operatori più attivi per quanto riguarda le iniziative di sostenibilità. Tutto ciò ci rende estremamente fieri di questa collaborazione", ha affermato Giordano Albertazzi, presidente di Vertiv in EMEA. "Questo accordo è un traguardo importante che rafforzerà la nostra partnership di lunga data e sottolinea la nostra costante dedizione nel fornire soluzioni all'avanguardia, caratterizzate da prestazioni elevate, ed efficienti sul piano energetico per il settore delle telecomunicazioni. Siamo impazienti di sviluppare questa nuova collaborazione incentrata sul risparmio energetico come servizio e di creare un valore forte e duraturo insieme a Telefónica».

Partner da oltre venti anni, Vertiv e Telefónica lavoreranno insieme per garantire un'ampia gamma di soluzioni innovative volte a supportare i siti della rete di Telefónica in tutto il mondo.

RED HAT AL TOP DEI GRADIMENTI PER IL CLOUD PUBBLICO

Red Hat Enterprise Linux

Secondo una recente ricerca, Red Hat Enterprise Linux risulta essere la piattaforma Linux commerciale preferita per il cloud pubblico

Nell'ultimo decennio Linux è diventato quasi uno standard de facto per la gestione di workload mission critical, e non solo nei data center aziendali. Nove dei dieci principali cloud pubblici, evidenzia in proposito Red Hat, si appoggiano su Linux e tutti i più importanti provider, da Amazon Web Services a Microsoft Azure, forniscono svariate distribuzioni Linux nei rispettivi marketplace.

Uno studio commissionato da Red Hat nel luglio 2017 ha evidenziato come Red Hat Enterprise Linux rappresenti la prima scelta di Linux commerciale sul cloud pubblico e soprattutto sia percepito come leader di mercato per l'implementazione di applicazioni, indipendentemente dal fatto che il workload sia in esecuzione in un data center o nel cloud.

I risultati del sondaggio, riporta ancora la società, indicano che le aziende scelgono Red Hat Enterprise Linux per il cloud pubblico per svariati morivi, tra i quali perché è ottimizzato per i loro workload, è certificato per un ampio ecosistema di casi d'uso aziendali e supporta una libreria di migliaia di applicazioni aziendali certificate

Il blind survey (condotto da Management Insight Technologies), ha esaminato in particolare quali siano le preferenze e le caratteristiche di un sistema operativo Linux nel cloud pubblico.

Più di 500 decision maker IT - impegnati in implementazioni cloud in tutto il mondo - hanno fornito un feedback che aiuta a tracciare un quadro più chiaro di come le organizzazioni utilizzino Linux nel cloud e in quali contesti la versione enterprise sia realmente valida.

Oltre a Red Hat Enterprise Linux, che è risultata essere la principale piattaforma Linux aziendale nel cloud pubblico, il sondaggio ha rivelato anche altri elementi interessanti:

- Oltre il 50% degli intervistati esegue le proprie applicazioni nel cloud pubblico su macchine virtuali Linux-based.
- Affidabilità, sicurezza, facilità di implementazione e manutenibilità sono le funzionalità chiave per le implementazioni Linux su cloud pubblico
- Il 65% delle implementazioni Linux nel cloud pubblico da parte delle imprese sono pagate e commercialmente supportate
- Il cloud in sostanza si evidenzia essere non più solo un banco di prova per gli sviluppatori e, dove vanno i workload aziendali, va anche Linux commerciale, in particolare la piattaforma enterprise.

SI AFFERMA SEMPRE PIÙ LA DIGITAL TRANSFORMATION

Un'azienda italiana su due ha realizzato progetti di digital transformation e ha migliorato il business. Lo evidenzia una ricerca Fujitsu

Bruno Sirletti - Fujitsu Italia

Fujitsu ha diffuso i risultati relativi al campione italiano coinvolto nella sua recente ricerca: The Digital Transformation PACT, che esamina le performance delle aziende nei confronti dei quattro elementi strategici necessari per potersi trasformare digitalmente: Persone, Azioni, Collaborazione e Tecnologia (PACT).

Il campione italiano, rappresentato da 150 business leader di tutti i settori industriali, ha evidenziato Fujitsu, ha sottolineato l'importanza della tecnologia digitale nel processo di trasformazione dei processi aziendali (40%) e del modello di business delle proprie organizzazioni (29%), indicando nelle 'Azioni' e nella 'Tecnologia' (28% in entrambi i casi) gli elementi principali su cui fare leva; 'Persone' e 'Collaborazione' sono indicati come elementi importanti rispettivamente dal 25% e dal 16% del campione.

Interrogati sul numero di progetti di trasformazione digitale, la maggioranza del campione nazionale (49%) ha dichiarato di aver già ottenuto dei risultati, mentre il 25% ha affermato che i progetti sono attualmente in fase di implementazione, ma i risultati non ancora disponibili.

Il campione italiano (per il 56% degli intervistati) ha messo in evidenza come nelle loro organizzazioni la tecnologia digitale venga utilizzata non solo a livello di processi e funzioni aziendali, ma anche per crearne di nuovi, da affiancare a quelli esistenti, non ancora digitali.

Una trasformazione guidata dai clienti

Principale driver della trasformazione digitale si confermano i clienti (per il 39% degli intervistati), seguiti a breve distanza da partner e terze parti (35%) e concorrenti (33%).

Passando all'aspetto economico e finanziario, dall'implementazione di progetti di trasformazione digitale le imprese italiane si aspettano di ottenere un ritorno dall'investimento entro un anno e mezzo e benefici organizzativi entro 16 mesi dalla data di partenza (a livello globale si parla rispettivamente di 20 mesi e un anno e mezzo).

Nonostante la focalizzazione sui risultati in tempi rapidi, le organizzazioni italiane non sono immuni da fallimenti o insuccessi, anche se questi accadono in misura minore rispetto alla media globale: solo il 27% (rispetto al 33%) delle organizzazioni italiane ha annullato progetti di trasformazione digitale, con una perdita media di 455.951 euro, e solo il 21% dei progetti digitali in Italia fallisce, anche se, sorprendentemente, il costo medio di questi progetti arriva a 559.984 euro.

«Le aziende italiane sembrano avere consapevolezza del loro livello di maturità digitale per affrontare progetti di trasformazione digitale» ha dichiarato Bruno Sirletti, Presidente e Ammini-

stratore Delegato di Fujitsu Italia. «I progetti vengono pianificati e implementati – alcuni con più successo di altri – ma la cosa importante è che le aziende abbiano chiaro che l'immobilità porta a un sicuro insuccesso, mentre la costante spinta all'innovazione tecnologica – a livello di processi, funzioni e non da ultimo organizzazione - è la strada che permetterà di continuare a competere nei prossimi anni».

Persone

Il gap di competenze interne è il principale ostacolo per affrontare la cybersecutity nella propria organizzazione: lo afferma il 68% del campione italiani. La buona notizia è che la maggior parte non sta a guardare: il 91% sta lavorando per attrarre più competenze digitali.. .

Ma l'aggiornamento non basta e diventa cruciale – per il 37% del campione - la capacità di saper attrarre e reclutare le persone. Secondo l'85%, entro il 2020 l'Intelligenza Artificiale (AI) inciderà sulla tipologia di competenze necessarie per la propria organizzazione, tanto che il 93% di essi si sta muovendo per far fronte a questa necessità e il 91% ammette che saper attrarre personale 'digitally native' sarà vitale per il successo della sua azienda nei prossimi tre anni.

Fondamentale una precisa strategia

La strategia è alla base del successo di un progetto di trasformazione digitale e il 92% del campione italiano dichiara di averne una ben definita, grazie anche al coinvolgimento diretto del top management (94%).

Si ammette però anche l'esistenza dei cosiddetti progetti ombra, quelli avviati senza un'approvazione organizzativa esplicita: per i quasi due terzi (62%) del campione costituiscono un serio problema per la loro organizzazione, anche se il 59% dichiara che spesso sono l'unico modo per provare ad ottenere un'innovazione significativa.

Collaborazione

La co-creazione sembra essere la chiave del successo di una azienda. In generale, le organizzazioni italiane sembrano aperte a un mondo collaborativo: il 58% sta implementando o sta pianificando progetti di co-creazione in cui lavorano a stretto contatto con un'altra organizzazione per fornire innovazione digitale. In questo caso, i partner preferenziali sono esperti di tecnologia, scelti dal 53% del campione, start-up (46%) o altre organizzazioni (45%), anche dello stesso settore (31%).

Tecnologia ad una svolta

Nei programmi degli intervistati, nei prossimi 12 mesi ci sono progetti che riguardano i sistemi di sicurezza informatica (59%), l'Internet of Things (51%) e il cloud computing (43%). Relativamente al tema della sicurezza informatica, il 95% afferma che questa sia fondamentale per supportare il successo finanziario della propria organizzazione nei prossimi 10 anni. In egual misura - 95% - vengono citati anche big data e analytics. In un panorama digitale in rapida evoluzione, la capacità di saper cambiare il proprio modello di business (87%) e pianificare l'impatto della tecnologia oltre l'anno (83%) è considerato cruciale per la sopravvivenza del proprio business nei prossimi cinque anni dall'84% del campione intervistato.

Si tratta di un percorso certamente non semplice e che desta più di una preoccupazione: il 61% degli intervistati teme che la sua organizzazione non saprà adattarsi all'implementazione di tecnologie digitali come l'Intelligenza Artificiale; il 78% ammette che i propri clienti si aspettano da loro un maggior livello di digitalizzazione e il 64% ritiene di essere in ritardo su questo punto rispetto alla concorrenza, tanto che per il 57% la trasformazione digitale nel proprio settore porterà una perdita di clienti.

IL GDPR È ALLE PORTE, ULTIMI AVVISI

Sta scadendo il tempo concesso alle aziende per mettersi in regola, ma i motivi dei ritardi sono in parte giustificati dalla complessità e dai costi per farlo

Parlare di Cloud e relativa sicurezza porta a considerare la situazione per quanto concerne la prossima entrata in vigore del GDPR. Fatte le debite proporzioni, quando si affronta il tema del GDPR oramai imminente (GDPR, General Data Protection Regulation) viene in mente la frase preoccupata di Tito Livio "Dum Romae consulitur, Saguntum expugnatur". E i dati, mutatis mutandis e proiettati ad oggi in relazione alle normative europee riguardo la riservatezza e la protezione dei dati sensibili, e le azioni da intraprendere per mettersi in regola, sembrano dare ragione al preoccupato Livio.

Gli obiettivi del GDPR (che sarà in vigore dal 25 maggio di quest'anno) sono semplici ma di non semplice attuazione. Riguardano la tutela e la uniformazione del trattamento dei dati personali all'interno dell'Unione Europea e sostituiscono la precedente Direttiva Comunitaria. Gli estensori del regolamento hanno anche voluto introdurre nuove disposizioni atte a snellire l'utilizzo e i flussi di dati personali tra gli stati membri dell'Unione e tra questi e i paesi extra-UE.

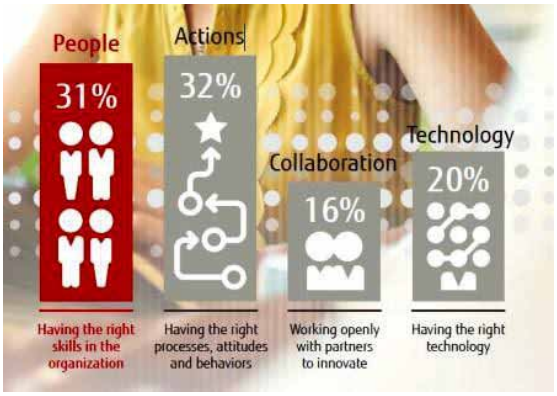
In sintesi l'obiettivo del GDPR è assicurare che coloro che gestiscono dati personali procedano nella raccolta, conservazione e trasferimento in modo corretto e responsabile. Peraltro, il regolamento ha anche l'obiettivo di ridurre le lungaggini burocratiche e così facendo dare la massima priorità ai diritti delle persone e alla sicurezza dei dati.

Il GDPR: una necessità giustificata dai fatti

Va osservato che qualcosa in proposito alla sicurezza e alla riservatezza dei dati andava fatto. Secondo dati contenuti nel rapporto Clusit 2017, l'Associazione Italiana per la Sicurezza Informatica, il 2016, e non è che quello da poco chiuso sia stato poi meglio, è risultato l'anno nero per la sicurezza informatica in tutto il mondo e tra le nazioni più colpite c'è stata anche l'Italia, che è risultata tra le prime dieci per quanto riguarda gli attacchi più gravi registrati e il numero di utenti colpiti.

Nutriti per la realtà italiana sono stati li attacchi ransomware, una tipologia di malware che cripta i file presenti sull'hard disk e poi chiede il pagamento di un riscatto all'utente per rimetterli in libertà.

La motivazione è semplice: le aziende nazionali sono risultate impreparate e dotate di limitate difese da questo tipo di cyber attacco e spesso hanno quindi dovuto obtorto collo abbozzare e porre mano al borsellino per poter avere di nuovo accesso a file importanti. La cosa preoccupante è che si è trattato di eventi che hanno coinvolto non solo privati o piccole aziende, ma anche enti



pubblici ed ospedalieri.
Il GDPR, che stringe le maglie della sicurezza, è quindi per molti aspetti un benvenuto perché mette di fronte a responsabilità e obblighi ben precisi.

La situazione delle aziende

A confermare però la sensazione di sostanziale ritardo nell'attuazione di quanto richiesto dal GDPR sono i dati riportati da IDC che indicano in un esiguo 3% la percentuale delle aziende con oltre 10 dipendenti che afferma di essere compliant, e in poco oltre il 40% quelle che hanno iniziato ad analizzare la cosa. Solo poco più del 50% ha affermato di avere un piano per la conformità. Rimane da capire cosa vuol dire avere un piano e quanto sia effettivamente efficace, perché, viene da dire, anche Napoleone la mattina di Waterloo un piano l'aveva. Ma i suoi avversari, nelle vesti di cyber hacker, ne avevano evidentemente uno migliore.
In altri settori altrettanto strategici e in particolare nel Manufacturing e nei Servizi la percentuale delle aziende che hanno iniziato di recente ad affrontare il problema è, anche se non di molto, superiore e pari rispettivamente al 53% e al 60%. Stante i dati riportati da IDC qualche raggio di sole riesce però a filtrare dalle nubi ancora abbastanza grigie. I settori strategici come il Finance e la PA si evidenziano sono quelli ove si ha un maggior tasso di compliance, rispettivamente con una percentuale del 10% e dell'8%, e anche con roadmap già definite per l'adeguamento con una rispettiva percentuale del 76% e dell'85%.
Il quadro generale di sostanziale ritardo, in alcuni settori e fasce di aziende anche molto forte, si conferma anche tra le aziende oltre i 250 dipendenti. Aspetto consolante, non solo italiane ma anche europee.

Il perché del ritardo

Viene spontaneo chiedersi a cosa sia dovuto. In proposito IDC ritiene che dipenda dalla percezione che hanno le aziende di come alcuni requisiti della nuova normativa siano vere e proprie sfide tecnologiche e organizzative. In particolare per la realtà italiana, oltre la metà delle aziende considera molto impegnativi i requisiti tecnici, ad esempio l'obbligo di segnalare quando si riscontrano perdite di dati entra tre giorni, il dover implementare soluzioni di crittografia o atte a rendere anonimi i dati nonché il dover definire casi d'uso specifici nella gestione del consenso.
Ma ci sono altri aspetti che riguardano l'organizzazione che risultano molto critici e sollevano perplessità da parte delle aziende e dei loro manager. Quelli che sono ritenuti costituire la sfida maggiore, con una percentuale oltre l 60%, sono inerenti la classificazione dei dati, la sensibilizzazione dei dipendenti ai cambiamenti nelle policy di sicurezza e il dover eliminare i dati irrilevanti.
Il motivo delle preoccupazioni è sostanzialmente di tipo economico e di certo non lo è a torto. Quelli da introdurre in azienda per ottemperare al GDPR sono cambiamenti importanti che comportano di certo dei costi significativi da affrontare. Implicano il dover creare nuovi processi documentali e intervenire e cambiar le modalità di comunicazione interna e di formazione, a cui si aggiunge quanto dovrà essere fatto in tema di Identity and Access Management, per la mappatura dei dati e l'aggiornamento dei processi di back-up.