Cloud & Business

n.71
Maggio 2018

LA RIVISTA PER IL MANAGER CHE DEVE OTTIMIZZARE COSTI E PROCESSI

IN QUESTO NUMERO

COVER STORY

LA CYBER SECURITY È IL PUNTO CHIAVE PER IL CLOUD

Un servizio cloud che sia trusted è una delle condizioni chiave per accelerare la trasformazione digitale di uffici e ambienti produttivi

La oramai universale o quasi adozione in toto o più di sovente come mix ibrido del cloud come modo veloce per testare nuove applicazioni e successivamente portarle in field senza proibitivi investimenti in Capex quando ancora non si è certi della risposta del mercato, presenta indubbiamente diversi problemi che vanno considerati. Quello che sembra essere il maggiore a chi si occupa dell'IT aziendale, concordano gli analisti e non è difficile essere d'accor-

Reportec Cloud&Business - Numero 71 - Maggio 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

do con loro, è che più ampio è il cloud, ibrido o multi-cloud che sia, il perimetro di esposizione ai rischi aumenta con ogni nuova applicazione scritta e rilasciata, sia che si tratti di qualcosa per uso interno che rivolta ai clienti.
Il progressivo svanire dei confini fisici di un'azienda e la diffusione crescente di architetture di cloud ibrido e multi-cloud, che contribuiscono nel rendere un confine ancor più evanescente di quanto già non fosse a seguito della crescente mobility, enfatizza all'estremo i rischi chi si corrono a causa di applicazioni che vengono progettate utilizzando metodologie consolidate ma sempre meno corrispondenti alle esigenze di sicurezza attuale e alle architetture su cui si estendono le applicazioni, con il rischio di esportare criticità nel cloud e allo stesso tempo, cosa ancor più critica, importarne.
E' uno scenario che fa intravedere come l'adozione progressiva del paradigma DevSecOps pssa costituire un presidio valido se non essenziale nella lotta contro i criminali informatici e per rispondere e bloccare i loro attacchi su e tramite cloud. In estrema sintesi, Development, Security e Operations dovranno essere considerati sempre più un tutt'uno omogeneo e inscindibile al fine di assicurare la sicurezza dei dati aziendali, dei processi e in definitiva del proprio business nel Cloud.

DevOps per la sicurezza delle applicazioni

Quando si parla di sicurezza si tende sovente a considerare quanto necessario a proteggere da attacchi dispositivi e dati quando invece la reale criticità e vulnerabilità finisce con il trovarsi nelle applicazioni stesse. Da qui quello che serve è sia una particolare attenzione nel loro sviluppo e da questo partire per definire poi il livello di sicurezza al loro contorno fisico e progressivamente sempre più virtuale: protezione dello storage e delle informazioni, dei punti anche fisici in cui sono conservate, degli end-point, eccetera.
La vulnerabilità delle applicazioni è all'origine, evidenziano ricerche in proposito, del 70-80% delle più gravi violazioni della sicurezza recentemente balzate agli onori della cronaca. Per questo motivo, il concetto di DevSecOps sarà un presidio essenziale nella lotta contro i criminali informatici. In estrema sintesi, Development, Security e Operations diventano un tutt'uno.
Applicare un approccio DevSecOps significa incorporare la sicurezza in ogni singolo passo del ciclo di sviluppo del software – dai primissimi stadi fino al testing e deployment, cosa che non può trascurare il fatto che la tentazione è sempre forte e per uno sviluppatore può essere semplice infiltrare contenuti potenzialmente dannosi nell'applicazione che sta scrivendo e la cosa può proiettare per anni a venire il proprio effetto. In questo senso, DevSecOps è un modo efficiente ed efficace per combattere il fenomeno, in quanto consente di far diventare la sicurezza una parte integrante dell'intero ciclo di sviluppo del software.

Le credenziali vanno protette e gestite

Non sempre sono però gli hacker o il programmatore che si è lasciato "indurre in tentazione" a provocare i peggiori attacchi alla sicurezza. All'origine di molti degli incidenti sono spesso proprio gli utenti interni, che per distrazione spalancano la porta ai pirati informatici.
Le tecniche utilizzate stanno diventando sempre più sofisticate sia dal punto di vista della destrezza degli attacchi, che appaiono così più legittimi, sia perché consentono al malware polimorfo (software nocivo, distruttivo o intrusivo che continua a cambiare) di installarsi e provocare gravi danni ai sistemi interni ed esterni. Per evitare conseguenti problemi e aumentare la fiducia nelle relazioni è opportuno dotarsi di

Le soluzioni di sicurezza si basano sul cloud per collezionare le informazioni inerenti i nuovi tipi di malware, elaborare e distribuire le contromisure

strumenti che consentano di gestire le credenziali dei dipendenti, in particolare di quelli privilegiati, ad esempio per revocarne rapidamente i privilegi di accesso bloccando eventuali username e password trafugati.

Il rischio per utenti privilegiati o meno arriva anche da dove meno uno se l'aspetta. Una ricerca di CyberArk Lab ha di recente esaminato i rischi che si corrono con quelli che riferisce come hot spot e cold spot e suggerito come intervenire per prevenire il furto di credenziali di account privilegiati

In particolare, la ricerca ha identificato gli "HotSpot" e i "ColdSpot" come le aree deboli di una rete in cui un attacco è più probabile. In media, osserva la ricerca, le organizzazioni hanno attivi 5,5 HotSpot, aree che sono prevedibilmente esposte ad attacchi e che agiscono da collo di bottiglia per dozzine di potenziali vettori di attacco alla propria rete in qualsiasi momento. Le organizzazioni hanno invece una media di 37 ColdSpot, consistenti in apparati che ospitano account privilegiati che possono essere target di attaccanti alla ricerca di spazi per infiltrarsi e scalare i privilegi.

Il problema che si evidenzia è che in complessi aziendali di una certa dimensione e dove le divisioni hanno libertà nell'attivarli, una sorta di shadow IT legalizzato, rilevare gli hot spot critici può non essere immediato, con il rischio di accorgersi di un danno una volta che è stato fatto. Per evitarlo e identificare in tempo reale gli Hot Spot attivi nel momento stesso in cui sono creati, CyberArk Labs ha ad esempio rilasciato PreCog, uno specifico strumento ottenibile dalla società.

Trasformazione digitale e sicurezza

La sicurezza è uno dei paradigmi cardine dell'attuale trasformazione digitale in atto. Ma come andrebbe affrontata a livello aziendale? Una visione più ampia del problema è stata data da Fujitsu nel corso del Fujitsu World Tour. Il tema centrale di una trasformazione digitale efficace e sicura, ha evidenziato Bruno Sirletti, Presidente e AD di Fujitsu della società per l'Italia, è la "Co-Creation", vista come la combinazione di partnership e competenze tecnologiche.

L'esigenza della co-creation deriva dalla considerazione che la tecnologia è una condizione necessaria ma di per sé non sufficiente per garantire una trasformazione digitale di successo. E viene da aggiungere sicura. Ci vuole altro, e ancor prima di parlare di tecnologia.

Il vulnus nel come si è proceduto sino ad ora risiede, ha osservato Sirletti, nel fatto che la trasformazione digitale ha avuto inizio con l'entrata sul mercato di aziende che hanno adottato

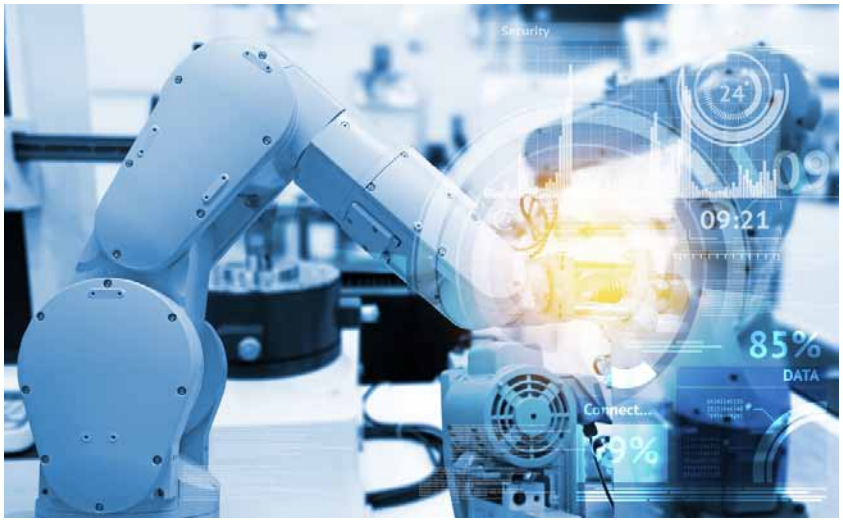
nuovi modelli di business abilitati dalla tecnologia che hanno permesso di realizzare cose nuove. Il loro successo ha portato le aziende tradizionali a imitarle, ma in buona parte dei casi quello che è stato fatto non aveva una reale corrispondenza alle reali esigenze delle aziende. E' mancato un approccio strategico, cosa che ha portato al fallimento di molti progetti.
Il fatto è che le aziende si aspettano di risolvere problemi concreti quali la globalizzazione, il mercato, le esigenze dei clienti, il time to market, la corrispondenza alle normative come nel caso del GDPR. In sostanza, in primis si deve partire dai bisogni e non dalla tecnologia, questa deve venire, certo, ma solo in un secondo tempo.
Ma come procedere? Quello che suggerisce Sirletti è di focalizzarsi su 4 elementi chiave: Persone, Azioni, Tecnologia, Collaborazione. E' solo con il loro corretto abbinamento e integrazione che un progetto può aver successo e rivelarsi produttivo e sicuro nell'immediato e nel lungo termine. In pratica, per concretizzare una digital transformation il focus sono le persone che comprendono il problema da risolvere e solo a quel punto può intervenire la tecnologia.

Verso l'Industry 4.0

Si è già evidenziato di come nel processo di digital transformation che sta interessando il mondo industriale la sicurezza sia uno dei punti chiave da affrontare e di come intervenga a livello informativo, progettuale, fisico, eccetera. Quello della globalizzazione e di una concorrenza sempre più agguerrita su scala planetaria, non è infatti l'unico dei problemi che le aziende impegnate nella produzione di beni materiali si trovano ad affrontare. A questi si aggiunge, e verrebbe da dire che piove sul bagnato, quello della sicurezza e in termini di cyber sicurezza Il 2017 è stato di certo un anno buio, osserva Stormshield, società focalizzata sulla protezione delle reti aziendali con soluzioni certificate EU RESTRICTED, NATO e ANSSI EAL4+.
La carente sicurezza dei sistemi industriali che tuttora si riscontra richiede l'adozione di misure appropriate, sia in termini di infrastruttura IT sia di integrità OT. E' un dato di fatto che la continuità del servizio, quando c'è di mezzo la produzione, è cruciale e il suo impatto risulta addirittura superiore a quello dei sistemi IT, poiché determinante per l'integrità di beni e personale addetto agli impianti.
L'assunto, quando si parla di sicurezza di impianti produttivi, è che il sistema informativo di un'azienda manifatturiera differisce da quello utilizzato in altri settori di mercato e le sue specificità richiedono dispositivi di protezione che integrino la logica legata al tipo di attività. Ne consegue che le tradizionali soluzioni multifunzione trasversali proposte sul mercato non sempre garantiscono il livello di sicurezza necessaria. Prima di avviare un progetto, le organizzazioni industriali dovrebbero in sostanza prendere in considerazione questi vincoli specifici e rivolgersi a specialisti del settore e a partner tecnologici e di canale.
Quello che può essere di aiuto, suggerisce l'azienda, è in ogni caso elaborare un progetto in maniera unificata, che ha il risultato di semplificare la gestione dei sistemi impiegati (in particolare in termini di amministrazione delle soluzioni).

Relazioni trusted e IIoT sicuro sono la base per l'Industry 4.0

La necessità di sinergie e la peculiarità del mondo industriale è anche il motivo per cui ultimamente si assiste allo sviluppo di un intero ecosistema imperniato sulla protezione dei sistemi informativi industriali. Sono nate alleanze tecniche e commerciali tra operatori complementari, che unendo le proprie forze hanno sviluppato sistemi ad alto valore aggiunto frutto della combinazione di soluzioni, integrazione, consulenza, formazione.



Relazioni trusted e IIoT sicuro è la base per l'Industry 4.0

Cloud e sicurezza

Nel considerare il tema della sicurezza entra prepotentemente in campo come punto chiave già accennato il cloud, sia come fattore di criticità che di business. Nel processo di trasformazione digitale, osserva Philippe Courtot, CEO di Qualys, l'uso del cloud computing congiuntamente a mobility, IoT e alle altre nuove tecnologie che rendono le aziende più innovative, agili e flessibili, diventa un requisito competitivo per la crescita.

Il processo è ampio e coinvolge anche gli enti governativi, che stanno ampliando le normative e in particolare quelle che incrementano la sicurezza e la privacy dei dati dei propri cittadini, e in primis la General Data Protection Regulation (GDPR). La convergenza di queste tendenze oggi impone alle organizzazioni di accelerare i propri processi di trasformazione digitale e di ripensare la sicurezza, affinché sia realmente integrata. La chiave di volta, o perlomeno una delle principali, ritiene Qualys, può essere trovata in architetture e soluzioni basate su cloud, che automatizzano e valutano costantemente entrambi gli aspetti legati a sicurezza e rispetto della conformità negli ambienti on premise, per gli endpoint e nelle strutture cloud pubbliche e private su larga scala.

E' indubbiamente un compito complesso poiché le iniziative legate alla trasformazione digitale introducono applicazioni e servizi web nuovi e in continua evoluzione, che generano, raccolgono e analizzano enormi quantità di dati dei clienti. La completa visibilità degli ambienti IT ibridi – on premise, in cloud e degli endpoint mobili – diventa quindi di primaria importanza per consentire alle aziende di monitorare e proteggere in modo costante queste risorse IT, per gestire i rischi e la compliance.

Una architettura cloud adeguata consente ad esempio di identificare gli asset distribuiti in qualsiasi ambiente ibrido, utilizzando agenti e scanner leggeri (attivi e passivi), tutti oggetti che raccolgono automaticamente e in modo continuo i dati provenienti da dispositivi IT, di sicurezza e di conformità e li inviano alla piattaforma per consentirne l'analisi in tempo reale.

Il fatto è che il consolidamento di tutti i componenti IT, osserva Courtot, è diventato un imperativo per CIO e CISO, in quanto non possono continuare ad aggiungere sicurezza e soluzioni di conformità in base a nuovi ambienti e normative. Grazie a soluzioni che abilitano le integrazioni a livello nativo della security aziendale con i principali provider di cloud pubblico, osserva il manager, diventa però possibile realizzare ambienti ibridi e multi cloud e disporre di suite di applicazioni in cloud integrate e dotate di self-update in grado di soddisfare le nuove esigenze imposte dalla normative, tutto fornibile da un'unica piattaforma che dà la visualizzazione da un singolo pannello per CIO, CISO, team di sicurezza e auditor di compliance.

DEDICATED CLOUD ACCESS DI COLT DISPONIBILE PER GOOGLE CLOUD

Grazie alla Colt IQ Hybrid Network il servizio Colt Dedicated Cloud Access permette di connettersi alla piattaforma di Google Cloud

Colt Technology Services ha annunciato il supporto di Google Cloud Partner Interconnect, un servizio di Google Cloud che permette ai clienti di connettersi da qualsiasi luogo alla piattaforma Google Cloud.

Google Cloud Partner Interconnect è, nello specifico, un nuovo prodotto di Google Cloud Interconnect. Lo scorso settembre, Google aveva annunciato Dedicated Interconnect, che fornisce una connettività veloce a costi inferiori rispetto alla VPN ed è diventata nella proposta della società la soluzione ritenuta ideale per connettere i data center on-premise al cloud.

Peter Coppens - Colt Technology Services

«Partner Interconnect offre ai clienti di Google Cloud maggiori possibilità di scelta per quanto riguarda la connettività in ambienti ibridi. Insieme a Colt vogliamo facilitare i clienti nell'estendere la propria infrastruttura on-premise alla piattaforma Google Cloud», ha dichiarato John Veizades, Product Manager di Google Cloud.

In sostanza, sfruttando il servizio Partner Interconnect è possibile affidarsi a Colt per collegare le proprie piattaforme applicative al Google Cloud più prossimo, con tagli di banda che vanno da 50Mbps fino a 10Gbps.

«Il servizio Colt Dedicated Cloud Access fornisce ai clienti una connettività di rete verso i servizi Google Cloud privata sicura ed affidabile», ha commentato Peter Coppens, Vice President Product Portfolio di Colt Technology Services. «Colt Dedicated Cloud Access offre alle aziende un'esperienza di cloud networking superiore rispetto a quella offerta dalla rete internet pubblica. Questo permette di creare un ambiente cloud agile e on-demand, di vitale importanza nell'iter di trasformazione digitale dei clienti».

Il rilascio del nuovo servizio fa parte della strategia di Colt volta a far divenire l'operatore una società di riferimento nel settore telco nell'abilitare la trasformazione digitale delle aziende tramite soluzioni flessibili, on demand e a banda larga. La rete Colt IQ Network collega oltre 800 data center in Europa Asia e nei principali hub del Nord America, con oltre 25.000 edifici on-net.

SERVIZI F5 PER AMBIENTI MULTI-CLOUD SICURI

Maurizio Desiderio - F5 Networks

BIG-IP Cloud Edition fornisce i servizi applicativi per l'implementazione, la gestione, l'orchestrazione e l'automazione delle applicazioni

F5 Networks ha rilasciato BIG-IP Cloud Edition, una soluzione che ha l'obiettivo di consentirà alle aziende di implementare rapidamente servizi applicativi critici e indipendentemente dall'ambiente.

BIG-IP Cloud Edition è offerto sotto forma di Application Delivery Controller (ADC) virtuale, per-app, che può applicare e automatizzare i servizi basati su policy nelle varie fasi del processo di sviluppo e produzione di una applicazione.

E' un approccio, ha osservato Maurizio Desiderio, country manager per Italia e Malta, che abilita una più facile integrazione con ambienti NetOps, DevOps e SecOps all'interno di un framework che permette di migliorare le performance, la disponibilità e la sicurezza delle applicazioni. Come piattaforma combina il portfolio di servizi applicativi di F5 con le capacità potenziate in termini di analitiche, visibilità e gestione di BIG-IQ. La soluzione, software-based, permette in sostanza di aggiungere agli esistenti servizi 'su misura', personalizzati per le applicazioni individuali, gli ambienti di cloud composito e per richieste specifiche degli utenti. Ad esempio, permette di implementare policy di Advanced Web Application Firewall per gestire minacce sofisticate alle applicazioni in modo coerente nei cloud pubblici e privati.

«Ben poco è cambiato in un anno nell'IT. Il focus rimane sempre sulla sicurezza e come garantirla. Ma quello che si conferma fondamentale è proteggere le applicazioni. E per farlo non basta più proteggere i confini fisici dell'IT ma bisogna partire dal contesto e operare su una realtà virtuale che si estende sino al multi-cloud. E questo è proprio quello che le soluzioni di F-5 permettono di fare», ha commentato Desiderio.

Ampia la dotazione di funzioni di BIG-IP Cloud Edition. Tra queste:

- Servizi e protezione "software based" di classe enterprise.
- Servizi applicativi dedicati e su misura per app indipendentemente dall'ambiente.
- Catalogo self-service dei servizi applicativi per provisioning, configurazioni e aggiornamenti.
- Visibilità per-app, analisi e scalabilità automatica.

Quello di rendere i servizi più accessibili per le applicazioni è solo uno degli obiettivi di BIG-IP Cloud Edition. Altre a questo, ha spiegato la società, la possibilità che fornisce di implementare, aggiornare e automatizzare servizi collaudati di F5 su base per-app aiuta i NetOps a sostenere le priorità di business in cooperazione con i SecOps e i DevOps. In particolare, nel suo sviluppo attenzione è stata posta alle operazioni collaborative e al self-service da parte dei team di sviluppo delle app, Non ultimo, ha poi evidenziato l'azienda, dashboard dedicate forniscono visibilità, analisi e controlli per-app che semplificano le operazioni e migliorano la gestione e l'orchestrazione.

CON FORCEPOINT LA PROTEZIONE DEL DATO È DINAMICA E ARRIVA DAL CLOUD

Forcepoint Dynamic Data Protection monitora e rafforza il controllo dinamico e protegge i dati in base a livelli di rischio che caratterizzano utente e dati

Heath Thomson - Forcepoint

Il problema della prevenzione della perdita dei dati (DLP: Data Loss Prevention) è sempre più stringente ed è un'esigenza generale e trasversale a tutte le tipologie di aziende e di settori enfatizzata dal prossimo entrare in vigore del nuovo regolamento europeo sulla sicurezza e protezione dei dati.

Quello della protezione del dato, osserva Heath Thompson, Executive VP per i prodotti di Forcepoint, è un settore dove sempre più si fa ricorso a metodologie di cybersecurity di tipo human centric, in modo da adattare la protezione di dati e utenti in base al loro comportamento e all'interazione tra le entità, sistemi e dati.

Quello del ricorso a soluzioni basate sul comportamento umano ha poi avuto una ulteriore espansione, osserva il manager, con l'integrazione tra DLP e CASB (Cloud Access Security Broker), cosa che ha permesso non solo di meglio ritagliare una soluzione in base alle esigenze dell'utente e del contesto ma anche di rispondere all'evoluzione strategica sul modo di come viene fruito in azienda l'IT.

Il problema, osserva però Thompson, è che la maggior parte se non tutte le soluzioni DLP sul mercato bloccano o permettono un'azione basandosi su insiemi statici di policy predefinite. In sostanza il comportamento è del tipo "Permetti" o "Blocca" e vi è la mancanza di un meccanismo flessibile che permetta di gestire le eccezioni. E la frustrazione che si sperimenta quando non si riesce a gestire una eccezione porta un amministratore di sistema a disabilitare le regole stabilite o a perdere fiducia nella tecnologia.

Per bypassare proprio queste critiche situazioni Forcepoint ha rilasciato Forcepoint Dynamic Data Protection, che ha l'obiettivo primario di mettere in grado di monitorare e rafforzare il controllo dinamico, e di proteggere i dati in base a livelli di rischio comportamentale da parte dell'utente e del valore dei dati coinvolti.

Tra gli elementi chiave della soluzione va annoverato:

- Sistema per la collezione dei dati dagli endpoint
- Utilizzo dei dati in accordo a un modello comportamentale flessibile e dinamico.
- Determinazione di un punteggio di rischio assegnabile ad un utente.
- Punteggio di rischio correlabile a un livello di rischio da 1 a 5.
- Possibilità di assegnare un piano unico di protezione dei dati ai differenti livelli di rischio e per singolo utente.
- Rivalutazione nel tempo del punteggio e del livello di rischio, che può essere alzato od abbassato in base ai cambiamenti intervenuti nel comportamento umano.

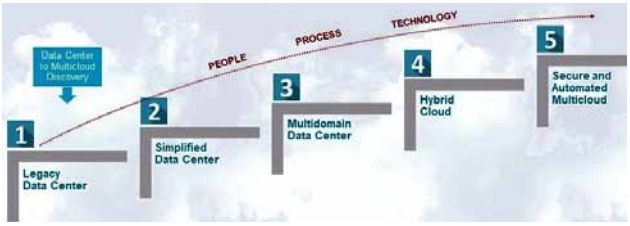
JUNIPER NETWORKS RILASCIA CONTRAIL ENTERPRISE MULTICLOUD

La piattaforma per l'orchestrazione e le analytics multicloud semplifica il percorso delle aziende verso un ambiente multicloud sicuro e automatizzato

Juniper Networks ha annunciato l'ampliamento di Contrail Enterprise Multicloud con servizi atti a consentire un maggior controllo e una gestione delle policy per qualsiasi workload in ambienti di rete fisici e virtuali, qualsiasi cloud e ambiente multivendor. Il problema, spiega la società, è che la maggior parte delle aziende deve affidarsi a due o più controller o sistema di gestione per gestire overlay, underlay e dispositivi di rete.

Le nuove funzionalità di orchestrazione e analytics multidominio di Contrail Enterprise Multicloud sono state sviluppate, ha spiegato la società, per eliminare questi vincoli e dare alle aziende la possibilità di gestire e monitorare qualunque workload da un unico centro di comando. In pratica, gli ambienti che utilizzano molteplici ambienti cloud (pubblici, privati o entrambi) dispongono di una soluzione di orchestrazione delle policy costruita su una piattaforma omogenea e con un unico punto di controllo. Tra gli elementi salienti della soluzione:

- Orchestrazione e visibilità multicloud: funzionalità di gestione delle policy e controllo end to end che permettono agli utenti di disporre di un singolo strumento per orchestrare la gestione di server, dispositivi di networking, contanier e macchine virtuali e gestire la sicurezza.



- Migrazione multicloud in 5 fasi: è un framework di migrazione multicloud in 5 fasi che consiste in una metodologia che permette di definire un proprio percorso personalizzato verso il multicloud, indipendentemente da quale sia il punto di partenza. Il framework considera gli aspetti architetturali, i prodotti, gli strumenti, i processi e le persone.
- Progettazione della infrastruttura: è un bundle che combinano gli switch QFX Series con Contrail Enterprise Multicloud e servizi professionali di supporto all'implementazione.
- Servizi professionali: sono servizi volti a supportare una realizzazione veloce e affidabile dell'infrastruttura tramite strumenti chiavi in mano per l'implementazione della rete e l'automazione dei test.

«Operare in un mondo multicloud non significa solo connettività ma anche un'infrastruttura invisibile agli utenti. Con lo spostamento dei workload su cloud, le aziende necessitano di un'architettura unica e coesa con funzionalità di gestione e visibilità end to end. Raggiungere questo obiettivo è un processo lungo e complesso. Sfruttando Contrail Enterprise Multicloud come abilitatore multicloud end-to-end, le aziende ora dispongono di un'unica piattaforma per la gestione di overlay e underlay, ambienti di calcolo eterogenei, inclusi server bare metal, macchine virtuali, contenitori e dispositivi di rete, cloud privati e pubblici, orchestrazione delle politiche di rete e di sicurezza e analytics avanzate», ha commentato Bikash Koley, CTO di Juniper Networks.

UN RETAIL AL TOP CON WAN OTTIMIZZATE

I servizi per reti software defined, di gestione IT e di ottimizzazione dei siti Web permettono di realizzare infrastrutture multi-cloud che spingono il business del Retail

Massimo Leonarda - Purple Ocean

Rispondere alle esigenze delle aziende e dei diversi settori industriali e del commercio richiede non solo creatività ma anche una forte esperienza e competenza ingegneristica in grado di coniugare in un progetto quanto necessario sotto il profilo dell'infrastruttura e della topologia di rete, con le applicazioni business, la gestione, la messa a punto, l'installazione e, qualora richiesto dal cliente, la gestione.

E' quanto mette a disposizione dei clienti Purple Ocean, un'azienda nata otto anni fa dalla vision del suo CEO Massimo Leonarda che, anticipando i tempi del Cloud e dell' "as a Service" ha messo a fattor comune le conoscenze maturate nel settore delle infrastrutture di rete geografica e del software applicativo e che con la combinazione delle due cose ha creato un portfolio di servizi centrato sui tre pilastri fondanti dell'attuale economia globale alle prese con la trasformazione digitale:

- Servizi per lo sviluppo e la gestione di infrastrutture di rete geografica, cloud ibrido incluso.
- Soluzioni e piattaforme per l'e-Commerce per aziende di ampia dimensione e fortemente e capillarmente distribuite sul territorio.
- Soluzioni per la misurazione proattiva della Quality of Experience degli utenti di un portale web

Negli otto anni trascorsi dalla sua costituzione, ha osservato Leonarda, la società ha accumulato con il suo team che ad oggi annovera circa 20 persone, in larga parte specialisti, una solida esperienza nei servizi infrastrutturali e nel retail.

«All'interno di Purple Ocean abbiamo sempre avuto due anime. Una è legata ai servizi infrastrutturali e alla gestione di infrastrutture complesse dove operiamo come managed service provider con logiche di business severe che comprendono l'H24, il monitoraggio proattivo, il rispetto degli SLA, le KPI, il tutto con competenze che spaziano dalle reti allo storage e ai sistemi di elaborazione. La seconda è relativa al mondo dello sviluppo software, dove operiamo su input del cliente o su nostri progetti, ad esempio nel settore dell'e-Commerce, dove abbiamo accumulato una forte esperienza sia per quanto concerne la parte tecnica che quella connessa al workflow», ha evidenziato Leonarda.

Un sito di qualità aumenta il business

Quella delle infrastrutture e dei servizi è un'anima che è stata poi integrata da una terza costituita da soluzioni sviluppate a seguito sia di esigenze interne nate nel corso degli sviluppi software che

da input dei clienti alle prese col problema di ottimizzare siti web o di e-Commerce.
«Quella della ottimizzazione di siti web è una nostra terza anima che comprende una piattaforma, PurpleX, in fase di brevetto, che forniamo come soluzione SaaS che permette di misurare la qualità della navigazione dell'utente su un sito web o un e-commerce. Si basa su automi che attivano dei browser ed emulano il comportamento di un utente rilevando, durante la navigazione, eventuali problemi di carattere tecnico dalla mancanza di immagini, link interrotti, errori javascript a problemi di tipo prettamente editoriale ma di impatto negativo sull'utente», ha osservato Leonarda.
Servizi di SD WAN per aziende e retail
Quello delle reti è un settore che ha visto Purple Ocean impegnata sin dalla sua nascita, settore dove ha portato i concetti innovativi e i nuovi paradigmi rappresentati dal software defined networking.
Il suo impegno risale al 2015 quando ha avviato la ricerca sul mercato di una soluzione da proporre ai clienti che permettesse di affrontare in modo del tutto nuovo, flessibile e aperto il problema di ridefinire le proprie reti geografiche, soprattutto con l'esigenza di fruirne sia in abbinamento a architetture di cloud ibrido che multi-cloud.
«Nel 2015 abbiamo proceduto ad una attenta selezione delle offerte sul mercato e alla fine abbiamo identificato in quella sviluppata da Viptela una piattaforma che si è dimostrata particolarmente adatta per le reti geografiche e in linea con la nostra proposizione di servizi e soluzioni per aziende e il retail. E' una soluzione che permette di orchestrare WAN di ampie dimensioni, come ad esempio quella che abbiamo realizzato per un nostro cliente retail, con centinaia di siti, e gestire in maniera semplice quello che sino ad ora era molto complesso», ha spiegato Leonarda.
In pratica, la piattaforma Viptela integrata dai servizi Purple Ocean permette di realizzare una software defined WAN che disaccoppia la parte fisica di trasporto, Il data layer ottenibile da un comune carrier, dalla parte software di gestione e orchestrazione delle risorse, il control plane. Il risultato è che si ha la possibilità di vedere in profondità come si comporta la rete, adattarla automaticamente alle esigenze delle applicazioni, gestire i flussi in modo ottimizzato e ritagliarvi sopra quello che va sotto il concetto di overlay network, ovverosia reti virtuali separate per funzioni o utenti che però fruiscono dei medesimi canali trasmissivi. Varie le modalità con cui è possibile fruire dei servizi di Purple Ocean.
«Il nostro intervento a supporto del cliente può essere molteplice e parte dal fatto che già operiamo come managed service provider. A questo, se il cliente lo desidera, possiamo aggiungere anche la gestione della soluzione e farci carico dell'operation. Se invece il cliente ha già una struttura che vuole mantenere possiamo operare come professional services e affiancare il cliente nel progettare la soluzione di SD WAN e fornire sessioni di formazione per rendere autonomo il suo team», ha spiegato Leonarda.

TREND MICRO E F5 METTONO RETI E DATI AL SICURO

La complementarietà delle offerte delle due aziende abilita l'analisi e il controllo del traffico crittografato e una risposta all'l'80% delle esigenze di security

La digital transformation è un dato di fatto che sta profondamente modificando il modo di essere presenti sul mercato e di produrre e che offre un concreto beneficio al business ma, rovescio della medaglia, facendo svanire le barriere fisiche che sino ad ieri proteggevano le aziende apre ampi spazi per attacchi alle applicazioni e ai silos di dati, sino a coinvolgere ambienti industriali e infrastrutture critiche .

Una risposta, evidenzia Renaud Bidou, Technical Director Southern Europe di Trend Micro, si è cercato di darla facendo un crescente ricorso alla crittografia ma anche con chiavi di cifratura di lunghezza crescente e algoritmi sofisticati, di reti private e quanto la tecnologia ha reso disponibile, si è scoperto che i cyber criminali riescono lo stesso a farsi strada e a penetrare le difese poste in atto.

La crittografia, è vero, garantisce la riservatezza dei dati scambiati su una rete aziendale, ma può essere anche manipolata per impedire il rilevamento di azioni dannose e un attaccante può stabilire un canale di comunicazione illegittimo e, tramite vettori, estrarre informazioni dai dispositivi di rete e in rete senza essere rilevato. E la cosa può andare avanti per settimane o mesi prima che qualcuno se ne accorga.

In questo contesto, Trend Micro, leader globale nelle soluzioni di cybersecurity, annuncia una partnership con F5 Networks, leader nella delivery delle app, ovunque e in sicurezza..

Esperienze complementari per una sicurezza a 360°

E' a questa situazione critica che si è proposta di dare una risposta la partnership tra Trend Micro e F5, le cui esperienze e soluzioni sono complementari e che nell'insieme, evidenzia Trend Micro, sono in grado di dare una positiva risposta ad oltre l'80% delle esigenze di sicurezza di una rete e di una infrastruttura IT, compreso quanto attinente ai sempre più diffusi ambienti IoT e Industrial IoT

Ma quali sono gli elementi chiave su cui si deve basare una strategia per contrastare attacchi sempre più pericolosi? .I punti chiave, e pilastri della sua vision, nell'affrontare e contrastare gli attacchi alla sicurezza - ci ha illustrato Bidou - sono essenzialmente tre. soluzioni ibride; artificial intelligence e analytics; Interconnection.

In sostanza, si tratta di disporre di un sistema di sicurezza distribuito su tutti i livelli di una infra-

struttura IT, da quella fisica a quella applicativa, cloud ibrido o multi-cloud incluso, che tramite l'analisi comportamentale e evoluti analytics permetta di individuare al loro insorgere le deviazioni da comportamenti normali sia della rete che degli utenti e delle applicazioni , ed intervenire automaticamente incapsulando il dispositivo, l'applicazione o l'area di rete interessata impattando il minimo possibile sul restante IT.

Naturalmente, osserva Bidou, se è complesso intervenire in un normale ambiente IT, più complesso è proteggere adeguatamente una infrastruttura industriale che sia evoluta verso l'IIoT, perché in questo caso si aggiungono due fattori ulteriori che devono essere gestiti: il primo è il fatto che in molto ambienti sono in esercizio soluzioni SCADA e quindi vanno gestiti prodotti di generazione anche datata e nativamente insicuri, il secondo è che la risposta a un attacco deve essere rapidissima perché in molte industrie non si può accettare il fermo macchina o di un impianto nemmeno per pochi secondi.

«In un tale scenario un ruolo chiave nel garantire la protezione, oltre a considerare il contesto, lo ha sempre più il modo di sviluppare le applicazioni e il come è organizzato il DevOps, che si avvia ad essere l'approccio obbligato per una sicurezza a prova di hacker», ha osservato Bidou.

Traffico crittografato e protetto

La partnership tra Trend Micro e F5 Networks si propone, per quanto concerne l'infrastruttura di trasporto e di rete, di abilitare l'analisi e il controllo in profondità del traffico crittografato, a partire dai canali dedicati al Command & Control (C&C), fino al rilevamento degli Advanced Persistent Threat (APT) e, in particolare:

- Intercettare ed analizzare il traffico SSL in uscita, effettuato tramite la combinazione di SSL Orchestrator di F5 Networks con Trend Micro Deep Discovery Inspector). In pratica, i flussi in uscita vengono crittografati in modo da rendere complessa la loro analisi. L'orchestrator decritta poi il traffico SSL e lo trasferisce a Trend Micro Deep Discovery Inspector per l'analisi e la notifica di azioni sospette.
- Scansione dei file, realizzata tramite la combinazione delle soluzioni Big IP di F5 Networks e di Trend Micro Deep Discovery Analizer. Big IP (con funzione di Load Balancer) invia a Trend Micro Deep Discovery Analizer i file in transito, per un'analisi del contenuto dinamico in una sandbox, ad esempio un documento caricato su un'applicazione Web o trasmesso tramite un'API. Qualsiasi contenuto dannoso, sia esso un file, una macro o un URL contenuto in un file, viene bloccato da Deep Discovery Analizer, blocco che protegge il server di destinazione da qualsiasi infezione.

«Attraverso l'integrazione delle tecnologie Trend Micro e F5 Networks, le aziende possono ora sfruttare il meglio dei due mondi: proteggere la privacy dei dati implementando la crittografia all'avanguardia e garantendo la sicurezza del traffico sia in entrata che in uscita», ha commentato Alessandro Fontana, System Integrator Alliance Manager Trend Micro Italia.

CYBERARK TRA GLI INNOVATORI NELLA LISTA CYBERSECURITY 500

La società per la sicurezza informatica è stata inserita tra quelle più innovative nella sicurezza degli accessi privilegiati e al terzo posto complessivo

CyberArk ha annunciato di essere stata inclusa nella Cybersecurity 500 list, l'elenco preparato da Cybersecurity Ventures che identifica le società di cybersecurity operanti in diversi campi e aree dell'IT, hardware e software, a livello mondiale e da osservare con attenzione nel corso del 2018. Peraltro, non si tratta per l'azienda dedita alla sicurezza degli accessi e degli utenti privilegiati solo di esserci nella lista, ma anche di come c'è e viene quotata.

La società, infatti, è valutata al top tra i Fornitori di soluzioni di cyber security e in particolare al primo posto per quanto concerne le soluzioni di sicurezza per utenti privilegiati e al terzo posto complessivo. Dopo di lei si qualificano nomi importanti nella security.

L'elenco, ha evidenziato CyberArk, che non nasconde la soddisfazione per il valore e la posizione che le è stato riconosciuto, è stilato in base a criteri che comprendono la capacità di indirizzare e rispondere in modo innovativo alle sfide inerenti la cybersecurity che le aziende si trovano a dover fronteggiare, la base di clienti a portfolio, il parere dei CISO e dei decision maker, il trend di crescita della società e la robustezza e capacità in termini di leadership.

Il settore della sicurezza è in ogni caso in continua crescita e fermento e il motivo è facilmente comprensibile se si guardano le cifre in gioco.

Secondo l'Official 2017-2018 Cybercrime Report realizzato da Cybersecurity Ventures, il cyber crime avrà un costo annuale a livello mondiale pari a 6 trilioni di dollari entro il 2021, e questo a partire dai 3 trilioni di dollari del 2015, un raddoppio in soli 6 anni e allo stesso tempo una cifra che rende il settore persino più profittevole del traffico globale di droga.

L'interesse dei malintenzionati, che esprimono l'intenzione di aumentare il proprio "fatturato" deve indurre le aziende a dotarsi di difese in profondità e di una strategia che permetta di stare innanzi a quelle di cui si possono dotare gli attaccanti in modo da proteggere i propri asset rilevanti. In breve, prevenire prima di dove pensare, in modo oneroso, a reprimere.

«Di certo è un onore essere stati qualificati assieme ad altri innovatori come Herjavec Group e KnowBe4 e di sicuro è un riconoscimento che ci fa molto piacere. Ed è il riconoscimento che soluzioni come CyberArk Privileged Access Security Solution costituiscono una piattaforma di sicurezza che permette di implementare un livello critico in grado di proteggere dalla continua evoluzione degli attacchi contro le credenziali degli utenti e informazioni riservate sia in ambito cloud che in ambienti DevOps, e a livello degli end-point privilegiati», ha commentato Amy Burnis, Senior Manager, Marketing Communications di CyberArk.

ENTER DIVENTA MEMBRO DEL CISPE

Mariano Cunietti - Enter

Uno status europeo per Enter, che entra nel novero dei big della grande alleanza cloud in Europa per la protezione dei dati

Enter ha comunicato di essere diventata ufficialmente membro del CISPE (Cloud Infrastructure Services Providers in Europe), l'associazione dei provider di servizi cloud che operano in Europa.
Ente, che è annoverata tra i maggiori Internet Service Provider in Italia ed attiva dal 1996, è fornitore ufficiale di servizi cloud per la UE grazie alla sua Enter Cloud Suite e nel 2013 Enter ha creato Login, un grande spazio di coworking tecnologico a Milano.
Il CISPE è l'associazione dei provider di servizi cloud che operano in Europa. All'associazione possono partecipare tutte le aziende, indipendentemente da dove è ubicata la loro sede centrale, purché dichiarino che almeno uno dei loro servizi di infrastruttura cloud soddisfa i requisiti del codice di condotta sulla protezione dei dati dell'associazione. L'accoglimento di Enter come membro del CISPE è un riconoscimento che ha come prodromi l'anno 2017, anno in cui il provider italiano ha aderito al codice di condotta CISPE sulla protezione dei dati, un marchio di conformità che stabilisce gli standard e le pratiche per proteggere i dati dei clienti e rispettare le leggi europee sulla protezione dei dati.
Enter si è così aggiunta agli attuali membri del CISPE, aziende che operano in oltre 16 Paesi europei tra cui Francia, Germania, Italia, Irlanda, UK, Finlandia, Svezia, Paesi Bassi, Spagna, Bulgaria, Polonia, Svizzera.
«Diventare membri del CISPE significa essere tra coloro che definiranno il primo standard di sicurezza dei dati personali nel cloud basato su una reale esperienza di mercato, e non su un'astrazione. Avremo modo finalmente di dar voce e risposte alle reali esigenze di sicurezza dei clienti, non solo alle paure», ha commentato Mariano Cunietti, CTO di Enter. «Enter Cloud Suite è un servizio che è stato interamente progettato con la normativa UE in mente, fin dall'inizio nel 2013. Quando l'UE nel 2015 ci ha nominato come fornitore IAAS pubblico ufficiale per le sue 52 istituzioni, abbiamo capito che essere di supporto alla normativa UE è la chiave per essere competitivi in questo mercato».
Enter Cloud Suite, ha continuato Cunietti, è il primo servizio europeo multi-region IaaS basato su OpenStack distribuito in differenti Paesi (Italia, Germania, Olanda), costruito per le aziende e gli sviluppatori europei.
Si basa su un'infrastruttura di rete proprietaria, un backbone Carrier Ethernet a 10 Gbps connesso a 5 POP internazionali (Milano, Francoforte, Amsterdam, Londra e Parigi) e, in quanto tale abilita il controllo su tutto lo stack di rete e elevati livelli di performance e di servizio per gli utilizzatori.
Comprende servizi di computing, storage e networking as a service, oltre a servizi avanzati di CDN (Content Delivery Network) e di DNS dinamico per il balancing e il failover geografico.

DATA DRIVEN E CLOUD NELLA VISION DI HITACHI VANTARA

Hitachi Vantara ha illustrato i risultati dell'anno fiscale appena chiuso e la strategia per un IT data centric al servizio delle aziende e pronto per il futuro

Marco Tesini - Hitachi Vantara

La digitalizzazione è al centro di una rivoluzione su scala globale ed è una realtà da cui non solo non ci si può esimere ma che è sempre più considerata centrale da parte del management delle aziende nel definire la propria vision strategica in termine di soluzioni, prodotti e go to market. E centrale nel processo di digitalizzazione è il "dato", sia che si tratti di dato strutturato o non strutturato. E' questo che è alla base della strategia e della vision di Hitachi Vantara e dei risultati estremamente positivi ottenuti nel suo ultimo anno fiscale chiusosi a fine marzo, ha evidenziato Marco Tesini, CEO della società per l'Italia.

Prepararsi per le trasformazioni richieste alle aziende, sia che si tratti di società di servizi che di produzione di beni materiali, più che una opportunità sembra essere sempre più un obbligo.

E i tempi per farlo sono sempre più stretti, osserva il manager alla guida della società da due anni e che l'ha portata a crescere in termini di mercato e fatturato, perché se la pervasività del dato rappresenta già in sé una rivoluzione, ancor più lo è la rapidità con cui ciò avviene. E nessuna azienda, anche la più grande, può dirsi al sicuro di fronte agli incomer che affrontano il mercato sfruttando a fondo le possibilità offerte dalle nuove tecnologie. Basta considerare che il 90% delle aziende che facevano parte nel 1955 delle Fortune 500 sono scomparse dal mercato e che lo stesso si prevede avvenga entro un decennio per le aziende comprese tra le S&P 500.

Il messaggio è chiaro, o ci si trasforma, e lo si fa rapidamente, o si rischia di finire marginali al marcato.

Una proposta dallo storage agli analytics all'IIoT

Per rispondere alle esigenze delle aziende alle prese con una trasformazione in chiave digitale e dove il dato ha sempre più un valore economico, e quindi va non solo conservato ma anche fatto fruttare, Hitachi ha avviato a livello di gruppo, che comprende oltre 900 aziende impegnate in quasi tutti i settori industriali e dei servizi per favorire il processo di trasformazione digitale, un processo di consolidamento e di snellimento che l'ha portata da una parte a ridurre il numero di aziende che ne fanno parte e ha permesso di applicare in-house le nuove tecnologie che ora propone alle aziende, e dall'altra le ha permesso di aumentare la sua quota di mercato, il fattura-

to e il numero di clienti. «Per favorire l'evoluzione centrata sui dati presso i nostri clienti lo scorso anno abbiamo affrontato noi stessi un percorso di profonda trasformazione che ha coinvolto il management, le business unit, l'R&D e il go to market. Lo abbiamo ritenuto fondamentale per rispondere a un mercato che vede esplodere il volume dei dati generati e da gestire come conseguenza di quella che va sotto il nome di rivoluzione digitale. Va considerato ad esempio che il 90% dei dati oggi presenti sono stati generati negli ultimi due anni. L'impatto sulle aziende sarà quindi profondo e chi non si adegua sarà estromesso dal mercato», ha spiegato Tesini.

Come evidenziato, molto positivi i risultati finanziari conseguenti alla riorganizzazione ottenuti in Italia nell'anno fiscale appena chiuso, risultati a cui ha contribuito anche la nascita di Hitachi Vantara come conseguenza della fusione tra Hitachi Data Systems, Pentaho, specializzata negli analytics, e Insight, specializzata nello sviluppo di piattaforme per l'IoT.

"In Italia siamo cresciuti del 40% nelle soluzioni per data center di nuova concezione, del 26% nella data governance, dell'821% negli analytics, del 21% per le revenues e del 5% in addetti. Abbiamo consolidato la nostra posizione nell'area dell'Enterprise storage, siamo cresciuti di oltre il 40% nell'area dei dati non strutturati, di fatto acquisendo la leadership nel settore dell'object e del content storage, un risultato enfatizzato da un raddoppio del fatturato di Pentaho nel campo del big data analytics. Complessivamente abbiamo chiuso l'anno fiscale con un fatturato di 1,2 miliardi di euro che ci aspettiamo di far crescere sino a 1,5 miliardi nel corrente anno fiscale», ha commentato i risultati fiscali Tesini.

Un futuro flash e software defined

Se l'anno fiscale chiuso ha visto i risultati positivi portati dalla nuova organizzazione di Hitachi Vantara, quello in corso vedrà il rilascio d nuove soluzioni, soprattutto in chiave Software Defined. Per la fine del corrente anno fiscale, ha illustrato Tesini, Hitachi Vantara completerà una profonda trasformazione della sua offerta rendendo disponibile, a fianco dell'attuale famiglia di strage basata tutta sulmedesimo sistema operativo SVOS SF (Storage Virtualization Operating System), ottimizzato per storage flash , anche una soluzione completamente software defined che permetterà all'utente finale di scegliere come realizzare la sua infrastruttura di storage a livello fisco e gestirla mediante le soluzioni software di orchestrazione, di sicurezza e di backup che renderà disponibile. Tre le aree in cui saranno suddivise le proposte di Hitachi Vantara:

- Storage: comprende soluzioni storage per la modernizzazione dei data center e la velocizzazione delle operation tramite l'utilizzo diffuso di tecnologie a stato solido SSD.
- Enrich: Soluzioni per operazioni di intelligence sui dati e di data governance.
- Activate: soluzioni di data driven insight per estrarre valore dai dati.

«Nel corso dell'anno annunceremo numerose nuove soluzioni storage. Saranno soluzioni dotate in maniera nativa di applicazioni derivate dal mondo IoT, in grado di auto ottimizzarsi e con un up-time garantito contrattualmente del 100%» ha spiegato Tesini.

LA STRATEGIA DATA DRIVEN DI NETAPP PUNTA SUL CLOUD

Con Cloud Volumes per Google Cloud Platform la società, NetApp rafforza il portfolio dei servizi di dati per il cloud

Chiuso da poco l'ultimo anno fiscale con risultati lusinghieri e una crescita a due cifre in numerosi settori chiave dello storage e della gestione dei dati, cloud compreso, Marco Pozzoni, responsabile per l'Italia della società, ha illustrato su cosa NetApp si appresta a puntare nel suo prossimo anno fiscale appena iniziato per favorire la trasformazione digitale dei clienti, una trasformazione che sempre più fa leva sul cloud pubblico, sul cloud ibrido e sugli analytics per trarre beneficio dalle informazioni e riorganizzare i processi aziendali, il rapporto con il cliente e la produzione di fabbrica tramite soluzioni IIoT evolute.
"Analytics, Data Drive, Artificial Intelligence, Cloud, sono i temi di cui parlano i manager delle aziende, e non solo i responsabili IT ma anche, significativo del cambio di paradigma in atto, i responsabili delle risorse umane, ed è a questi che rispondiamo con le nostre soluzioni e quelle annunciate", ha commentato Pozzoni.
Tre gli aspetti del percorso verso l'innovazione che persegue NetApp. Il primo consiste nell'abilitare l'innovazione tramite l'ampio utilizzo del cloud, sia in base ad accordi con i principali provider come Amazon e Microsoft, a cui si è da poco aggiunta Google, che tramite lo sviluppo di soluzioni iperconvergenti e ad altissime prestazioni che permettono di realizzare un cloud a casa propria. Il secondo consiste nel permettere alle aziende di far leva proprio sul cloud per poter realizzare e rilasciare rapidamente nuovi servizi atti a espandere il business.
Il terzo, ma non ultimo, osserva Roberto Patano, senior manager systems engineer di NetApp, consiste nel permettere di modernizzare l'architettura dell'IT tramite l'ausilio di apparati basati su tecnologia storage flash in grado di interagire ed integrarsi in modo trasparente con i servizi e le infrastrutture del cloud pubblico.
Conferma dell'impegno di NetApp per una strategia sempre più data driven è il citato accordo siglato con Google e il rilascio di NetApp Cloud Volumes, un servizio di file storage nativo in cloud integrato con Google Cloud Platform (GCP).
«Questo è solo il primo passo della partnership che combina i servizi dati di prim'ordine di NetApp con l'innovativa leadership di Google Cloud nello sviluppo applicativo, negli analytics e nell'apprendimento automatico. NetApp riunisce servizi dati per il cloud pubblico leader di settore e le soluzioni flash con il più alto livello di connessione al cloud, attraverso il Data Fabric, per aiutare i clienti ad automatizzare e monetizzare le proprie risorse dati», ha commentato l'accordo Pozzoni.
Uno dei punti chiave delle soluzioni cloud sviluppate e in sviluppo in casa NetApp è la tecnologia flash, che connessa al cloud permette di migliorare le performance e aumentare la protezione dei dati.

LA STRATEGIA VEEAM PER LA HYPER-AVAILABILITY ENTERPRISE

Le soluzioni Veeam Hyper-Availability facilitano la data orchestration behavior- driven su infrastrutture multi-cloud di grandi dimensioni

Veeam Software ha illustrato la propria vision per la Hyper-Available Enterprise e la sua strategia per accompagnare le aziende clienti nel viaggio verso l'Intelligent Data Management su vasta scala.

Alla base della vision vi è la considerazione che il concetto di disponibilità è tradizionalmente associato a quelli di business continuity, backup e recovery. Le nuove sfide legate alla gestione dei dati aziendali e la necessità che questi siano sempre disponibili, impongono un'evoluzione da semplici soluzioni di Backup e Recovery con copia meccanica dei dati ad orari prestabiliti, a soluzioni con un'intelligenza molto superiore, grazie alla quale i dati imparano a rispondere in modo istantaneo ed appropriato a ciò che accade in un qualunque punto dell'infrastruttura dati aziendale.

La protezione e la gestione dei dati pensata come salvaguardia attraverso policy reattive è in sostanza superata e deve trasformarsi in un sistema che fornisca, in modo propositivo, valore di business, cosa che per la Hyper-Availabile Enterprise prevede 5 fasi:

Fase 1, Backup: Effettuare il backup di tutti i workload, assicurandosi che siano sempre ripristinabili in caso di interruzioni, attacchi, perdita o furto di dati.

Fase 2, Aggregazione: Assicurare la protezione e la disponibilità dei dati in ambienti multi-cloud per abilitare servizi digitali ed assicurare una vista aggregata della compliance a livello di servizio.

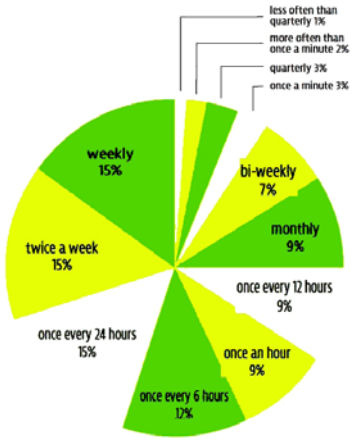
Fase 3, Visibilità: Migliorare la gestione dei dati in ambienti multi-cloud grazie alla visibilità e al controllo unificati dell'utilizzo, prestazioni e operatività; la gestione dei dati inizia a trasformarsi da reattiva a preventiva, per evitare perdite in termini di disponibilità grazie ad avanzate caratteristiche di monitoraggio, ottimizzazione delle risorse, capacity planning e intelligenza integrata.

Fase 4, Orchestrazione: Spostare i dati all'interno degli ambienti multi-cloud senza interruzioni per garantire la continuità del business, la compliance, la sicurezza e l'utilizzo ottimale delle risorse. Questo richiede un motore per l'orchestrazione che consenta all'azienda di eseguire, verificare e documentare progetti di disaster recovery in modo altamente automatizzato.

Fase 5, Automazione: I dati si auto-gestiscono, imparando a duplicarsi, spostarsi verso la location migliore in base alle esigenze di business, proteggersi in caso di attività anomale e ripristinarsi in modo istantaneo. Questa fase assicura nuovi livelli di automazione alla gestione dei dati aziendali attraverso una combinazione di funzione di analisi dei dati, pattern recognition e machine learning.

CLOUD E DEVOPS AIUTANO NELLO SVILUPPO DELLE APPLICAZIONI

Per i tre quarti dei CIO la spinta aziendale ad una rapida e continua innovazione mette a rischio la customer experience. Un aiuto dal Cloud e da DevOps



Il problema che si prospetta è presto detto: le organizzazioni rilasciano nuovi aggiornamenti software tre volte all'ora, ma quasi due CIO su tre è costretto a scendere a compromessi tra il perseguire un'innovazione più veloce e il rilascio di applicazioni software che siano adeguatamente testati e perfettamente funzionanti.

Una conferma basata sui pareri dei diretti interessati viene da uno studio commissionato da Dynatrace . I risultati del lavoro, basato su un sondaggio condotto da Vanson Bourne su 800 dei sistemi informativi di tutto il mondo appartenenti a grandi aziende con oltre 1.000 dipendenti,

evidenziano come per il 73% delle organizzazioni la necessità di accelerare in innovazione digitale stia mettendo a rischio la customer experience.

I compromessi minano la qualità

Lo studio ha rilevato che, in media, a causa delle pressioni della concorrenza e dalle crescenti aspettative dei consumatori, le organizzazioni di una certa dimensione rilasciano nuovi aggiornamenti software tre volte ogni ora lavorativa, un compito che grava sul reparto IT che le deve sviluppare, assicurarne qualità e prestazioni e supportarle su infrastrutture proprietarie, nel cloud o in ambienti ibridi.

Ma se questo è lo stato non entusiasmante dell'arte il futuro cosa riserva ? La situazione non sembra che sia destinata a migliorare, tutt'altro.

Quasi i due terzi dei CIO hanno ammesso di essere costretti a scendere a compromessi tra un'innovazione più rapida e la necessità di garantire ai clienti un'esperienza software di alto livello.

Il punto critico risiederebbe nel fatto che praticamente ogni organizzazione al mondo è diventata un'azienda di software, l'hardware una commodity e si è in presenza di una forte evoluzione verso ambienti software defined accompagnata da una crescente propensione al servizio.

Il problema è che nella gara ad essere più veloci e ad anticipare i concorrenti chi ne soffre sono gli utenti finali, che invece si aspetterebbero che il flusso costante di nuove funzionalità e aggiornamenti avvenisse con prodotti adeguatamente provati e senza dover scendere a compromessi.

La sfida che l'IT nel suo complesso si trova a dover affrontare e in qualche modo risolvere è quindi offrirli in modo rapido, cosa possibile tramite il ricorso a architettura native cloud e curando però adeguatamente l'esperienza dell'utente.

Se è chiaro il come e il perché, più difficile è pensare che la forte spinta competitiva che su scala globale coinvolge produttori e mercato permetta

realmente di porre freno ad una situazione che rischia di sfuggire di mano.
Se il ricorso al Cloud consente una maggiore agilità i CIO ciononostante sperimentano significative difficoltà in punti quali:

- Garantire che le prestazioni del software non subiscano un impatto negativo (67%)
- Identificare se spostare un'applicazione nel cloud abbia prodotto realmente i benefici desiderati (57%)
- Capire se un'applicazione sia particolarmente adatta al cloud (55%)
- ï Riprogettare applicazioni legacy in chiave cloud (51%)
- Garantire che l'esperienza dell'utente non sia influenzata durante il processo di migrazione da un ambiente legacy al cloud (48%)

Il problema della collaborazione e il DevOps

Quello dei tempi di sviluppo brevi e del loro impatto sulla qualità del prodotto finale, e sull'impatto che possono avere sul brand aziendale software non adeguatamente testati, non è però l'unico degli aspetti critici evidenziati dallo studio. Un altro problema è posto dalla cooperazione inter-divisionale.
In proposito, poco meno dell'ottanta per cento dei CIO ha affermato che la propria organizzazione ha subito ritardi in progetti IT che potevano essere evitati se i team di sviluppo e quelli operativi fossero stati messi in grado di collaborare più facilmente, a cui si aggiunge il fatto che le iniziative di digital transformation sono spesso finite su un binario sbagliato a causa di:

- interruzioni IT derivate da problemi esterni (55%)
- interruzioni IT causate da modifiche interne (50%)
- rettifica del codice errato che è stato spinto attraverso la pipeline (45%)

Ma da dove potrebbe venire un aiuto per eliminare o perlomeno mitigare fortemente questi problemi? Una risposta sempre più perseguita, perlomeno come potenzialità, è quella del DevOps, vista come approccio allo sviluppo atto a favorire e migliorare la collaborazione. I dati dello studio sostanziano questa posizione, pur se evidenziano alcune criticità nel farlo:

- Il 68% delle organizzazioni, e si tratta di una percentuale di certo significativa, ha implementato o sta esplorando le possibilità di una cultura DevOps per migliorare la collaborazione e promuovere un'innovazione più rapida.
- Il 74% dei CIO ha affermato che gli sforzi DevOps sono spesso indeboliti dall'assenza di dati e strumenti condivisi, il che rende difficile per i team IT ottenere un'unica visione della "verità" .
- Il 56% dei CIO ha identificato differenze nelle priorità tra i silos dipartimentali come ulteriore barriera all'adozione di DevOps.

In pratica, osserva il committente dello studio, la sfida per tutte le organizzazioni consiste nell'ottenere una visione olistica della pipeline DevOps, dall'idea al codice fino all'esperienza.
I dati evidenziano come con la maturazione del DevOps le aziende stiano perseguendo in modo crescente la strada dell'automazione e dell' integrazione nello sviluppo software in modo da abilitarne un più veloce rilascio, ma facendolo con una maggior qualità e un minor sforzo manuale.

SERVIZI TOP PER ALTRAVIA CON LE PRESTAZIONI DEL CLOUD

L'infrastruttura basata sul Private Cloud di OVH ha permesso a Altravia di aumentare il business facendo leva su un servizio affidabile, sicuro e flessibile

Altravia è una società informatica con la mission di sviluppare, con la propria R&D nella sede di Terni, tecnologie open source a supporto della evoluzione tecnologica e della diffusione di Internet. L'azienda nel corso degli anni ha consolidato la propria posizione sul mercato italiano e internazionale, aggiungendo a quella iniziale una offerta di attività di consulenza tecnologica e applicativa, di coordinamento progettuale, di sviluppo di servizi web e marketing e nella vendita online di prodotti informatici e camerali.

Gli sviluppi dell'offerta, ha spiegato Luca Scuriatti, CEO di Altravia hanno portato alla necessità di utilizzare una nuova infrastruttura di cloud privato sicura, affidabile e flessibile, sulla quale migrare tutti i propri servizi, in modo da poter disporre di prestazioni più elevate.

Un'analisi molto attenta e centrata sulla affidabilità e sulla flessibilità dell'offerta di mercato ha portato l'azienda a rivolgersi a OVH. Due i motivi: il primo perché i siti gestiti da Altravia registrano spesso e volentieri picchi di accesso, nel caso di scadenze o di attività promozionali, ed è importante che il servizio venga sempre garantito. Il secondo perché, trattandosi spesso di e-commerce, ogni interruzione di servizio porterebbe con sé un impatto negativo diretto in termini di fatturato.

«OVH si è dimostrato il cloud provider più affidabile e disponibile sul mercato. Ci siamo quindi convinti subito a spostare tutti i nostri servizi nella loro infrastruttura di private cloud», ha rimarcato Scuriatti. Ad oggi l'infrastruttura dedicata è basata sul Private Cloud di OVH composta da 101 macchine virtuali. Le attività dell'azienda producono un flusso di traffico intenso e costante, con una quantità di dati generati pari a 9 TB. Il servizio, sviluppato da OVH su tecnologia VMware, garantisce al flusso di dati la scalabilità del cloud in un'infrastruttura hardware che, osserva l'azienda, è dedicata al 100%.

Suddivisi i compiti operativi. Le macchine virtuali sono gestite internamente dal team Altravia, mentre la manutenzione e l'aggiornamento hardware sono a carico di OVH. Di OVH, ha spiegato la società, sono stati particolarmente apprezzati l'efficienza e la disponibilità dell'infrastruttura e le capacità di supporto e di problem solving fornite dal team tecnico.

Molto apprezzata è stata la trasparenza garantita nel trattamento dei dati personali, anche in relazione all'applicazione del GDPR. Aspetto enfatizzato dal fatto che OVH sia una delle aziende che ha contribuito alla creazione di CISPE.

I benefici per Altravia, evidenzia OVH, non si sono fatti attendere. Da quando è iniziata la collaborazione con la società ha avuto la possibilità di focalizzarsi ancor più sulle proprie attività core, facendo leva su un'infrastruttura agile e scalabile che garantisce una elevata disponibilità e continuità del servizio.