Cloud & Business

n.88
Febbraio 2020

LA RIVISTA PER IL MANAGER CHE DEVE OTTIMIZZARE COSTI E PROCESSI

IN QUESTO NUMERO>>>

La Unified Communication e il workplace viaggiano sul cloud

di Giuseppe Saccardi

La UCC è sempre più fruita nel cloud e facilita la digital transformation e l'adozione dello smart working

Con il termine di Unified Communication & Collaboration (UCC) ci si riferisce a un insieme di tecnologie, applicazioni, modalità di interazione con le applicazioni office, che permettono di interagire con colleghi o persone esterne all'azienda mediante una varietà di strumenti hardware e software.
Conversazioni in fonia, sessioni video a due o più partecipanti, lo scambio di mail, chat, presence e così via, sono tutti elementi che costituiscono un moderno sistema di co-

Reportec Cloud&Business - N.88 Febbraio 2020 - società- Editore: Reportec Srl **(www.reportec.it)** - Direttore responsabile: Giuseppe Saccardi
In redazione: Gaetano Di Blasio - Paola Saccardi - Immagini: Dreamstime.com

municazione unificata e collaborativa, per l'appunto quella che è riferita come Unified Communication&Collaboration o, più di frequente, con l'acronimo UCC.
Prese singolarmente, tutte le componenti di un sistema di UCC, che in nuce ha quelle funzioni che caratterizzavano i classici centralini di un tempo (in letteratura anglosassone riferiti come Pbx, acronimo di; Private Branch Exchange) non rappresentano di certo delle novità. In particolare, la videocomunicazione, la videoconferenza, lo scambio di messaggi, e naturalmente la fonia sono strumenti disponibili da decenni.
Quella che è la vera novità è costituita da evoluzioni sostanziali sotto il profilo tecnologico e dalla integrazione di queste funzionalità, ed altre attinenti le applicazioni di ufficio, all'interno di una unica soluzione omnicomprensiva, che ne fa uno strumento ideale ed indispensabile per applicazioni di Smart Working, nonché il fatto che la sua fruizione avviene sempre più tramite Cloud.
Che si sia seduti in ufficio alla propria scrivania o in smart working seduti sulla panchina di un parco con una mano sulla tastiera e l'altra che stringe un gelato, non fa differenza. Tramite i dispositivi mobili e il cloud o reti a larghissima banda, ci si può impegnare in una conversazione in fonia o in una sessione di videoconferenza.
Quello della evoluzione dell'UCC e del suo migrare nel cloud come fruizione è un settore che attrae crescenti interessi da parte delle aziende , e di converso da parte dei fornitori di soluzioni. Gli esempi non mancano né in un senso che nell'altro.

Il data center di Naquadria

I PBX VIRTUALI DI SELTA E LA FIBRA DI OPEN FIBER ABILITANO SERVIZI DI UCC EVOLUTI

La realizzazione di ambienti tecnologicamente evoluti e di servizi smart e di UCC passa sempre di più attraverso operatori locali animati da un forte spirito innovativo. Un esempio è Naquadria con il suo nuovo brand HD-Fibra (hdfibra.it), un provider piacentino che, tramite l'innovazione tecnologica, si è posto l'obiettivo di diventare il primo operatore di valore del territorio.
L'obiettivo è stato perseguito tramite un progetto che ha portato Piacenza ad essere una delle prime città italiane iperconnesse, grazie all'infrastruttura in fibra di Open Fiber. Il progetto è stato realizzato in partnership con l'operatore nazionale che sta lavorando alla posa di una rete capillare sul territorio piacentino. Open Fiber, tramite collegamento dedicato, ha congiunto il data center di Naquadria con il suo POP di Piacenza.
Grazie alla fibra e il suo data center di tipo tier 3 certificato ISO 27001, Naquadria è in grado di fornire servizi ad altissime prestazio-

ni sia agli utenti business che consumer. In particolare, propone ai clienti un servizio di centralino intelligente valorizzato dall'elevata prestazione dell'infrastruttura su cui si appoggia il data center e dal livello di sicurezza dei flussi di comunicazione che transitano sulla rete come se si trattasse di una rete privata e non Internet.

Per fornire ai clienti il servizio di centralino intelligente, Naquadria si è rivolta a SELTA (selta.com), di cui ha adottato la soluzione multi-tenant BRAVO. La soluzione di UCC è stata installata nel data center e configurata in modo da servire più clienti contemporaneamente con la stessa piattaforma, con possibilità di connessione di telefoni SELTA in modalità plug & play, oltre al collegamento di telefoni di terze parti già in dotazione del cliente.

Per le aziende che hanno l'esigenza di ottimizzare le comunicazioni in mobilità e i costi per nuovi dispositivi, l'offerta del provider comprende anche la smart app di SELTA che può essere installata direttamente su smartphone iOS e Android dei collaboratori aziendali. Data la semplicità dell'installazione dei terminali il servizio non prevede costi di attivazione (hdfibra.it/centralino-voip/).

«I clienti che hanno sottoscritto il servizio basato sulla soluzione SELTA - ha commentato **Alessandro Solari**, Ceo di Naquadria -, hanno dichiarato di essere molto soddisfatti per la velocità e semplicità di attivazione, e la qualità del servizio».

La soluzione ha evidenziato benefici sia per il provider che gli utenti. Il provider ha lavorato in partnership con SELTA, che ha nella propria mission lo studio di nuove esigenze nell'ambito delle comunicazioni aziendali, e ha beneficiato dei vantaggi di una soluzione di smart working innovativa che incontra le esigenze dei propri clienti.

Per i clienti i benefici sono persino maggiori e derivano dalla possibilità di dematerializzazione del centralino fisico on-premise, dall'utilizzo di risorse as-a-service non vincolanti, dalla velocità e semplicità di attivazione e da una elevata qualità e sicurezza del servizio.

PIÙ PRODUTTIVITÀ IN FAAC CON CISCO WEBEX DI VEM SISTEMI

FAAC, multinazionale bolognese specializzata nell'automazioni in ambito residenziale, industriale e pubblico, si è affidata alla consulenza di VEM sistemi per adottare nuove tecnologie digitali atte a favorire la collaborazione tra i dipendenti.

L'obiettivo è stato quello di creare un digital workplace che eliminasse le barriere tra le persone e rendesse le informazioni disponibili ovunque si trovino e in qualsiasi momento.

La notevole crescita del Gruppo FAAC, la ampia presenza internazionale, i centri di R&D distribuiti nel mondo hanno portato l'azienda a valutare tecnologie che fossero in grado di mettere in collegamento, in remoto, persone, informazioni e dispositivi in modo sicuro e integrato.

Enrico Minelle, Group CIO FAAC

È questo il contesto in cui sono entrati in campo

i consulenti di VEM sistemi che hanno supportato Luca Bauckneht, Group HR Director FAAC e Enrico Minelle, Group CIO FAAC, nella scelta della soluzione di Collaboration più adatta per raggiungere l'obiettivo.
Il team di esperti VEM ha individuato in Cisco Webex Teams la tecnologia più efficace per rispondere alle esigenze di FAAC e ha supportato la multinazionale nell'utilizzo e nella diffusione della cultura dei meeting digitali fra tutte le risorse del variegato Gruppo.
La scelta è caduta su Cisco Webex perché si tratta di una soluzione che permette di portare sul cloud tre strumenti di comunicazione aziendale: riunioni, messaggistica e chiamate. In particolare, tramite Webex Teams è possibile accelerare il lavoro di squadra.
Inoltre, ogni progetto può essere facilmente gestito in modo collaborativo da più persone in ogni parte del mondo, anche appartenenti ad aziende esterne a FAAC, e il lavoro di gruppo si evolve in un "workstream" continuo fatto di messaggi, riunioni virtuali, documenti, annotazioni e registrazioni.
Oltre al cloud e all'applicazione per laptop, tablet e smartphone, giocano un ruolo fondamentale i dispositivi Webex che permettono di garantire un'elevata qualità e affidabilità della collaborazione anche nelle sale riunioni di diverse dimensione, cosa che ha fatto si che molti manager di FAAC abbiano adottato dei dispostivi Webex per i loro uffici.
Attraverso l'uso di questa tecnologia FAAC è riuscita a sviluppare un ambiente di lavoro sicuro che abilita un aumento della produttività e del vantaggio competitivo dell'azienda.
La creazione di questo nuovo posto di lavoro digitale, ha imposto un profondo cambiamento nelle abitudini dei dipendenti.
Di questo aspetto si sono presi cura da un lato i professionisti di VEM sistemi, che hanno realizzato una serie di video pillole cartoon che hanno come protagonisti i dipendenti FAAC, dall'altro la multinazionale che ha promosso il cambiamento ingaggiando il top management, creando un "change management team" e un gruppo di evangelizzatori a disposizione per il training e il supporto dei colleghi.

AUTOMOTIVE PIÙ SMART CON IL VOIP SU RETI IP E IN CLOUD

Con il progredire delle tecnologie e con la prospettiva dell'adozione di nuove infrastrutture di comunicazione come la 5G atte a favorire un modo di cooperare sempre più smart, le prospettive con cui ci si rivolge alle telecomunicazioni sono destinate a mutare.
Tuttavia, le Tlc sono per lo più ancora percepite come lunoo strumento per mettere in contatto le persone. Di certo questo è vero ma con l'evolversi degli strumenti di cooperazione e tecnologie quali il VoIP, si è usciti dallo stretto ambito delle infrastrutture e si e approdati in quello più ampio delle applicazioni business anche in settori sino ad ora poco permeabili.
«Per le organizzazioni commerciali che fanno capo al settore automotive, migrare al VoIP non è più questione di rendere fissi i costi altrimenti variabili della telefonia ma, trattandosi di un servizio critico


Michele Piccini, CEO di IPKom

per l'impresa, di dotarsi di un'infrastruttura concepita secondo il criterio della massima resilienza e sicurezza, in grado di integrarsi pienamente con gli strumenti di business intelligence di cui sono dotate» osserva **Michele Piccini**, CEO di IPKom.

Numerosi sono i casi in cui IPKom ha riscontrato presso concessionarie mono o multi-sede la presenza di sistemi di BI all'avanguardia ma, allo stesso tempo, la carenza di statistiche attendibili sul contributo della telefonia alla produttività aziendale.

«Si tratta di carenze che non solo minano l'efficacia dei processi commerciali implementati dalle concessionarie ma anche la loro capacità di fidelizzare il cliente, poiché sviluppati su una base di informazioni incompleta», evidenzia Piccini.

In questo un aiuto è fornito dal VoIP. Dal punto di vista aziendale, un'infrastruttura VoIP resiliente, combinata ad un Pbx VoIP di nuova generazione in grado di interfacciarsi con gli applicativi e i sistemi informativi aziendali, consente di analizzare i picchi delle chiamate e quanto personale dedicare alla gestione di chat e chiamate, in quali orari o nel fine settimana.

Tramite l'interazione nativa con le soluzioni CRM è possibile altresì correlare i log delle chiamate in arrivo o in uscita al processo di vendita per generare statistiche attendibili in merito all'intero percorso. Tale integrazione e le funzionalità di numero unico consentono inoltre di indirizzare chi chiama al giusto interlocutore in base al numero chiamante.

Creare un contesto smart evita al cliente da un lato di dover spiegare a terzi l'intera situazione magari più volte per essere poi inoltrato al collaboratore di riferimento, e dall'altro all'addetto di essere informato automaticamente della chiamata ricevuta, informazione registrata anche nel CRM o in sistemi di gestione del workflow.

Non ultimo, diventa possibile sapere se una vendita ha avuto origine con una telefonata e quindi analizzare l'effettivo contributo delle telecomunicazioni alla produttività aziendale, rispetto ad altre modalità di contatto.

Mirco Balboni, Business Developer Manager Cloud & UC di Centro Computer

IL DIGITAL WORKPLACE MIGLIORA I PROCESSI INTERNI DI BUSINESS

A differenza del posto di lavoro fisico composto dalla tradizionale scrivania, il Digital Workplace assicura nuove opportunità. Accedere ai dati, sempre e da ogni applicazione, condividere informazioni con il team anche se lavora in luoghi diversi, riduce sensibilmente i tempi di sviluppo e costruisce un nuovo spazio di condivisione.

Le applicazioni più innovative infatti, permettono di condividere efficacemente informazioni, strutturare la conoscenza e mantenersi costantemente aggiornati, ma diventa prioritario saper scegliere lo strumento tecnologico più adatto ai nostri obiettivi.

Passare dalla teoria alla pratica non è però solo questione di tecnologie. Ad esse, che devono naturalmente essere efficaci, si deve

necessariamente abbinare una concreta capacità progettuale ed una esperienza realizzativa, senza le quali gli investimenti in soluzioni di digital workplace potrebbero risultare poco produttivi.

Un esempio di azienda che ha affrontato il tema nei suoi diversi aspetti è Centro Computer, una società di consulenza specializzata in prodotti, servizi e soluzioni IT per le aziende, e che ha accumulato una forte competenza nei progetti di Digital Workplace per le aziende che si sono poste l'obiettivo di far leva sulle nuove sfide della trasformazione digitale.

L'obiettivo è stato perseguito dalla società tramite una gestione efficace ed efficiente dei canali organizzativi e ricorrendo all'utilizzo delle tecnologie avanzate disponibili sul mercato, nonché coniugando applicazioni di digital workplace con il concetto di servizio basato su cloud

I suoi progetti sono basati in particolare su Microsoft Office 365, la suite su cloud che ha l'obiettivo di permettere di lavorare in modo ottimale ovunque, in qualunque momento e su qualunque dispositivo, e tramite le soluzioni di video conferenza HD di Logitech, Poly ed i dispositivi audio di qualità business di Jabra e Plantronics.

«Riscontriamo sul mercato molte richieste che coinvolgono il Digital Workplace, con precisi requisiti legati alle caratteristiche di semplicità, qualità, flessibilità, integrazione e sostenibilità. Il cloud è certamente maturo e ci troviamo a soddisfare esigenze fino a poco fa impensabili, anche se il percorso è ancora critico. Resta il fatto però che oggi, quando il cliente valuta una nuova soluzione, fa le opportune considerazioni sulla piattaforma cloud o in alcuni casi solo in cloud» ha osservato **Mirco Balboni**, Business Developer Manager Cloud & UC di Centro Computer.

La scelta della società si è orientata sulla piattaforma Microsoft Office 365 e più in particolare Microsoft Teams perché costituiscono e forniscono strumenti collaborativi di comunicazione unificata per aziende di qualsiasi dimensione, mentre con OneDrive for Business è possibile archiviare, sincronizzare e condividere i file di lavoro in cloud. A questo l'azienda abbina nei progetti Microsoft Yammer, che consente alle persone di collaborare e rimanere aggiornate su quello che succede in azienda.

Microsoft Teams, l'Hub di Office 365 che integra persone, contenuti e strumenti per permettere un ampio coinvolgimento delle persone, permette inoltre di integrare la fonia nei progetti di Intelligent Communication e Digital Workplace.

«La trasformazione digitale sta spingendo le imprese a valutare con estrema attenzione la nostra soluzione di 'Fleet Management', strumento che integra i vantaggi dell'acquisto e della locazione operativa, consentendo di gestire con un unico contratto tutto il parco dei posti di lavoro con assoluta modernità, flessibilità, semplicità ed efficienza. Fleet Management offre i vantaggi sia dell'acquisto tradizionale che della locazione operativa comprendendo la gestione delle opzioni, la diminuzione del TCO e soprattutto una definizione certa del budget e della diminuzione dei costi amministrativi di gestione» ha evidenziato Balboni.

Armando Trivellato, vice president SEMEA di Poly

CON IL VIDEO AS A SERVICE DI POLY VIDEOCOMUNICAZIONE PIÙ EFFICIENTE

Poly, nata dalla fusione di Plantronics e Polycom ha annunciato che si impegnerà a fornire a tutti i clienti che utilizzano applicazioni di videocomunicazione Zoom un dispositivo Poly nell'arco di due giorni.

L'annuncio fa seguito ad una collaborazione avviata da Poly con Starin, un distributore leader specializzato in soluzioni audio, video, multimediali e di comunicazione, collaborazione volta a fornire ai clienti Zoom servizi esclusivi e a valore.

In particolare e come parte dell'accordo, ha evidenziato la società, la video bar nativa Zoom Poly Studio X sarà una delle prime soluzioni ad essere disponibile per i clienti europei. «Abbiamo creato Poly Studio X per offrire un'esperienza Zoom Room semplicissima. L'annuncio fa parte del nostro impegno a rendere la distribuzione di Zoom Rooms ancora più rapida per i nostri clienti europei e amplia ulteriormente la nostra visione di un mondo del lavoro ancora più collaborativo, produttivo e meno complicato», ha commentato **Nick Tidd**, vice presidente, responsabile dei canali di vendita globale di Poly.

L'annuncio è però solo l'inizio di un'operazione più ampia, che vedrà Poly e Starin allargare progressivamente la distribuzione della famiglia Studio X di video bar, anche con altre soluzioni in modo da costituire un portfolio tecnologico di sale riunioni end-to-end tra cui sia possibile scegliere la più adatta alle specifiche esigenze di comunicazione video e audio.

Tra queste, la soluzione Poly Studio USB, il Poly G7500 all-in-one meeting room e le soluzioni di conference phones Poly Trio.

«Quello che rappresenta una costante nelle nostre soluzioni e che puntiamo continuamente a migliorare è l'elevata qualità della tecnologia della voce e del video che le caratterizza, con soppressione di echi fastidiosi e una resa del parlato che permette di realizzare sessioni di comunicazione business di qualità sorprendente e altamente efficienti», ha osservato **Armando Trivellato**, vice president SEMEA di Poly.

Sottovalutare il Security Operations Center può costar caro

In oltre il 40% delle grandi imprese italiane manca il SOC. E' una carenza che, spiega Maurizio Tondi di Axitea, può mettere in forse la sicurezza aziendale

Una recente ricerca, condotta su 6.000 dipendenti di PMI e grandi aziende di vari paesi, tra cui anche l'Italia, ha analizzato la percezione di sicurezza negli ambienti aziendali. In Italia, il dato più interessante riguarda la scarsa presenza di SOC e, di conseguenza, la sensazione di arretratezza nello svolgimento delle pratiche inerenti la sicurezza informatica.

Ma, in primis, cos'è il SOC e perché è così importante? In sintesi, il Security Operations Center è un centro che comprende diversi team di esperti dal quale vengono erogati servizi di gestione, monitoraggio e, in alcuni casi, di incident response.

Il suo obiettivo è quello di garantire la sicurezza dei sistemi informativi aziendali o di clienti esterni.

Dall'indagine realizzata da Bitdefender è emerso che circa la metà dei dirigenti italiani ignora quali siano le policy essenziali della sicurezza informatica e ammette di non avere risorse economiche sufficienti da investire.

Oltre alle risorse limitate anche la percezione dei dipendenti sugli investimenti è negativa, infatti solo meno di un quarto degli intervistati ritiene che l'investimento della propria azienda in strategie di sicurezza sia adeguato.

In relazione con gli altri stati europei, il dato in cui l'Italia è fanalino di coda è la presenza di un SOC: è assente in oltre il 40% delle aziende è assente, a fronte di una media del 30%.

Avere un servizio di questo tipo, evidenzia **Maurizio Tondi**, Director Security Strategy di Axitea, aumenta la velocità di reazione a un attacco informatico o alla rilevazione di un problema nella propria infrastruttura, diminuendo notevolmente le conseguenze sui sistemi informativi, sulla produttività e sul "portafoglio" dell'azienda. Più del 60% dei dipendenti del reparto IT crede che la propria azienda, in caso di un attacco malware, non sia pronta ad agire in modo tempestivo.

Diffusione limitata

Quello che emerge dai freddi dati statistici, evidenzia Tondi, è che la diffusione e la conoscenza del SOC in Italia rispetto ad altri paesi è ancora troppo bassa, le aziende non sanno cosa può offrire nello specifico, o credono che sia un servizio troppo costoso perché non possiedono la percezione di quali siano i reali vantaggi che può apportare. Perlomeno, viene da considerare, sino a che non si è coinvolti in un incidente serio che obblighi, obtorto collo, a riconsiderare la propria postura nei confronti della cyber security.

«Non tutte le aziende hanno le risorse economiche e umane per crearne uno interno, ma aziende come Axitea possono offrirlo come servizio gestito, al fine di dare ai clienti tutta la visibilità e la protezione necessaria, condividendo la professionalità e il know-how acquisito con esperienza e mettendo a disposizione personale altamente specializzato. Il SOC rappresenta uno strumento prezioso per molte realtà, sia piccole che grandi, contribuendo alla difesa dei più importanti asset aziendali» ha osservato Tondi.

Il ruolo dei vCPE nella virtualizzazione di reti e servizi

I vCPE e gli uCPE ricoprono un ruolo chiave nello sviluppo delle VNF e dei nuovi servizi. Luigi Meregalli di CIE Telematica ne evidenzia gli aspetti salienti

Luigi Meregalli - General Manager CIE Telematica

La virtualizzazione delle reti e la distribuzione a livello di periferia (o di Edge) della capacità di calcolo, l'esigenza di attivare rapidamente e a basso costo nuovi servizi hanno accresciuto negli ultimi tempi l'attenzione posta su una nuova interpretazione del classico CPE (Customer Premises Equipment, ovverossia il dispositivo di rete posto presso l'utente finale e riferito come vCPE o CPE virtuale.

In sintesi , un vCPE consiste in un approccio che trasforma le operazioni precedentemente basate su hardware in funzioni virtuali basate su software.

Se dalla enunciazione concettuale si passa a quella pratica, quello che ne deriva è che i dispositivi di rete degli utenti quali router, firewall o VPN sino ad ora basati su hardware dedicato si trasformano in applicazioni software e assumono una incarnazione virtuale fruibile in base alle specifiche esigenze.

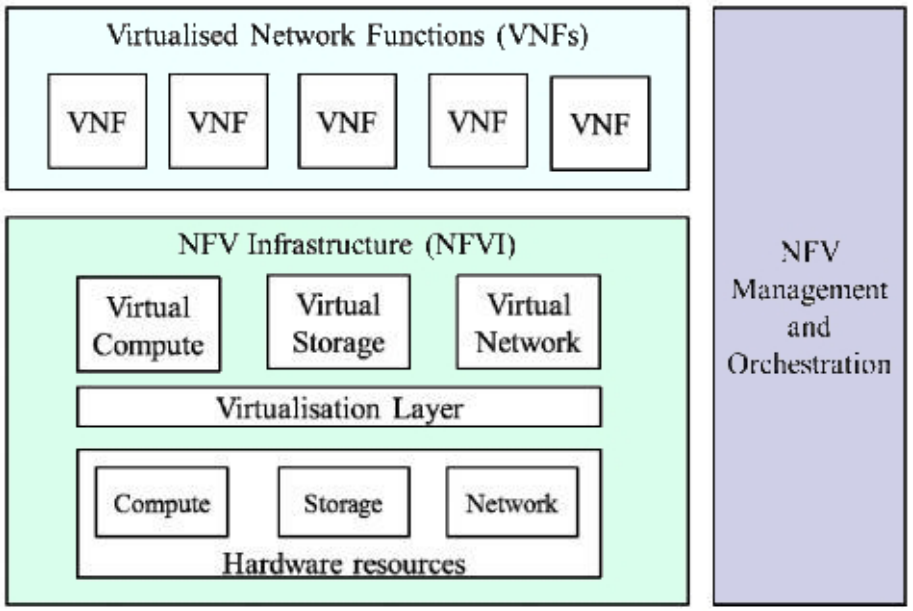
Il motivo dell'interesse per i vCPE ha varie motivazioni, alcune di costo e altre meramente funzionali. Nel complesso però, è il risultato della ricerca da parte dei provider di soluzioni atte a realizzare infrastrutture di rete a costi più bassi e allo stesso tempo in grado di erogare servizi a valore facilmente attivabili ed espandibili, da aggiungere alla mera fornitura di connettività e di capacità di banda che offre profitti sempre più limitati.

L'elenco dei servizi può essere molto lungo ma un esempio è rappresentato dai servizi IP-VPN per la connessione di sedi distribuite, servizi di sicurezza gestita, o il trunking SIP (Session Initiation Protocol).

Sono tutti servizi, questi ed altri, che permettono di operare su due piani: da una parte riducendo i costi di erogazione e gestione, dall'altra differenziando i servizi in modo da ottenere un vantaggio competitivo nei confronti dei concorrenti.

vCPE e NFV

La virtualizzazione di un CPE è un processo inserito nel più ampio contesto della virtualizzazione delle funzioni di una rete (NFV). Quest'ultima si riferisce alla separazione delle funzioni svolte da una rete dall'hardware di base. In pratica è una visione per cui è possibile sviluppare funzioni senza doversi dotare di hardware specifico e bloccante ma utilizzando uno strato fisico che svolge le funzioni fondamentali e che lo fa con apparati



Architettura di una rete virtuale (fonte ETSI)

gli uCPU (universal CPE) e le VNF.

economici e standardizzati.

Il core di una NVF è costituito dalle funzioni che gestiscono servizi quali quelli di firewalling o di load balancer.

A loro volta le funzioni NFV possono essere fatte girare su macchine virtuali (VM) nel livello alto dell'infrastruttura hardware della rete così come su un white box (ovverossia un hardware non specializzato) possono risiedere più macchine virtuali che ne utilizzano le risorse.

Espresso come sopra sembrerebbe che tutto vada bene e non ci siano problemi. Dopo tutto si può vedere un vCPE e il suo sistema operativo (OS) come una piattaforma su cui vengono di volta in volta ospitate le funzioni NFV necessarie. Invece delle domande da porsi ci sono e derivano dalla considerazione che:

- Si è in presenza di una varietà di fornitori di piattaforme OS vCPE e di opzioni open source.
- Diverse esigenze richieste alla piattaforma vCPE e relativo software.
- Le modalità di provisioning zero-touch (ZTP) e di gestione dei servizi virtuali e la complessità dei controlli in ambienti cloud e multi-cloud.
- Sono diversi i fornitori nella catena del valore, compreso in questo le aziende che forniscono

Prevedere l'evoluzione che si avrà nel futuro non è quindi semplice. Indipendentemente da come si evolverà l'ecosistema in vCPE nel prossimo futuro una società di ricerca e analisi come AvidThink prevede in ogni caso che la piattaforma vCPE ricoprirà sempre più un ruolo strategico nel mercato SD-WAN, considerazione basata sul fatto che già ora molte delle funzioni che semplificano l'uso, la scalabilità e la gestibilità che le aziende si aspettano da una SD-WAN sono fruibili tranne una piattaforma vCPE.

Alcune piattaforme vCPE forniscono già funzionalità integrate di tipo VNF come routing e firewall. Linux stesso è già dotato di una serie di funzionalità che potrebbero essere integrate nella piattaforma vCPE per fornire un ampio set di funzioni.

Con l'evoluzione del mercato i fornitori di piattaforme vCPE aggiungeranno probabilmente ulteriori funzionalità alla propria piattaforma per far fronte alle esigenze di aziende e service provider

L'approccio RAD e CIE Telematica per un vCPE a prova di rete virtuale

Passando dai concetti teorici alla loro concretizzazione pratica, una risposta alle esigenze sopra

analizzate per quanto concerne in particolare i vCPE, l'ha data RAD, società specializzata nello sviluppo di soluzione per la virtualizzazione dello strato di edge di una rete.
Le soluzioni che ha sviluppato, evidenzia Luigi Meregalli, general manager di CIE Telematica (www.cietelematica.it), società di ingegneria che rappresenta storicamente RAD in Italia, hanno l'obiettivo di fornire gli strumenti necessari a operatori e gestori di reti per erogare servizi garantiti basati su CPE virtuali e carrier grade.
Tra le funzionalità che li caratterizzano vi sono ad esempio:

- Un sistema operative unificato (vCPE-OS) che gira su qualsiasi piattaforma del tipo white box e che garantisce una base comune per il software e le funzioni da erogare.
- Dispositivi pluggable per i diversi tipi di connettività richiesta.
- Una orchestrazione dei dispositivi di rete tramite il software di gestione e di orchestrazione dei domini centralizzata RADview, orchestrazione che viene realizzata tramite API standard.
- Funzioni embedded di sicurezza.

«L'aspetto saliente dell'approccio RAD è che il vCPE è una soluzione modulare e aperta che si adatta ad ambienti di rete di qualsiasi fornitore di rete di accesso, VNF, alla piattaforma hardware e alla orchestrazione. Inoltre, il vCPE sviluppato da RAD abilita l'accelerazione dell'hardware e mette a disposizione funzioni specializzate che includono MEF CE2.0, PTP Grandmaster timing e uno switching wire-speed sia a livello 2 che 3. Della rete. E, non ultimo, l'analisi del traffico e l'encryption» ha osservato Meregalli.

Rete rivoluzionata con i vCPE Service Assured di RAD

Come osservato i fornitori di servizi di comunicazione nel segmento dei servizi alle imprese si trovano ad affrontare una forte concorrenza, sia da parte di giganti OTT che offrono servizi di connettività cloud semplici ed economici, sia da fornitori SD-WAN che offrono un'alternativa a basso costo alle VPN basate su protocollo IP.
Per far fronte a queste esigenze, un primario fornitore di servizi di livello 1 operante nel sud est asiatico, ha adottato la soluzione vCPE Service Assured di RAD come parte di un progetto per trasformare profondamente la sua rete in una rete NFV / SDN (.
La soluzione adottata dal provider include le piattaforme pCPE ETX-2v uCPE e ETX-2p a livello di sito aziendali, entrambe che girano sul sistema operativo vCPE aperto che ha il compito di gestire le risorse dedite alla virtualizzazione, nonché l'orchestrator di domini RADview integrato con SDN / NFV Orchestrator.
uCPE e pCPE di RAD verranno utilizzati per continuare a fornire servizi IP VPN esistenti su MPLS e banda larga, ma consentiranno anche l'erogazione di servizi a valore aggiunto che finora non erano possibili. Tali servizi includono l'accesso sicuro e affidabile a cloud pubblici e privati, firewall personalizzati, soluzioni DDoS, Intrusion Detection Systems (IDS) / IPS e altri.
Il fornitore di servizi prevede inoltre di qualificarsi nei confronti dei concorrenti utilizzando vCPE Toolbox per offrire servizi personalizzati a settori verticali specifici. Ad esempio, un pacchetto di servizi su misura per le filiali al dettaglio potrebbe includere un firewall per il breakout locale di Internet, l'ottimizzazione WAN, il controller WiFi gestito e un servizio CCTV gestito, mentre nel settore della logistica potrebbe includere anche RFID gestito per il tracciamento degli asset e il tracciamento dei veicoli.
Ciò consentirà ai clienti finali aziendali e delle PMI, ha osservato Luigi Meregalli, anche di utilizzare un portale self-service per implementare e attivare autonomamente varie funzioni del loro servizio dati aziendale.

CyberArk Blueprint mette al sicuro gli accessi privilegiati

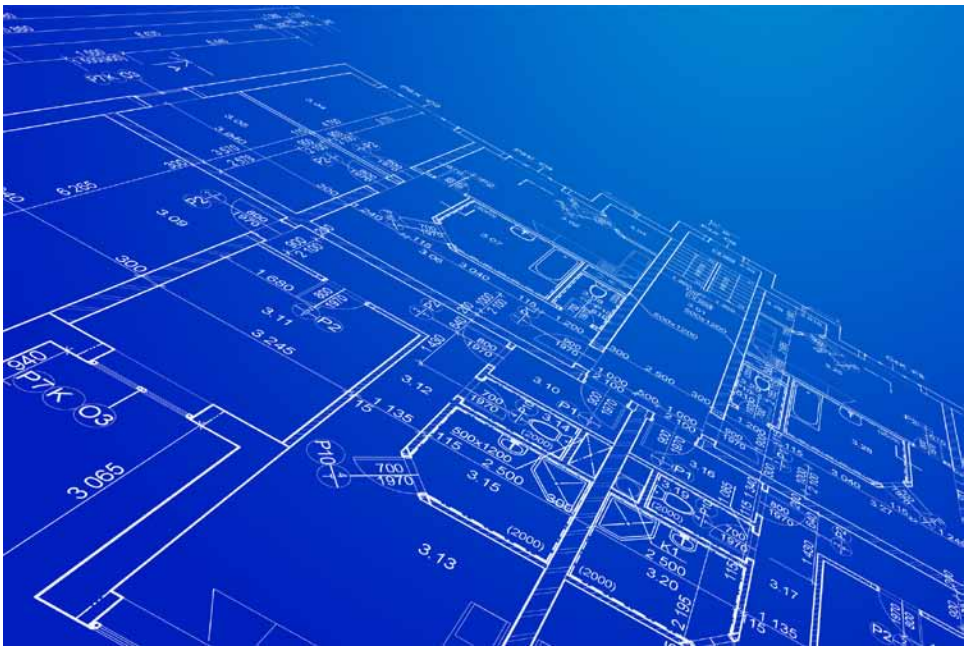
Il Blueprint comprende strumenti e supporto normativo che permettono di innalzare i livelli di sicurezza e di concentrarsi sulle priorità della trasformazione digitale

Nir Gertner, chief security strategist di CyberArk

CyberArk, azienda che sviluppa soluzioni per la protezione degli accessi privilegiati, ha annunciato il via al suo nuovo programma CyberArk Blueprint for Privileged Access Management Success, progettato per supportare le aziende nell'adottare un approccio flessibile, adattabile alle esigenze, modulare e misurabile che permetta di ridurre i rischi in cui possono incorrere gli utenti privilegiati.
In base all'esperienza dei CyberArk Labs, di Red Team e degli sforzi per rispondere agli incidenti, osserva l'azienda di cyber security, praticamente tutti gli attacchi mirati seguono uno schema standard per la compromissione delle credenziali privilegiate.
Questi modelli hanno avuto un'importante influenza nella definizione dei tre principi guida fondamentali del programma CyberArk Blueprint: prevenire il furto di credenziali, fermare i movimenti laterali e verticali, limitare l'escalation dei privilegi e gli abusi.

Keep it simple

La soluzione adotta in pratica un approccio semplice e prescrittivo basato sulle linee guida evidenziate al fine di contenere il rischio nelle cinque fasi di perfezionamento della gestione degli accessi privilegiati.
Le aziende che adottano il cloud, migrano alla Sicurezza fruita come servizio, sfruttano DevOps e automatizzano i processi con RPA (Robotic Process Automation) hanno la possibilità, nota CyberArk, di beneficiare della possibilità di dare priorità ai risultati raggiungibili con uno sforzo limitato, derivanti dall'affrontare progressivamente i casi d'uso avanzati e dall'allineare i controlli di sicurezza agli sforzi di trasformazione digitale in ambienti ibridi.
CyberArk Blueprint dispone di modelli e sessioni di progettazione di roadmap personalizzabili in modo da permettere alle organizzazioni dei diversi settori di ampliare in modo progressivo i controlli e la strategia di accesso inerente gli account privilegiati.



In particolare diventa ad esempio possibile:

- **Prevenire il furto di credenziali:** Per mitigare i rischi interni ed esterni, le aziende devono prevenire il furto di credenziali critiche – ad esempio quelle di amministratori IaaS, amministratori di dominio o le chiavi API - che potrebbero essere utilizzate per realizzare attacchi di acquisizione di rete o compromettere gli account delle infrastrutture principali. Tramite l'isolamento delle sessioni, la rimozione delle credenziali codificate e le strategie di rilevamento e blocco dei furti, diventa possibile proteggere l'accesso privilegiato da parte di persone, applicazioni e nei processi CI/CD.
- **Blocco dei movimenti laterali e verticali:** Il principio fa leva sul rafforzamento dei confini delle credenziali, sull'accesso just-in-time e sulla randomizzazione delle credenziali. L'obiettivo è di impedire ai malintenzionati di passare da dispositivi non affidabili a console cloud o controller di dominio di alto valore e bloccare e interrompere di conseguenza la catena di attacchi.
- **Limitare l'escalation di privilegi e abusi:** Per impedire agli aggressori di abusare dei privilegi e ridurre la superficie complessiva dell'attacco, è importante implementare controlli forti sui privilegi minimi, disporre di analisi comportamentale e rispondere agli attacchi in modo adattativo.

«Semplice ma completo, CyberArk Blueprint offre una guida imparziale che allinea le iniziative di gestione degli accessi privilegiati alla riduzione del rischio potenziale, aiutando le aziende ad affrontare le principali responsabilità il più rapidamente possibile. Indipendentemente dal loro livello di gestione degli accessi privilegiati, CyberArk Blueprint consente alle aziende di rendere gli investimenti in nuove tecnologie a prova di futuro, migliorando la sicurezza, riducendo la superficie di attacco e ottimizzando l'efficienza operativa» ha commentato **Nir Gertner**, chief security strategist di CyberArk.

Ottimizzare lo storage per l'Hybrid IT

Una nuova generazione di appliance Fujitsu per la protezione dei dati permette di condividere i dati attraverso gli ambienti edge, core e cloud

Maurizio Ranghetti, Product Portfolio Management di FINIX Technology Solutions

La praticità e la convenienza economica del cloud computing hanno prodotto un significativo cambiamento nel modo in cui le aziende fanno funzionare le applicazioni e gestiscono i dati, adottando un modello che oggi è diffuso dal data center principale fino al cloud e alle installazioni edge.

Gli ambienti IT ibridi sono oggi una realtà in numerose aziende, tanto che il modo in cui viene gestito l'elemento critico dello storage dati è stato ripensato. Ora il servizio business essenziale non è più la sola capacità, ma l'essere in grado di creare e accedere ai dati memorizzati. Per ottenere nuovamente il controllo dei dati, riprendendolo dalle fonti distribuite, Fujitsu ha annunciato Fujitsu Storage ETERNUS CS800 ed ETERNUS CS8000, che fanno parte di una nuova generazione delle sue appliance per la protezione dati e progettate per il backup, l'archiviazione e lo storage di secondo livello.

Sono caratterizzate, ha osservato la società, da elevati livelli di efficienza storage, funzionalità avanzate per la protezione dei dati e stretta integrazione software.

In pratica, hanno l'obiettivo di permettere alle aziende di creare un unico livello storage trasparente e unificato per la protezione dei dati all'interno degli ambienti IT ibridi.

A livello commerciale sono disponibili in Italia esclusivamente attraverso FINIX Technology Solutions.

I nuovi modelli delle appliance costituiscono nel complesso una piattaforma di consolidamento per la gestione dei dati che abbraccia backup e recovery, archiviazione, conformità e business continuity. La sua funzione è quella di migliorare i livelli di disponibilità, protezione, condivisione e interoperabilità dei dati per le applicazioni residenti in ambienti ibridi.

«Consolidando i servizi storage e separando lo storage dal layer applicativo, le aziende possono implementare strategie per la gestione dei dati a lungo termine. Il consolidamento dello storage introduce anche la possibilità di migliorare la governance e la sicurezza dei dati e, aspetto importante, tenere aperta la porta all'aggiunta di futuri servizi applicativi, un punto nel quale le appliance ETERNUS CS forniscono un concreto valore di business, tanto oggi quanto nel futuro» ha commentato il rilascio **Maurizio Ranghetti**, Product Portfolio Management di FINIX Technology Solutions.

Storage Fujitsu ETERNUS

Protezione per ambienti di grandi e piccole dimensioni

Costruttivamente, ETERNUS CS800 è una appliance intuitiva basata su disco che fornisce uns piattaforma ideata per il consolidamento dei dati negli ambienti di backup di piccole e medie dimensioni.

La soluzione è scalabile e, coem evidenziato, è dotata di funzioni per la deduplica automatica, la replica integrata e il supporto dei principali software per il backup.

E' una soluzione che apre la strada ad una strategia di protezione dati cvolta a massimizzare la disponibilità delle applicazioni e a proteggere da disastri e perdite di dati.

Di fascia più elevata è il modlelo ETERNUS CS8000, una soluzione storage versatile per il backup, l'archiviazione, lo storage di secondo livello e i dati a oggetti che fornisce protezione continua per il ripristino dei dati mission-critical.

La appliance è progettata per ambienti impegnativi di grandi dimensioni come quelli degli istituti finanziari, dei provider di servizi di telecomunicazione e degli operatori delle reti di trasporto.

Sfruttando l'automazione intelligente dei processi e il pooling della capacità storage, i dati e le loro copie vengono automaticamente gestiti tra i differenti livelli storage e supporti, come SSD, dischi, deduplica e nastri, a seconda delle performance e dei livelli di disponibilità richiesti.

Completa il portfolio di appliance per la protezione dei dati ETERNUS CS, lo storage su nastro Fujitsu ETERNUS LT, che costituisce una soluzione economicamente efficiente per il backup offline a scopo di conservazione o archiviazione dei dati a medio e lungo termine.

Consolidamento del cloud

Nel suo complesso, la nuova proposta di storage Fujitsu costituisce un approccio unificato alla protezione dei dati che permette di consolidare i dati provenienti da fonti come il cloud, le applicazioni e il data center, e mette in condizioni di far fronte alla sfida della gestione di crescenti volumi di dat.

Non ultimo, ha osservato Finix, facilita l'introduzione di nuovi servizi per l'intero ambito aziendale come l'archiviazione, le ricerche, l'analytics e la governance dei dati.

Storage più semplice per l'Hybrid Cloud e il Multi Cloud

Le nuove famiglie di storage IBM FlashSystem semplificano la realizzazione di infrastrutture storage in azienda o nel multi cloud e ne facilitano la gestione

IBM FlashSystem

Complice la trasformazione digitale in atto le necessità storage delle organizzazioni possono essere di diversa tipologia, così come sono diversi i parametri delle applicazioni all'interno di una specifica organizzazione, come l'entry point, le performance, la scalabilità, i data service, la funzionalità e la disponibilità.
I produttori di dispositivi storage nel passato anche recente hanno risposto alle esigenze delle organizzazioni sviluppando piattaforme di archiviazione uniche che però hanno finito con il risultare obsolete a causa dell'insorgere di complessità nella gestione e nella risoluzione di problemi, nei possibili percorsi evolutivi verso il cloud eccetera.
A questo si è aggiunta la complessità derivante dal fatto che molti utenti implementano sistemi di archiviazione multi fornitore.
Il risultato di tutti questi fattori è che i costi di archiviazione, la gestione e l'ottimizzazione dell'allocazione e della movimentazione dei dati siano tra le principali preoccupazioni degli utenti storage e costituiscano a loro volta il punto di origine di ulteriori criticità, tra cui i ritardi nell'adozione di nuove tecnologie di archiviazione o la riduzione della flessibilità, cose che finiscono a loro volta con l'impattare sulle applicazioni, sui carichi di lavoro e sui i costi.
La soluzione IBM per ambienti Enterprise e Multi Cloud
Per far fronte a queste esigenze IBM ha annunciato una nuova famiglia di soluzioni di archiviazione flash progettate con l'obiettivo di soddisfare l'ampia gamma di tipiche esigenze Enterprise, dall'accesso ai sistemi di fascia media a quelli di fascia alta, sino alle implementazioni di archiviazione ibrida multicloud.
In pratica, IBM ha adottato un approccio che l'ha portata a semplificare ulteriormente la sua famiglia storage IBM FlashSystem e dato vita a una piattaforma singola creata per semplificare l'infrastruttura storage, ridurre la complessità e tagliare i costi.
Le nuove soluzioni di storage di classe enterprise e per ambienti ibridi multicloud si caratterizzano con caratteristiche quali una disponibilità a "sei 9", la replica a 2 e 3 siti, configurazioni

ad alta disponibilità su più siti e l'opzione per una disponibilità dei dati garantita al 100%.la crittografia, copie "air gap" su nastro e cloud, rilevamento di malware e snapshot sensibili alle applicazioni.
Particolarmente evoluta è la dotazione di funzioni per il cloud, che comprende API coerenti per l'automazione fornita in locale e nel cloud, con il supporto di implementazioni bare metal, virtualizzate, containerizzate e per il multicloud ibrido.
Consistenti anche le analitiche e le funzionalità di gestione, che permettono un management basato su cloud, intelligenza artificiale, storage analytics e il supporto proattivo integrato.
In particolare, IBM Storage Insights abilita una gestione di storage eterogeneo attraverso un'unica console, sia IBM che non, congiuntamente a storage cloud gestito da IBM Spectrum Virtualized per il Public Cloud.

Tre i sistemi che si sono aggiunti agli esistenti:

- **IBM FlashSystem 7200:** E' una soluzione End-to-end NVMe (Non-Volatile Memory Express) con funzionalità di classe Enterprise per il multicloud ibrido ideata per implementazioni di fascia media. Dispone sia case" di espansione che clustering fino a 4 vie, un massimo di 9.2 milioni di IOPS e 128GB/s.

- **IBM FlashSystem 9200:** Ha caratteristiche tecniche simili al precedente ma con più alte prestazioni: un massimo di 18 milioni di IOPS e 180GB/s con cluster a 4 vie. Sia i dispositivi 7200 che 9200 presentano una latenza ridotta a 70µs.

- **IBM FlashSystem 9200R**: E' una soluzione storage ideata per aziende che richiedono un sistema storage costruito e testato da IBM, con installazioni e configurazioni effettuate da IBM.

Tutti i componenti della famiglia di IBM FlashSystem, eccetto tutti i FlashSystem 9200 e 9200R, sono disponibili in versioni all-flash e hybrid flash.

Endpoint al sicuro nel cloud con la cifratura dei dati

Il criptaggio e il monitoraggio dei dati permettono di migliorare la sicurezza degli endpoint nel cloud e contrastare le minacce, spiega Matrix42

Se la digitalizzazione dei processi di business, della produzione e delle relazioni umane apporta consistenti benefici, non c'è dubbio che la stessa apre la strada a concreti rischi per la sicurezza dei dati.

Generalmente si tende ad attribuire a cause esterne, tipicamente hacker, l'origine dei problemi, ma sovente questi sono invece da ricercare internamente, perlomeno come uno dei motivi che abilitano o rendono possibile un attacco. Un esempio in tal senso è la carenza o la totale mancanza di un piano per la sicurezza degli endpoint organico e ben strutturato. In sua mancanza risulta difficile contrastare attacchi portati su più piani, in profondità e a partire dai punti più deboli, gli endpoint.

I dipendenti, manager in primis, di un'azienda, osserva Matrix42, azienda specializzata nella sicurezza degli endpoint, gestiscono necessariamente al fine di svolgere il loro compito un consistente volume di dati, e il problema è che complice la crescente mobilità questa gestione avviene in luoghi deputati diversi da quello aziendale che è relativamente più facile proteggere, ad esempio in aereo, in treno, in hotel o nei momenti di home working.

La virtualizzazione del workspace apre in sostanza la strada a concreti rischi per la sicurezza e amplia anche notevolmente la superficie di attacco.

La cosa è resa più critica dal fatto che non solo i computer e i notebook, ma anche gli smart device e i dispositivi IoT o Industrial IoT finiscono con il costituire un serio rischio per le aziende.

Proteggere i dati con la cifratura

I rischi, osserva Matrix42, in cui incorre un'azienda non sono solo dovuti alla perdita di dati ma anche agli aspetti legali e normativi in cui si può incorrere. In proposito, il regolamento europeo per la protezione dei dati personali prevede concrete conseguenze nel caso in cui accessi non autorizzati ai dati portino a infezioni da malware e perdita dei dati, soprattutto di clienti o terze parti.

Non a caso, per il rafforzamento delle difese, il regolamento in oggetto stabilisce che la protezione contro la perdita dei dati avvenga mediante la cifratura e il log degli accessi ai dati non cifrati.

In linea generale, persino la perdita di un singolo file può costituire un danno considerevole

per le imprese. Tuttavia, sebbene proteggere dati e file mediante cifratura fornisca una maggiore sicurezza, non tutte le aziende la applicano per il timore che l''operazione porti a una riduzione della produttività dei dipendenti.
Cifrare i dati, osserva Matrix42, e si può di certo essere d'accordo con lei, è oramai una procedura quasi inevitabile e il non implementarla può essere percepito come un colpevole vulnus. A giustificarla può bastare citare i dati di un recente studio dell'associazione digitale Bitkom, che ha evidenziato come nel corso del 2018 circa l'84% delle imprese nel settore industriale sia stato vittima di attacchi informatici ancora più intensi che nel 2016. Circa il 70% di questi attacchi hanno avuto origine a livello di endpoint, e i due terzi di questi non sono stati rilevati. Nel 2019 le cose non sono di certo migliorate.

I benefici dell'analisi in tempo reale

Altre ricerche evidenziano la crescente importanza della protezione degli endpoint. Le soluzioni di sicurezza per gli endpoint quali la cifratura d hoc, costituiscono un'ulteriore barriera a soluzioni quali i firewall nel confronto dell'esfiltrazione di dati e permettono agli amministratori IT di implementare e rafforzare le policy di sicurezza.
Il concetto trova applicazione anche nell'eventualità che gli end device vengano smarriti o rubati. Il criptaggio dei dati, la cui efficacia è massimizzata da smart card e eToken, garantisce che i criminali informatici non abbiano accesso alle informazioni sensibili.
Sono quindi raccomandate, osserva Matrix42, soluzioni di Cloud Storage Encryption, iOS e Android Encryption, Full Disk Encryption, Local Folder Encryption, Network Share Encryption, così come di Removable Device Encryption e il criptaggio permanente file-base.
Per una difesa efficace contro gli attacchi, peraltro, la società suggerisce anche di utilizzare un sistema di difesa multilivello contro il trasferimento non autorizzato dei dati.
In questo caso, le soluzioni software devono però poter analizzare e classificare i processi in tempo reale, così come anche la migrazione dei dati e la loro archiviazione ai diversi livelli.
E, non ultimo, garantire che la cifratura e la relativa decifratura siano applicate non solo per le classiche workstation, come i sistemi Windows, ma anche per macOS, Android, iOS e similari.

Cifrare in modo sicuro

Va comunque osservato che la cifratura è un campo solo parzialmente esplorato ed utilizzato. Sin dalla ideazione della macchina Enigma si è assistito ad una rincorsa tra l'ideazione di nuovi metodi pubblici e privati, a più chiavi, eccetera, e chi cerca di trovare il modo di effrangere i dati cifrati.
Esiste poi una concezione diffusa, ma non del tutto corretta, evidenzia Matrix42, che le aziende debbano cifrare la comunicazione stessa solo quando si procede alla sincronizzazione

dei dati.
I provider dei rispettivi servizi di sincronizzazione, generalmente, possiedono le chiavi per la cifratura. Tuttavia, i dati stessi non sono criptati: ciò significa che persone o organizzazioni non autorizzate, come ad esempio degli hacker, possono ottenere l'accesso alle chiavi segrete dei provider oppure accedere direttamente all'archivio dei dati.
Di certo, la modalità più sicura si verifica quando sono le stesse imprese a detenere le chiavi e criptano i dati prima della sincronizzazione.
Le aziende dovrebbero cifrare le interfacce di dati che utilizzano, preferibilmente file-based e on-the-fly. Questa procedura ha il vantaggio di essere un metodo sostenibile, poiché le aziende non devono preparare un archivio dati in anticipo e non sono costrette a installare o gestire applicazioni aggiuntive per l'autenticazione, il decriptaggio o il criptaggio.
In ultima istanza, un monitoraggio sistematico degli endpoint rende possibile implementare funzioni di alert a livello aziendale che sono accompagnate da risposte automatiche in caso di minaccia.
Il principio alla base è che l'IT controlla, accede e cripta gli accessi ai dati negli endpoint. Le nuove tecnologie basate sul Machine Learning (ML) e l'Intelligenza Artificiale (IA) forniscono in tal senso capacità potenziate correlate alle strategie di sicurezza degli endpoint.
Sono peraltro soluzioni che evolvono e apprendono da eventi passati e rendono persino possibile combattere minacce non solo già note ma anche sconosciute, e farlo in tempo reale.
Ma non solo. Il ricorso contemporaneo a ML e IA semplifica anche identificare ed evitare falsi positivi quali i falsi allarmi. Di certo nel prossimo futuro vi saranno ulteriori sviluppi in questo campo, ma una cosa è già certa, osserva la società: un concetto di sicurezza che non considera gli endpoint è incompleto.

Il cloud ibrido si conferma come il modello preferito per l'IT

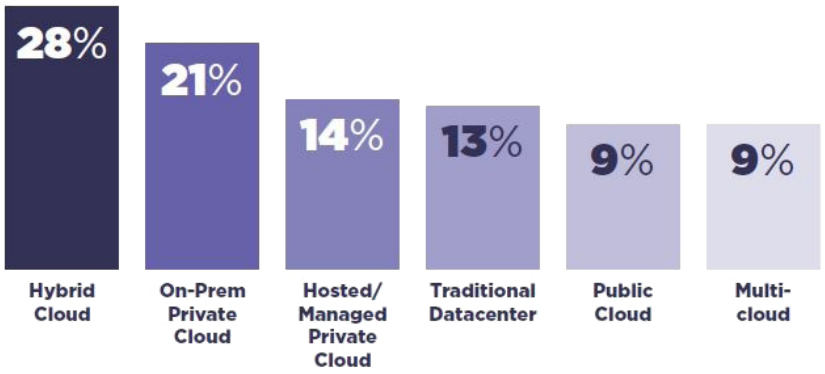
L'area EMEA è in linea con il piano quinquennale per la migrazione al cloud ibrido, ma in ritardo nel breve termine. Lo evidenzia un report realizzato da Nutanix

Nutanix, società che sviluppa soluzioni per l'enterprise cloud computing, ha annunciato i risultati per la regione EMEA del report annuale Enterprise Cloud Index.
Il report è stato realizzato da Vanson Bourne. La società di ricerca ha intervistato 2.650 responsabili delle decisioni in ambito IT in 24 paesi, in merito a quale tipologia di cloud utilizzano per le loro applicazioni aziendali e quale prevedono di utilizzare in futuro, alle problematiche degli ambienti cloud e a come i loro progetti cloud si sovrappongono rispetto ad altri progetti e priorità IT.
I dati ottenuti mostrano che, come in altre regioni, le aziende in Europa, Medio Oriente e Africa continuano a considerare il cloud ibrido come il modello IT 'ideale', ma che l'implementazione di tale approccio, con la migrazione delle applicazioni fuori dal data center, sta richiedendo più tempo di quanto previsto.
Anziché ridurre l'utilizzo dei data center di circa il 20% entro il 2019 (come previsto dagli intervistati nell'Enterprise Cloud Index EMEA 2018), il report di quest'anno evidenzia al contrario un aumento effettivo di quasi il 14%, di pari passo con un calo dell'utilizzo del cloud ibrido di circa il 5%, in contrapposizione al 7% di incremento previsto in precedenza.
Il risultato è che le aziende nella regione EMEA si trovano in ritardo di circa 6 punti percentuali rispetto alle Americhe nell'implementazione del cloud ibrido nonché in termini di adozione di un approccio multi-cloud.
Nonostante questi dati, tuttavia, le aziende intervistate indicano piani ambiziosi per rafforzare la penetrazione del cloud ibrido nella regione dall'attuale 12% al 53% entro il 2024.

L'impatto della sicurezza

Al fine di spiegare le disparità, il report rileva approcci contrastanti e meno entusiasmo in tutta la regione EMEA quando si prende in considerazione il ruolo del cloud pubblico in un progetto di cloud ibrido.
Per esempio, le aziende di quest'area hanno indicato la sicurezza dei dati e la conformità come i principali vantaggi del cloud pubblico più spesso (circa il 19%) di quanto le Americhe e la regione APJ abbiano scelto qualsiasi altro fattore, mentre, allo stesso tempo, più della metà (60%) considera la sicurezza una delle principali sfide del cloud pubblico.
Un minor numero di aziende nella regione EMEA riferisce che il cloud pubblico soddisfa "total-

Il modello cloud ritenuto più sicuro



mente" le loro esigenze rispetto ad altre regioni. Inoltre, in questa regione vi è una maggiore propensione a superare il budget stanziato per il cloud pubblico, cui si aggiunge la necessità di perfezionare i piani e, talvolta, di far rientrare i carichi di lavoro nel data center al fine di adeguarsi velocemente per l'implementazione del loro modello di cloud ibrido preferito.

I risultati del report per la regione EMEA evidenziano in particolare che:

- In linea con le tendenze globali, i piani di migrazione dai data center tradizionali verso il cloud ibrido - ipotizzati nel 2018 nella regione - non si sono ancora concretizzati. L'utilizzo dei data center è in realtà aumentato del 14% nel 2019, invece di diminuire come previsto nel report del 2018, mentre i dati del cloud ibrido sono diminuiti del 5% invece dell'incremento previsto.
- Nonostante la battuta d'arresto a breve termine, la regione riferisce di piani aggressivi per sostenere l'uso del cloud ibrido nei prossimi cinque anni. Si prevede che la penetrazione del cloud ibrido nella regione EMEA passerà dal 12% a circa il 53% entro il 2024.
- Le aziende della regione sono meno ottimiste nei confronti del cloud pubblico come parte di una strategia di cloud ibrido rispetto ad altre aree. Inoltre, sono anche leggermente meno propense a utilizzare un cloud privato gestito o ospitato come parte di un ambiente cloud ibrido delle aziende nelle Americhe e nell'area APJ.
- Per le aziende la sicurezza dei dati è uno dei principali vantaggi del cloud pubblico nonché la sua sfida più grande. Le aziende interpellate hanno scelto la sicurezza dei dati e la conformità come i principali vantaggi del cloud pubblico più spesso (circa il 19% delle volte) di quanto le Americhe e la regione APJ abbiano scelto qualsiasi altro fattore. Allo stesso tempo, tuttavia, più della metà (60%) considera la sicurezza una delle principali sfide del cloud pubblico.
- Le competenze IT esistenti e la portabilità delle applicazioni cross-cloud hanno una minore influenza nel processo decisionale rispetto ad altre regioni. Tutte le aree geografiche prese in considerazione ritengono che la sicurezza tra cloud abbia il maggior impatto potenziale sul futuro del cloud computing. Tuttavia, mentre il 46% delle aziende delle Americhe e quasi il 44% delle aziende in Asia-Pacifico ritengono le competenze IT esistenti fattori importanti per il processo decisionale, le controparti in EMEA rispondono con solo il 38%. Analogamente, il 42% e il 43% delle aziende nelle Americhe ed Asia-Pacifico, rispettivamente, hanno citato la portabilità delle applicazioni come il principale fattore di influenza del cloud, contro il 36% delle aziende della regione EMEA.

Veeam ha annunciato la Veeam Availability Suite V10

150 nuove funzionalità , il support NAS 3 e la Multi-VM Instant Recovery ampliano la disponibilità, la portabilità e l'estensibilità per il Cloud Data Management

Danny Allan, CTO e Senior Vice President of product Strategy di Veeam

Veeam Software, fornitore di soluzioni di backup volte ad abilitare il Cloud Data Management, ha annunciato la disponibilità della versione v10 della Veeam Availability Suite, versione che amplia le funzionalità per la protezione dei dati, la disponibilità, l'accesso e l'estensibilità dei dati.

Presentata per la prima volta nel 2008 come Veeam Backup & Replication, la soluzione fornisce, ha evidenziato l'azienda, una moderna protezione dei dati per i sistemi Networked Attached Storage (NAS), funzionalità Multi-VM Instant Recovery per automatizzare le attività di disaster recovery (DR) e una maggiore protezione dai ransomware.

«Come leader nel Cloud Data Management, la nostra priorità è stata quella di focalizzarci sulla creazione di una soluzione innovativa e di adattare i nostri prodotti alle esigenze dei clienti. la Nuova Veeam Availability Suite v10 è fedele a questi ideali e garantisce alle aziende di qualsiasi dimensione che i propri dati siano sempre accessibili e protetti in qualsiasi tipo cloud o piattaforma, in modo che possano utilizzarli intelligentemente per avere successo subito così come per pianificare le esigenze future» ha commentato **Danny Allan**, chief technology officer e senior vice president of product strategy di Veeam.

La risposta alle esigenze del cloud e del multicloud

La nuova versione vuole essere una risposta alle esigenze delle aziende che stanno adottando strategie di cloud ibrido per favorire una rapida trasformazione digitale e in quest'ottica i dati sono sempre più essenziali per il successo aziendale.

Secondo lo studio 2019 Veeam Cloud Data Management Report, il 73% delle aziende non riesce però a soddisfare la richiesta degli utenti di avere accesso continuo alle applicazioni e ai dati; oggi, molte aziende stanno adottando il Cloud Data Management per soddisfare al meglio le esigenze di protezione e per sfruttare appieno la potenza insita nei loro dati.

E' in questo scenario che si cala la v10, con cui Veeam ha ampliato la propria soluzione per supportare un numero sempre maggiore di piattaforme e fornire funzionalità evolute che

permettono alle aziende di avere un maggior controllo dei propri dati.
A livello funzionale Veeam Availability Suite v10 protegge i carichi di lavoro tramite nuove funzionalità di backup, fornisce maggiore sicurezza tramite backup non modificabili grazie alla funzionalità S3 Object Lock, e fornisce maggiori opzioni di integrazione dell'ecosistema di API.
In pratica, osserva l'azienda, la Suite v10, fornisce una protezione avanzata per qualsiasi applicazione, qualsiasi dato, su qualsiasi cloud. Suoi punti salienti sono:

- Ottimizzazione e semplificazione della protezione delle condivisioni di file di grandi dimensioni e di file server con potenti backup NAS.
- Business sempre operativo grazie all'engine Instant Recovery di nuova generazione e a funzionalità di Multi-VM Instant Recovery per proteggere le attività di disaster recovery da gravi interruzioni nel datacenter.
- Semplificazione del backup off-site e protezione da ransomware e minacce interne grazie all'integrazione dello storage di oggetti S3 e a backup non modificabili.
- Riutilizzo dei dati del backup per analisi in profondità e un'integrazione semplificata del software di analisi dei dati di terze parti con la Nuova API Veeam Data Integration.
- Piattaforma e ecosistema più ampi incluse nuove funzionalità per Linux, HPE Primera and HPE StoreOnce Nutanix AHV, PostgreSQL, MySQL.

La versione, che è disponibile, mantiene anche il supporto di Veeam per i servizi Microsoft Cloud, compresa l'integrazione con Veeam Availability Suite, Veeam Backup for Office 365 e Veeam Backup for Azure.

Vertiv ha ampliato il Customer Experience Center

Le funzionalità disponibili per i clienti abilitano severi test delle unità di alimentazione e la verifica della flessibilità e dell'efficienza di un data center

La trasformazione dell'IT, oltre che sui dispositivi di utente quali Pc, dispositivi portatili e apparati di rete, implica un profondo ripensamento di quanto necessario a mantenere in esercizio e manutenere in modo che sia sempre al massimo dell'efficienza e della disponibilità, quello che è il cuore di un sistema informativo, il Data Center.
L'evoluzione del Data Center sta seguendo due strade, a secondo delle esigenze. Una è quella della sua distribuzione in unità più piccole in modo da portare la capacità di calcolo all'edge di una rete.
Una seconda è quella che vede il potenziamento del sistema centrale per metterlo in grado di supportare maggior capacità elaborativa, di storage e di connettività.

Verifica delle espansioni in condizioni reali

Soprattutto nel secondo caso, un elemento chiave a cui diventa impossibile rinunciare è l'esigenza di business continuity ed il fatto che il data center operi in condizione di "always-on".
Il problema è che mentre un server lo si può installare in un impianto pilota, e lo stesso si può fare per un router o una batteria di storage, farlo con un Data Center diventa praticamente impossibile, sia in termini di costi che di spazi necessari.
Verificare se una soluzione progettata sulla carta è realmente adatta a supportare il carico di lavoro previsto e con che limiti è però una cosa indispensabile prima di procedere con l'installazione o l'espansione di un data center.
Un aiuto alle aziende alle prese con questo critico problema, che potrebbe rallentare la trasformazione in chiave digitale di un'azienda e metterla in difficoltà nei confronti dei competitor, si è proposta di darlo Vertiv, società con circa 20.000 dipendenti che opera in oltre 130 paesi e che progetta, realizza e fornisce hardware, software e servizi di diagnostica e monitoraggio per la continuità operativa di applicazioni mission critical.
Il suo portfolio comprende nello specifico soluzioni e servizi per la continuità elettrica e il raffreddamento delle infrastrutture IT, che si estende dal cloud fino ai dispositivi connessi in rete.

Customer Experience Center a portata di mano delle aziende

Vertiv, proprio per supportare le aziende nelle decisioni inerenti i data center, ha dato il via all'espansione del suo Customer Experience Center di Bologna.
Il piano di ampliamento prevede l'inserimento di una nuova infrastruttura di alimentazione da

4MVA per sostenere le funzionalità di test, la flessibilità e l'efficienza.
I miglioramenti che verranno apportati sono volti in sostanza ad aiutare le aziende nel fare scelte ponderate per quanto concerne alle esigenze dei data center e impianti industriali più grandi, e rispondere alla crescente necessità di estendere i test preliminari fuori sede per accelerare le implementazioni del proprio sito.
I miglioramenti pianificati raddoppieranno la capacità di test attualmente disponibile per grandi gruppi di continuità (UPS), con la disponibilità di fino a 7,5MVA di potenza e la capacità di ospitare sei sessioni simultanee.
La struttura è comunque già in grado, ha spiegato l'azienda, di eseguire test di capacità utilizzando carichi rigenerativi con un principio di power-loop che consente di riutilizzare circa il 96% dell'energia ed evitare così inutili sprechi energetici.
Pianificati nell'ampliamento è anche la possibilità di realizzare test efficienti e approfonditi, tra cui test dinamici sulle batterie, un simulatore di circuito a Corrente Continua per replicare qualsiasi tipo di batteria e la capacità di testare i sistemi a 480V.

Esperti a disposizione

Va osservato che l'investimento programmato da Vertiv giunge sei anni dopo l'apertura del Customer Experience Center, che alla sua apertura costituiva l'unica struttura in Europa appositamente progettata per la convalida dell'infrastruttura del data center e dove era possibile effettuare le dimostrazioni di preinstallazione con evidenza delle prestazioni tecniche, dell'interoperabilità e del rendimento dei sistemi UPS di Vertiv in condizioni operative realistiche.

Andrea Ferro - Direttore della Divisione AC Power EMEA di Vertiv

A tutt'oggi, la struttura consente di sperimentare direttamente numerose tecnologie con il supporto degli esperti di R&D e degli ingegneri di Vertiv. Sul piano realizzativo il completamento delle fasi di ampliamento della struttura è previsto entro il 2021, con la prima fase già a inizio 2020.
«Il centro era all'avanguardia quando aprì i battenti sei anni fa e oggi continua a promuovere l'innovazione. Questo ulteriore investimento testimonia il costante impegno di Vertiv verso i nostri clienti in continua crescita, in quanto ci consentirà di condurre più test contemporaneamente. L'opportunità unica di verificare di persona l'affidabilità e l'efficacia dei prodotti Vertiv in una serie di condizioni realistiche si traduce in una maggiore tranquillità per i nostri clienti», ha commentato **Andrea Ferro**, direttore della divisione AC Power per Europa, Medio Oriente e Africa di Vertiv.