

LA RIVISTA PER IL MANAGER CHE DEVE OTTIMIZZARE COSTI E PROCESSI

PAG. 01-05» Il lavoro agile richiede più attenzione e maggior sicurezza

PAG. 06» Nuovo PoP per il Global Cloud Data Center di Aruba

PAG. 07» collaborazione più facile con il Digital Workplace

PAG. 08» CIE assicura la sicurezza delle piccole e medie imprese

PAG. 09-10» Con HPE il 5G diventa as-a-service

PAG. 11» Soluzioni e esperti IBM abilitano la scuola a distanza

PAG. 12» Automotive più smart con il VoIP su reti IP e in cloud

PAG. 13» L'app di Italtel per monitorare le persone sotto presidio sanitario

PAG. 14» Smart Working più semplice e sicuro con il desktop virtuale

PAG. 16» Pbx virtuale e fibra abilitano servizi di UCC evoluti

PAG. 17» Con Snom SRAPS servizi a valore erogati anche da casa

PAG. 18» FAAC sceglie il digital workplace per produttività e competitività

PAG. 19» Da Vertiv e Uptime Institute data center modulari TIER-Ready

Il lavoro agile richiede più attenzione e maggior sicurezza

di Giuseppe Saccardi

Il ricorso a servizi di connettività e reti come il cloud, al di fuori del perimetro aziendale, espone web, dati e mail a maggiori rischi

I detti per riferirsi al momento attuale sono numerosi e risalgono ad epoche diverse. Extreme times call for extreme measures, dicono gli anglosassoni, mala tempora currunt, gli antenati latini, che nei momenti veramente difficili ricorrevano anche al detto dal sapore scaramantico probabilmente risalente agli albori dell'umanità stessa "in omnia pericula tasta".

Facile immaginare a quale gesto scaramantico, peraltro ancora in voga, si riferissero e



Nel lavoro agile meglio non affidarsi alla scaramanzia

comunque indicativo come di momenti critici nel passato l'umanità non sia stata di certo avara ma che, visto che se ne parla, alla fine li abbia superati tutti.

Tornando all'oggi uno degli imperativi del momento, e dove più che dalla scaramanzia ci si attende un aiuto dalla tecnologia e dalla ricerca scientifica, è quello di come mantenere attivi i canali di comunicazione e cooperazione in un mondo fortemente, e verrebbe da aggiungere forse sin troppo, globalizzato e interconnesso e dove si sta dimostrando che ogni medaglia ha il suo rovescio.

In sostanza, la domanda che ci si pone è in che modo l'attuale tecnologia permette alle aziende di continuare ad operare in momenti come quello che si sta attraversando.

Posti di fronte ad una situazione imprevista le aziende hanno dovuto studiare come continuare a operare in un mondo virtuale, facendo leva sulla tecnologia e sulle reti esistenti per infondere stabilità e ridurre al minimo le interruzioni delle loro attività.

In questo, le tecnologie di collaborazione, come le conferenze web e il project management, consentono ai dipendenti di lavorare da casa, mantenendo l'operatività.

Quello che però si rivela essenziale è che strumenti e applicazioni utilizzati online siano sicuri e protetti, e che lo siano i dati, per evitare che aggressori possano sfruttare questi momenti di difficoltà per i loro fini ed aumentino ulteriormente la criticità per le aziende.



Il problema della comunicazione

In uno scenario sotto forte pressione la diffusione, obtorto collo, di soluzioni per il lavoro agile, o smart working, implica il ricorso a infrastrutture esterne all'azienda, e di conseguenza un maggior rischio. In sostanza, se lo scambio di dati ed informazioni prima basate su reti di connessione di proprietà e fortemente controllate garantiva un adeguato livello di sicurezza, con l'apertura al mondo esterno in modo massiccio, questo non è più necessariamente vero.

In pratica, pur di mantenere attivo il workflow si viene a creare una interazione diretta da utente a utente che, realizzata in ambienti extra azienda e mediante connessioni che la bypassano, può mettere un grosso punto interrogativo sulla sicurezza dei dati scambiati o ricevuti.

Ricevere una mail, realizzare una videoconferenza con scambio di dati nel corso della sessione realizzata tramite un provider, collegarsi come utente all'ambito aziendale, eccetera,

e farlo mediante ambienti cloud di cui non si ha il controllo e non si sa esattamente cosa forniscono a livello di sicurezza, può costituire un passo falso foriero di forti dispiaceri.

Gli allarmi che provengono dal mondo tecnico e dagli esperti di aziende impegnate nella cyber security non vanno presi alla leggera. Questo vale in condizioni normali, ma ancor di più ora.

Se nella lotta ai cybercriminali non si deve mai calare la guardia, questo non va fatto nemmeno, e viene da dire soprattutto, proprio nei momenti più critici quando per motivi anche validi e spinti dalla necessità di essere comunque operativi si può essere portati a calare il livello di attenzione.

Una dimostrazione è ad esempio che crescono e diventano sempre più sofisticati gli attacchi di phishing che sfruttano l'emergenza Coronavirus e che possono trovare spazio per entrare in azione soprattutto laddove manca un congruo filtro aziendale o una specifica cultura da parte dell'utente che, se operante al di fuori del perimetro aziendale, può essere portato a pensare di operare in un contesto che goda degli stessi privilegi e livelli di sicurezza di quando si trova in ufficio.

In proposito i ricercatori di Barracuda, società fortemente impegnata nello sviluppo di soluzioni di sicurezza on-premise e nel cloud, hanno segnalato il verificarsi di un costante aumento del numero di attacchi via email collegati al Coronavirus dilagato dalla Cina da gennaio scorso e osservato un recente picco in questo tipo di attacco, in crescita del 667 per cento dalla fine di febbraio.

Tra l'1 e il 23 marzo, ad esempio, Barracuda Sentinel ha rilevato 47.825 attacchi spear

phishing email e di cui ben 9.116 di questi rilevamenti collegati al Coronavirus.

Per fare un raffronto, in febbraio erano stati rilevati 1.188 attacchi email relativi al Coronavirus e a gennaio solo 137. Mese su mese più che decuplicati. Sebbene il numero complessivo di questi attacchi sia ancora basso rispetto ad altri, è però indicativo di come la minaccia stia crescendo rapidamente.

Cosa fare per proteggersi

Sic stantibus rebus, viene da chiedersi cosa sia possibile fare per proteggersi prendendo ad esempio in considerazione il caso delle mail, che al di fuori del contesto aziendale possono essere scambiate, inviate e ricevute utilizzando dispositivi non aziendali e al di fuori delle più stringenti pratiche di protezione. I suggerimenti in proposito degli specialisti di Barracuda per la sicurezza della posta elettronica sono lapidari, alcuni intuitivi ed altri meno:

- Diffidare di email che cerchino di indurre ad aprire allegati o a cliccare sui link. Le soluzioni anti-malware e anti-phishing possono essere particolarmente utili per impedire a email e payload dannosi di raggiungere i destinatari predestinati, ma anche con tali protezioni in atto si dovrebbe sempre usare cautela poiché nessuna soluzione è efficace al 100%.
- Attenzione a comunicazioni da fonti dalle quali non si ricevono email. Questi sono probabilmente tentativi di phishing. Mentre ricevere email relative al coronavirus da liste di distribuzione legittime a cui si appartiene sta diventando frequente, le email di organizzazioni dalle quali non si

ricevono regolarmente messaggi dovrebbero essere esaminate attentamente.

- Cautela con le email di organizzazioni con cui si comunica regolarmente. La brand impersonation è piuttosto diffusa negli attacchi email relativi al coronavirus; è necessario quindi fare attenzione quando si aprono email che si prevede di ricevere da una determinata organizzazione..
- Enti di beneficenza. Una tattica delle truffe è la richiesta di donazioni per aiutare le persone ammalate. Per evitare di cadere vittima di uno di questi attacchi, non rispondere alle richieste via email di donazioni. Invece, è meglio individuare enti di beneficenza conosciuti e donare direttamente a loro per essere sicuri che i fondi finiscano dove possono fare del bene piuttosto che nelle mani dei truffatori.

Superficie di attacco estesa e rischi

Un fattore di rischio nel lavoro remoto e realizzato tramite infrastrutture disperse fisse e mobili, reti VPN o cloud e relativi dispositivi di utente, è dato dal fatto che si moltiplicano i punti che possono essere fruiti da malintenzionati per superare le difese, entrare nei sistemi e muoversi una volta entrati in ogni direzione. In pratica, ampliando la superficie esposta aumentano in modo esponenziale i rischi.

In pratica, lo smart working distribuisce e amplia la superficie in cui si può lavorare, ma lo possono fare non solo i lavoratori ma anche i malintenzionati, che comunque sono pur sempre dei lavoratori, seppure sui generis e che sfruttano computer, cellulari e email per accedere ad applicazioni e dati critici dell'azienda.

zienda.

Va poi considerato che molte imprese oggi si affidano a fornitori esterni per gestire porzioni della loro infrastruttura IT e, per farlo, queste organizzazioni devono disporre di un accesso privilegiato ai sistemi IT dell'azienda. Tuttavia, l'estensione degli accessi privilegiati a provider terzi può essere difficile quando ci si affida a sistemi di autenticazione e autorizzazione degli utenti convenzionali. I motivi sono svariati:

- I tradizionali sistemi di gestione dell'identità e le soluzioni di controllo degli accessi, progettati per l'autenticazione dei dipendenti aziendali e dei dispositivi di proprietà dell'azienda, non sono adatti a garantire la sicurezza del personale di terze parti e dei dispositivi esterni.
- La maggior parte delle aziende ha scarsa o nulla visibilità o controllo sull'accesso remoto alla rete aziendale. Fornire postazioni di lavoro a ogni fornitore non è una strategia applicabile e l'implementazione di VPN o agenti su laptop o desktop di un'altra azienda è spesso troppo oneroso da gestire per i team IT.
- Personale e requisiti di accesso possono cambiare da un giorno all'altro, rendendo poco o punto praticabili i tradizionali schemi di gestione delle identità basati su ID utente e password.
- Con un perimetro flessibile e una crescente dipendenza dalle attività in outsourcing, i team di sicurezza devono trovare modi innovativi per garantire ai fornitori esterni un accesso sicuro agli account privilegiati senza interrompere le operazioni.

Ce n'è per un SIO e un CIO, ma anche per



il board aziendale, che in fin dei conti è responsabile ultimo della protezione dei dati aziendali, abbastanza per passare delle notti inquiete.

Al sicuro con autenticazione a più fattori e biometria

Per dare una mano ad affrontare il momento difficile CyberArk, società attiva nello sviluppo di soluzioni on-premise e nel cloud per la protezione degli accessi privilegiati, si è proposta di aiutare le aziende nel risolvere le esigenze di Business Continuity accelerandone il processo ed estendendo una sua soluzione, la CyberArk Alero, a fornitori e dipendenti che devono accedere ai sistemi critici interni.

Si tratta, nella sua essenza, di una soluzione che combina accesso Zero Trust, autenticazione biometrica a più fattori e provisioning just-in-time in un'unica soluzione erogata sotto forma di SaaS. Tra gli obiettivi perseguiti dalla soluzione ed evidenziati dall'azienda,

va annoverato che:

- Può essere configurata rapidamente per consentire alle aziende di mettere in sicurezza la propria infrastruttura IT e le informazioni sensibili.
- Mitiga i rischi per la sicurezza tramite un approccio Zero Trust Access.

In pratica, assicura che i fornitori accedano solo a ciò di cui hanno bisogno.

- Non richiede VPN, agenti o password, e consente l'accesso dei fornitori attraverso sessioni tracciabili.
- Fornisce un accesso privilegiato senza password ai fornitori che hanno bisogno di accedere a sistemi interni critici.

Comunque, volendo dare un aiuto al detto scaramantico latino con comportamenti pratici, CyberArk suggerisce ai dipendenti che lavorano da casa, collegati tramite reti di incerta sicurezza, di mantenere i dispositivi mobili e i computer portatili al sicuro con password e crittografia, utilizzare la cifratura, l'autenticazione a più livelli e il blocco delle sessioni per proteggere i dati e, non ultimo, mantenere hardware e software aggiornati e dotati delle più recenti patch. La tecnologia aiuta di certo, ma di aiuto è di sicuro anche il buon senso.

Nuovo PoP per il Global Cloud Data Center di Aruba

L'attivazione del PoP di Cogent ha messo a disposizione dei clienti di Aruba un operatore Tier 1 che espande l'offerta di connettività del provider

Aruba, società attiva nei servizi di data center e cloud enterprise, ha annunciato l'attivazione del Point of Presence di Cogent, un Internet Service Provider, all'interno del Global Cloud Data Center, il campus data center di Aruba di Milano.

Il Point of Presence (PoP) consentirà in pratica ai clienti Aruba di disporre dalla rete internazionale di Cogent che si estende in tutto il Nord America, l'Europa e l'Asia attraverso oltre 92.000 km di fibra intercity e oltre 56.000 km di fibra metro, rete che fornisce servizi a oltre 204 mercati e collegandosi con oltre 6.840 ulteriori reti.

La presenza di Cogent si aggiunge ad altre e espande la rosa di carrier disponibili all'interno di Global Cloud Data Center.

Va osservato che Global Cloud Data Center, così come gli altri Data Center Aruba, è carrier neutral, per cui al suo interno sono ospitati numerosi operatori di telecomunicazioni con cui i clienti possono gestire in autonomia i propri rapporti di partnership:

In questo contesto Cogent è una ulteriore possibilità di tipo Tier 1 che si aggiunge a TIM, Fastweb, Wind-Tre, Retelit, Irideos, Planetel e



Vodafone.

«Abbiamo aggiunto valore alla nostra punta di diamante: l'ingresso di un operatore come Cogent, Tier 1 di livello internazionale all'interno di Global Cloud Data Center, oltre a porre il Data Center tra le possibili scelte a disposizione su scala mondiale, sta anche apportando numerosi vantaggi ai nostri clienti grazie ad un transito Internet di qualità», ha commentato Lorenzo Giuntini, CTO di Aruba.

Già lo scorso anno, Aruba aveva annunciato l'attivazione di un Point of Presence del Milan Internet eXchange (MIX) direttamente accessibile da Global Cloud Data Center. Un accordo che prevedeva l'aggiunta di nuove interconnessioni grazie agli apparati collegati a Milano in doppia via in fibra, così da facilitare lo scambio di traffico con numerosi altri carrier nazionali ed internazionali.

Collaborazione più facile con il Digital Workplace

Il Digital Workplace di Centro Computer aiuta l'impresa nello sviluppo competitivo e migliora i processi interni di business



Mirco Balboni - Centro Computer

A differenza del posto di lavoro fisico 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, ridurre i tempi di sviluppo e costruire uno spazio di condivisione. Ma diventa prioritario scegliere lo strumento tecnologico più adatto ai fini degli obiettivi.

Centro Computer, società di consulenza specializzata in prodotti, servizi e soluzioni IT per le aziende, ha spinto l'acceleratore sui progetti di Digital Workplace per le aziende che vogliono cogliere le nuove sfide della trasformazione digitale, assicurando una gestione efficiente dei canali organizzativi e l'utilizzo delle tecnologie più avanzate. I progetti sono basati su Microsoft Office 365, l'innovativa suite su cloud che consente di lavorare ovunque e su qualunque dispositivo, con le soluzioni di video conferenza HD di Logitech, Poly ed i dispositivi audio di Jabra e Plantronics.

«Riscontriamo sul mercato molte richieste che coinvolgono il Digital Workplace - ha sottolineato Mirco Balboni, Business Developer Manager Cloud & UC di Centro Computer - 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».

La piattaforma Microsoft Office 365 e in particolare Microsoft Teams, assicurano strumenti collaborativi di UC per le aziende di qualsiasi dimensione, mentre con OneDrive for Business è possibile archiviare, sincronizzare e condividere i file di lavoro in cloud. Con Microsoft Yammer inoltre ci si assicura il social network aziendale che consente di collaborare e rimanere aggiornate su quello che succede in azienda. Infine, con Microsoft Teams, l'Hub di Office 365 che integra persone, contenuti e strumenti per rendere le persone sempre più coinvolte, si può integrare la fonia nei progetti di Intelligent Communication e Digital Workplace. «Inoltre, la trasformazione digitale sta spingendo le imprese a valutare con estrema attenzione la nostra soluzione di 'Fleet Management' - ha evidenziato Balboni - lo 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».

CIE assicura la sicurezza delle piccole e medie imprese

I firewall della serie Check Point 1500 forniti da CIE Telematica preven- gono le minacce, migliorano la sicurezza della mail e abilitano una protezione zero-day

Se per una grande azienda che dispone di un team dedicato di sicurezza e capacità di investimenti il problema di come organizzare il lavoro e la protezione dei dati se non semplice è perlomeno gestibile, ben più critica è la cosa quando si tratta di una media o piccola azienda.

Quello delle PMI è un contesto dove raramente si dispone del know how e dei budget per approntare progetti che prevedano la selezione di soluzioni adatte alle specifiche esigenze produttive e settoriali, realizzare confronti e tantomeno impianti di test e di valutazione in campo.

Un aiuto alle PMI è quello offerto da CIE Telematica, società di ingegneria indipendente con esperienza trentennale nelle reti fisse e mobili e nella sicurezza che ha selezionato un portfolio di prodotti adatti a rispondere alle esigenze specifiche di cyber security delle PMI.

Tra le piattaforme selezionate da CIE Telematica vi sono ad esempio i firewall di nuova generazione Check Point SMB della serie Check Point 1500. Sono dei gateway ad alte prestazioni che sono stati sviluppati dall'azienda specializzata con l'obiettivo di fornire un elevato grado di prevenzione delle minacce, migliorare la sicurezza della posta elettronica e abilitare una protezione



di tipo zero-day.

In pratica, ha osservato Luigi Meregalli, general manager di CIE Telematica, si tratta di una soluzione che consente di rispondere agli eventi di sicurezza in tempo reale tramite anche un portale di gestione unificato. Permette anche di disporre in mobility e gestire la propria sicurezza tramite una apposita app mobile.

A livello di portfolio di soluzioni disponibili i gateway di sicurezza della serie 1500 estendono ulteriormente la famiglia di dispositivi di sicurezza per piccole imprese già disponibile, prodotti a cui hanno aggiunto protezioni di sicurezza a più livelli in un fattore di forma compatto da 1 unità rack adatto per ambienti quali quelli delle PMI ma in grado di assicurare la protezione di fino a 300 utenti, realtà tipiche queste di una filiale anche di medie dimensioni o di piccoli uffici.

Come evidenziato, il firewall dispone di targa di robuste caratteristiche operative. In particolare:

- E' consigliato da NSS (National Security Strategy)
- Presenta una frequenza di blocco del 100%.
- Provisioning Zero Touch out-of-box ,
- App mobile per la sicurezza in viaggio
- Portale di gestione unificato

«Check Point Small Business Appliances ci offre sicurezza di livello aziendale in una soluzione di sicurezza all-in-one» ha dichiarato Trevor Rowley, amministratore delegato della società di software per la gestione aziendale Optix.

Con HPE il 5G diventa as-a-service

Il portfolio HPE GreenLake fa leva sulle tecnologie cloud-native di HPE e Aruba per le telecomunicazioni per abilitare reti 5G e Wi-Fi integrate



Phil Mottram -
Communications and media Solutions BU di HPE

Hewlett Packard Enterprise (HPE) ha annunciato un nuovo portafoglio di soluzioni as-a-service per aiutare gli operatori di telecomunicazione a creare e implementare reti 5G aperte. La soluzione ha l'obiettivo di abilitare rapidamente servizi 5G per fornire esperienze real-time dinamiche e personalizzate a dipendenti, clienti e cittadini in genere.

La strategia Edge-to-Cloud, Platform as-a-service di HPE, fa leva su uno stack software cloud-native per la parte core della rete 5G, su sistemi per infrastrutture edge e core ottimizzati per le telecomunicazioni, e su servizi compatibili con Wi-Fi 6.

E' stata costruito sulla base di piattaforme aperte e interoperabili combinate con un'infrastruttura carrier-grade e componenti software modulari. La soluzione è in sostanza volta a consentire agli operatori di raggiungere un maggior grado di automazione, aumentare l'agilità e implementare più velocemente nuovi servizi 5G attraverso il core e l'edge della rete di telecomunicazione fino a estendersi all'interno degli ambienti enterprise. "L'essere open è strettamente legato alla natura evolutiva del 5G, e con HPE 5G Core Stack le compagnie di telecomunicazione possono ridurre

re i costi operativi, attivare funzionalità più rapidamente e tenersi aperte in direzione di più reti e tecnologie evitando di restare bloccate all'interno di un approccio monofornitore", ha dichiarato Phil Mottram, vice president e general manager della Communications and Media Solutions business unit di HPE.

Nuovo scenario tecnologico

Va osservato, ha evidenziato HPE, che il 5G promette di rivoluzionare lo scenario tecnologico, ma il cammino che conduce alla diffusione pervasiva del 5G è ancora nelle sue fasi iniziali.

Per concretizzare completamente i vantaggi e la potenza del 5G occorre combinare una core 5G indipendente con le nascenti RAN (Radio Access Network) 5G. Le reti di precedente generazione sono spesso dipese da sistemi proprietari verticalmente integrati forniti da un unico vendor, ma il 5G offre l'opportunità di passare a piattaforme cloud-native aperte che si avvalgono di server commerciali e componenti modulari di produttori differenti, consentendo agli operatori di monetizzare i nuovi servizi 5G con maggior rapidità. Inoltre, le frequenze più alte del 5G fanno fatica a penetrare all'interno degli edifici imponendo

quindi agli operatori di ricorrere a reti 5G sia con tecnologia RAN che Wi-Fi 6 per poter garantire un servizio senza interruzioni ai clienti che si recano nei centri commerciali, nei campus e nei palazzi di uffici.

In particolare, HPE 5G Core Stack è uno stack software cloud-native basato su container per la rete core 5G che si integra con le reti di precedente generazione. Sarà disponibile come piattaforma hardware e software integrata basata su modelli per core ed edge convalidati HPE Telco e supportata all'interno di HPE GreenLake.

Più flessibilità con la Container Platform

HPE ha reso disponibile anche HPE Container Platform, una soluzione presentata in origine nel novembre dello scorso anno.

È una piattaforma per container di livello enterprise progettata per supportare applicazioni cloud-native e non-cloud-native utilizzando il sistema open source Kubernetes per rendere possibili implementazioni in ambienti bare-metal o su virtual machine (VM), all'interno dei datacenter, su cloud pubblico o all'edge.

La società ha anche rilasciato dei nuovi servizi professionali il cui obiettivo, ha spiegato, è quel-

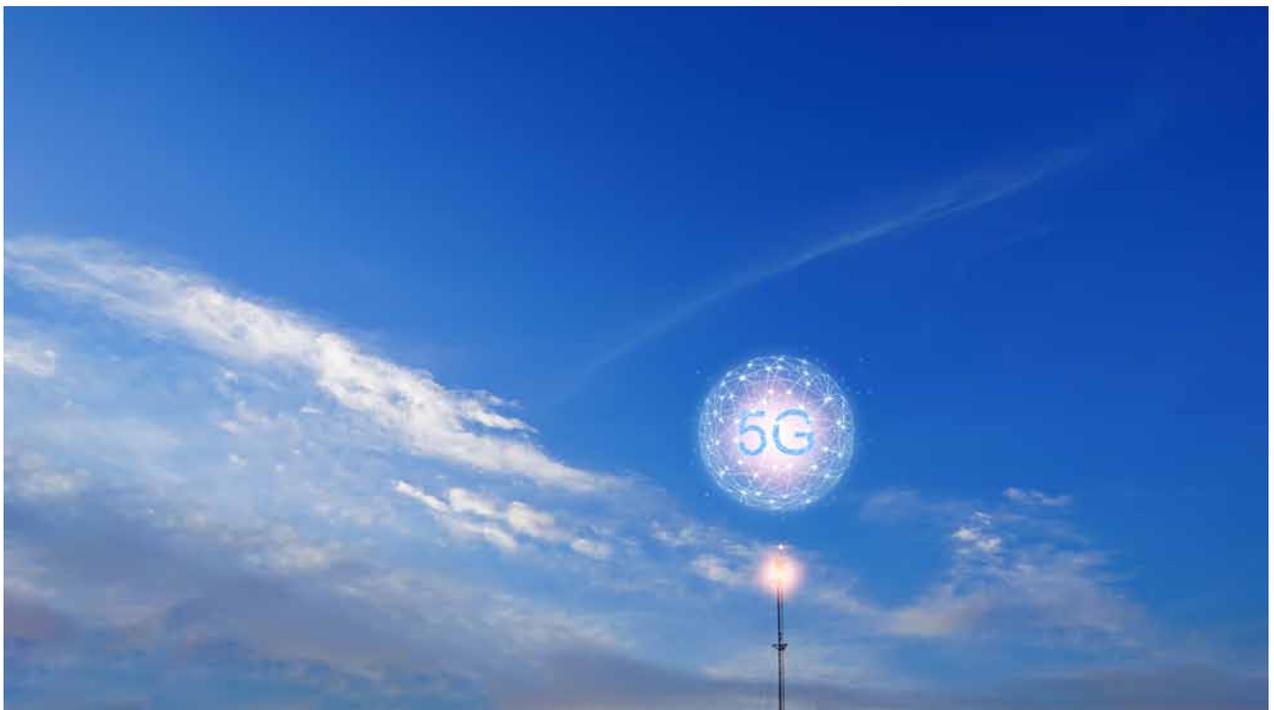
lo di fornire un time-to-value più veloce e diverse nuove architetture di riferimento per carichi di lavoro applicativi a uso intensivo di dati come AI, machine learning, deep learning, data analytics, edge computing e Internet of Things.

La soluzione è dovuta alla considerazione di HPE che molte aziende hanno iniziato ad avvalersi dei container con workload di tipo stateless, la cui transizione verso un'architettura di microservizi cloud-native risulta più semplice.

Tuttavia, la maggioranza delle applicazioni business prevede oggi workload di tipo monolitico, stateful e non-cloud-native diffusi nell'intero ambito enterprise.

Le aziende stanno quindi cercando di modernizzare e containerizzare queste applicazioni senza dover svolgere un lavoro di rinnovamento impegnativo, garantendo comunque la sicurezza necessaria alla produzione e uno storage di dati persistente.

In un tale scenario la Container Platform ha l'obiettivo di permettere il contenimento dei costi e della complessità nell'utilizzo dei container in ambienti bare-metal, lasciando la flessibilità necessaria per poter completare le installazioni all'interno di VM o istanze cloud.



Soluzioni e esperti IBM abilitano la scuola a distanza

IBM ha messo a disposizione degli studenti il proprio supporto e una piattaforma UCC che permette di continuare a seguire le lezioni durante l'emergenza in atto

IBM, a conferma del suo costante impegno nel sociale, ha comunicato di essersi mobilitata a supporto del sistema scolastico italiano offrendo l'accesso alla piattaforma di collaborazione Cisco Webex, dotata di funzionalità intuitive per l'educazione online, assieme ad un servizio di assistenza e supporto per docenti e studenti.

La decisione è una concreta e rapida risposta, in un momento in cui il tempo è poco e le decisioni devono essere rapide, ha evidenziato l'azienda, all'appello del Ministero dell'Istruzione per fronteggiare la crisi generata da Covid-19 e si inserisce nell'iniziativa di Solidarietà Digitale voluta dal Ministero per l'Innovazione.

La piattaforma, che è a disposizione fin dai primi giorni della pandemia, è in grado di collegare studenti e insegnanti in tempo reale.

Ad oggi, più di 80 scuole stanno già utilizzando la soluzione per fornire, attraverso le lezioni virtuali, un servizio essenziale a circa 50.000 studenti italiani. Inoltre, il numero delle scuole aderenti è in continua crescita.

«Vogliamo partecipare con i nostri professionisti e la conoscenza di cui disponiamo allo sforzo collettivo per alleviare gli effetti della crisi sanitaria. Il nostro obiettivo, come azienda a supporto del sistema paese, è quello di creare innovazioni



Enrico Cereda - IBM

a supporto della società, delle aziende e del bene comune. In questa particolare occasione, siamo orgogliosi di poter contribuire, coniugando tecnologia e volontariato, a dare continuità alle lezioni scolastiche degli studenti italiani», ha osservato Enrico Cereda, Presidente e Amministratore Delegato di IBM Italia

Una classe virtuale su misura

Sul piano pratico la piattaforma è disponibile in tutte le regioni italiane ed è in grado di supportare diversi tipi di esigenze anche per altre aree amministrative che, in questo momento, potrebbero beneficiare di uno strumento di collaborazione da remoto.

In particolare, la versione Meetings comprende sia la possibilità di effettuare video-conferenze che di condividere desktop, applicazioni e risorse multimediali in tempo reale.

Sono funzionalità, ha spiegato IBM, che permettono di creare una classe virtuale a tutti gli effetti, a cui gli studenti possono accedere in modalità ospite, senza la necessità di creare un account.

Tutto viene amministrato dall'area personale dell'insegnante, che può "invitare" gli studenti, gestire audio e microfoni di ognuno – dando loro la parola quando necessario – e può registrare la lezione per condividerla o rivederla in seguito. IBM ha anche messo a disposizione della comunità degli insegnanti un servizio di supporto per l'adozione e l'utilizzo della piattaforma, erogato da 350 esperti e volontari dell'azienda.

Automotive più smart con il VoIP su reti IP e in cloud

Migrare al VoIP permette di dotarsi di un'infrastruttura resiliente e sicura in grado di integrarsi con il CRM, gli strumenti di BI e di gestione del workflow



Michele Piccini -
IPKom

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 l'unico 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 è approdati in quello più ampio delle applicazioni business anche in settori sino ad ora poco permeabili.

«Nelle 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 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.

Sono numerosi 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 incomplete» 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 di dover spiegare a terzi l'intera situazione più volte per essere poi inoltrato al collaboratore di riferimento; permette invece all'addetto di essere informato automaticamente della chiamata ricevuta, di registrare tale informazione nel CRM o in sistemi di gestione del workflow, qualora in quel momento l'addetto non possa effettivamente rispondere.

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.

L'app di Italtel per monitorare le persone sotto presidio sanitario



Una soluzione di telemedicina pensata per il monitoraggio di persone sottoposte a presidi sanitari, deospedalizzate o che vengono curate presso le loro abitazioni

Italtel ha risposto alla call del Governo "Innova per l'Italia" con una soluzione di telemedicina pensata per il monitoraggio di persone sottoposte a presidi sanitari, deospedalizzate o che vengono curate presso le loro abitazioni.

La soluzione consente la continuità assistenziale dell'ospedale o del presidio medico con il territorio attraverso la trasmissione dei parametri clinici verso gli operatori sanitari che gestiscono il piano di assistenza individuale. Permette il teleconsulto e il telemonitoraggio per il singolo paziente o per l'intero nucleo familiare garantendo la privacy e la sicurezza dei dati personali.

E' costituita da una app caricabile su tablet con sistema operativo Android che attraverso sensori connessi rileva i parametri vitali della persona e li invia al personale sanitario. I sensori misurano battito cardiaco, ossigenazione del sangue, temperatura, pressione, ECG, spirometria. Il medico, in base ai parametri ricevuti può contattare il paziente in video chiamata ed effettuare un consulto online. Il paziente può visualizzare la terapia inviata dal medico, lo storico delle misurazioni, ricevere un promemoria per l'assunzione di un farmaco e mettersi in contatto con il personale medico in chat o in videoconferenza.

L'app utilizza la tecnologia WebRTC (Real Time

Communication) e IoT. La soluzione è già stata testata in Italia dall'Ospedale S. Martino di Genova, in Sudafrica dall'Ospedale Mamelodi di Pretoria e in Svizzera.

Italtel sta anche collaborando con diversi operatori di telecomunicazioni che in queste ore stanno lavorando per rispondere a "Innova per l'Italia". Tra le componenti di base di tali proposte c'è anche la componente Italtel legata alla telemedicina e al monitoraggio dei parametri vitali.

Oggi il 95% dei circa 1000 dipendenti di Italtel in Italia è in smart working nelle tre sedi di Milano, Roma Palermo. Il restante 5% è impiegato in attività in esterno e presso le sedi dei nostri clienti, per assicurare la continuità dei servizi di pubblica utilità e dei servizi essenziali quali sanità, telecomunicazioni e media.

Nell'ambito sanitario la società sta lavorando in questi giorni per i grandi gruppi ospedalieri milanesi per predisporre le infrastrutture di rete, i servizi di comunicazione e gli aspetti di sicurezza nei reparti di terapia intensiva.

Stiamo lavorando per garantire la continuità e la tenuta delle infrastrutture di telecomunicazione, messe particolarmente sotto pressione da smart working, e-learning e dall'impennata dello streaming video.

Dall'inizio dell'emergenza i dipendenti lavorano in modalità remota per attivare le licenze di Cisco Webex utilizzate per fare smart working. Le utenze attivate appartengono a grandi e medie aziende, scuole e PA.

Smart Working più semplice e sicuro con il desktop virtuale

I nuovi ThinOX4PC e ThinMan di Praim abilitano lo Smart Working sicuro da ogni postazione e con qualsiasi dispositivo



Mobilità, flessibilità, facilità di implementazione e di manutenzione, sicurezza, eccetera sono di certo caratteristiche molto importanti per le aziende in cerca di soluzioni a sostegno dei loro collaboratori che lavorano da remoto e a sostegno dei nuovi paradigmi di lavoro come il Nomad Work, lo Smart Working o la mobilità tra sedi e postazioni.

Il problema è però come passare dalla teoria alla pratica ottimizzando gli investimenti e minimizzando i rischi di trovarsi in casa una piattaforma che si rivela poi poco adatta e flessibile.

Una risposta l'ha ideata Praim con le soluzioni VDI di desktop virtuali abbinata a un software che consente di affrontare le sfide citate più tranquillamente a partire dall'amministratore IT sino all'utente finale.

In pratica, ha evidenziato l'azienda, una soluzione come il suo nuovo ThinOX4PC consente ad esempio di trasformare qualsiasi dispositivo in un Thin Client aziendale sicuro, facilmente controllabile e che può essere gestito attraverso un unico pannello di controllo.

Recentemente, inoltre, la società ha anche rilasciato delle nuove funzionalità, sia su ThinOX4PC che nella console di gestione ThinMan

Server, funzionalità indirizzate a favorire e semplificare la gestione "end-to-end" degli utenti remoti.

Comunicazione sicura con il protocollo Web Socket

Uno degli aspetti critici nello smart working è quello posto dalla amministrazione dei dispositivi e dalla sicurezza dei dati trasferiti da e verso remoto.

In pratica, servono gli strumenti necessari per la configurazione, la gestione e il monitoraggio dei Thin Client remoti, incluso in questo insieme anche un protocollo di comunicazione sicuro per la connessione del server centrale, come il di ThinMan Server, agli endpoint remoti.

Il problema di un protocollo sicuro è critico, osserva Praim. Questo perché gli utenti remoti devono disporre della connettività di rete necessaria per raggiungere le risorse aziendali ed essere coperti in modo efficace, anche se non in sede, per quanto concerne gestione, monitoraggio e sicurezza.

Detto altrimenti, agli amministratori viene chiesto di garantire la sicurezza fornendo flessibilità agli utenti anche quando questi si spostano o

si connettono da casa ma, non potendo conoscere ogni singolo ambiente da cui gli utenti si collegheranno, devono fornire strumenti e linee guida semplici per garantirne l'operatività. Per renderlo possibile Prais ha sviluppato uno specifico protocollo di comunicazione che ha l'obiettivo di semplificare notevolmente la comunicazione fra le soluzioni Thin Client Prais e ThinMan Server. Tramite il nuovo protocollo Web Socket Secure i prodotti Prais, tra cui ThinOX, Agile4PC, Agile4Pi e ThinOX4PC, possono comunicare con ThinMan Server salvaguardando la sicurezza delle comunicazioni.

Peraltro, evidenzia Prais, il nuovo protocollo fornisce funzionalità aggiuntive per la comunicazione tra gli endpoint Prais e ThinMan Server. Le funzionalità includono:

- Connessioni sempre attive verso ThinMan
- Maggiore visibilità dello stato dei client
- Flessibilità nella scelta del certificato di sicurezza
- Configurazione di rete meno onerosa

Per quanto concerne la sicurezza, in particolare, la crittografia su Web Socket è resa possibile utilizzando i certificati SSL. L'implementazione Prais di Web Socket sicuri nella comunicazione fra Thin Client e ThinMan consente nello specifico di adottare certificati SSL ottenibili con Let's Encrypt, oppure altri originati direttamente dalla propria infrastruttura PKI aziendale.

Numerose le possibilità di utilizzo evidenziate da Prais. Tra queste:

- Telelavoro: gli utenti remoti possono lavo-

rare ovunque, purché dispongano di una connessione Internet e possano connettersi a ThinMan utilizzando la porta 443.

- Service provider: un service provider è in grado di gestire più gruppi di sistemi client da un unico pannello di controllo in cloud.
- Gestione dei dispositivi in mobilità: i dispositivi come i laptop sono pensati per spostarsi tra reti e postazioni di lavoro diverse. Il nuovo protocollo di comunicazione lo abilita senza la complessità della configurazione di rete ed evitando problemi agli amministratori IT e agli utilizzatori finali.
- Accesso remoto semplificato: l'accesso remoto e la comunicazione con i servizi interni sulla rete aziendale sono tradizionalmente realizzati con una connessione VPN. Tramite il protocollo di comunicazione sicura con ThinOX4PC e Agile4PC, la comunicazione con la rete aziendale interna è semplificata dalla comunicazione sempre attiva e crittografata con il server ThinMan.

In sintesi, riassume Prais, con il nuovo protocollo di connettività sicuro Web Socket integrato nei software Prais e il nuovo configuratore WiFi per ThinOX4PC, si viene a disporre degli strumenti necessari per una connettività senza interruzioni e disponibile su qualsiasi dispositivo. Combinando le due soluzioni software Prais ThinMan e ThinOX4PC, qualsiasi dispositivo può essere trasformato in un Thin Client e qualsiasi luogo trasformarsi in una postazione di lavoro collegandosi al desktop virtuale aziendale.

Pbx virtuale e fibra abilitano servizi di UCC evoluti

Grazie a SELTA e a Open Fiber, l'operatore Naquadria ha realizzato un servizio di Pbx virtuale basato su iperconnessione e completamente sicuro

La realizzazione di ambienti tecnologicamente evoluti e di servizi smart passa sempre di più attraverso operatori locali animati da un forte spirito innovativo. Un esempio è Naquadria con il suo nuovo brand HDFibra (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 al data center di tipo tier 3 certificato ISO 27001, Naquadria è in grado di fornire servizi ad altissime prestazioni sia a utenti business che consumer. In particolare, propone 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.

Alessandro Solari -
Naquadria



Per fornire il servizio 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 a telefoni di terze parti già in dotazione.

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. Data la semplicità dell'installazione 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.

Con Snom SRAPS servizi a valore erogati anche da casa



Mark Wiegleb -
Snom Technology

Snom ha reso disponibile un servizio gratuito di configurazione automatica dei terminali via cloud che consente di soddisfare da casa le esigenze dei client

E' innegabile che il centralino telefonico e i telefoni IP impiegati in azienda costituiscano la colonna portante delle comunicazioni di qualsiasi organizzazione e di norma si tratta di soluzioni personalizzate.

Interruzioni del servizio o malfunzionamenti richiedono un intervento immediato. Modifiche all'impianto e ai terminali, l'aggiunta di ulteriori interni o la configurazione dell'accesso dei telefoni al sistema tramite VPN vanno implementate in tempi brevissimi.

In questo momento, tuttavia, soddisfare l'esigenza di adeguare anche l'infrastruttura per la telefonia aziendale all'attuale situazione risulta problematico perché le aziende non gradiscono ricevere personale tecnico esterno, a cui comunque viene richiesto di ridurre gli spostamenti il più possibile.

SRAPS, servizio all'utente senza rischi e con meno costi

Per far fronte a questa esigenza Snom, produttore internazionale di terminali IP per l'uso professionale, ha annunciato la disponibilità del suo servizio SRAPS (acronimo di Secure Redirection and Provisioning Service), uno strumento rivolto ai partner che permette loro di gestire il parco

installato e analizzare e risolvere da remoto e gratuitamente le problematiche in cui possono incorrere i terminali IP.

L'obiettivo del servizio, ha spiegato Snom, è quello di permettere alle aziende di rispondere alle esigenze della propria clientela in modo efficiente, nonostante la possibile carenza di personale o il verificarsi di situazioni che non consentono di recarsi presso il cliente stesso, ad esempio installare nuovi telefoni, modificarne la configurazione, aggiornare il firmware dei terminali. Tutti compiti che con SRAPS possono essere svolti dai tecnici dei partner anche da casa.

Si tratta però, ha commentato l'azienda, di uno strumento utile in generale, e non solo nella situazione contingente, perché consente di ridurre al minimo la necessità e i costi che derivano da eventuali appuntamenti in loco, e che di conseguenza permette di semplificare e velocizzare i tempi di messa in opera e di passaggio in esercizio di nuove installazioni.

«Con SRAPS i partner dispongono di un'arma in più per fidelizzare la propria clientela a lungo termine. Se da un lato riuscire a gestire in maniera perfetta le richieste più diverse della clientela in qualunque situazione contribuisce ad incrementarne significativamente il livello di soddisfazione e lealtà, dall'altro la clientela ha la certezza che il proprio fornitore dispone di strumenti ottimali per garantire che i terminali vengano costantemente mantenuti e adattati tempestivamente a nuove esigenze» ha commentato Mark Wiegleb, Responsabile del dipartimento Interop&Integration di Snom Technology GmbH.

FAAC sceglie il digital workplace per produttività e competitività



Enrico Minelli -
Group CIO FAAC

FAAC, in partnership con VEM sistemi, ha avviato un percorso di cambiamento nei processi di collaborazione tra i dipendenti basato sulle soluzioni Cisco Webex

FAAC è una multinazionale bolognese specializzata nell'automazione in ambito residenziale, industriale e pubblico. La notevole crescita del Gruppo FAAC, che conta 34 filiali in 5 continenti, oltre 80 distributori ufficiali e 17 siti produttivi, 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.

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 Minelli, 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 ge-

stito 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 dimensioni, cosa che ha fatto sì che molti manager di FAAC abbiano adottato dei dispositivi 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 del nuovo posto di lavoro digitale ha imposto un profondo cambiamento nelle abitudini dei dipendenti, cambiamento che la multinazionale ha promosso ingaggiando il top management, creando un "change management team" e un gruppo di "evangelist" a disposizione per il training e il supporto dei colleghi.

Per favorire l'adozione delle nuove tecnologie e diffondere la "netiquette" dei digital meeting, VEM ha realizzato per FAAC una serie di divertenti video pillole cartoon, che hanno come protagonisti gli stessi dipendenti dell'azienda a cui è affidato il compito di spiegare alcune fondamentali regole da seguire prima, durante e dopo la riunione, per sfruttare appieno le potenzialità delle nuove tecnologie e massimizzare l'efficacia dell'incontro digitale.

Da Vertiv e Uptime Institute data center modulari TIER-Ready

La partnership semplifica il processo di acquisizione della Certificazione TIER di Uptime Institute per le strutture basate sui data center modulari di Vertiv



Vertiv, fornitore di soluzioni infrastrutturali, ha annunciato che i propri data center modulari prefabbricati (PFM) hanno ricevuto da Uptime Institute la certificazione TIER-Ready per la resilienza delle prestazioni.

Il riconoscimento consentirà a Vertiv di fornire i servizi di Uptime Institute di livello Tier Certification of Constructed Facilities (TCCF) con le unità modulari Vertiv TIER-Ready, cosa che permette ai clienti della società di disporre di Certificazione Tier.

L'implementazione dei modelli PFM di Vertiv progettati come TIER-Ready garantisce ai fini pratici al cliente di poter conseguire in maniera semplice e veloce la certificazione TCCF.

Queste infrastrutture modulari e prefabbricate sono già peraltro disponibili in Europa, Medio Oriente e Africa (EMEA) e vi è l'obiettivo di renderle disponibili a livello globale nel corso del 2020. La partnership TIER-Ready è un accordo strategico in base al quale gli specifici modelli PFM di Vertiv vengono esaminati da Uptime Institute durante il processo di sviluppo ingegneristico, per garantire che tali soluzioni soddisfino i requisiti severi del TIER Standard of Topology riconosciuti a livello globale.

I prodotti PFM di Vertiv che sono qualificati TIER-Ready supportano in modo concreto i requisiti di disponibilità e uptime dei clienti più esigenti che hanno scelto a livello strategico di implementare l'infrastruttura digitale certificata TIER.

Come previsto dalla partnership, Vertiv ha completato la revisione del progetto TIER-Ready III di Uptime Institute per la propria infrastruttura PFM SmartMod per un massimo di 10 rack e 80 kW di carico IT.

Le strutture implementate utilizzando soluzioni SmartMod designate TIER-Ready, saranno in grado di ottenere rapidamente e senza difficoltà il TCCF di Uptime Institute.

Cosa è l'approccio PFM

Un approccio PFM è una modalità che consente l'implementazione dei nuovi data center con un numero di installazioni in loco significativamente inferiori rispetto ai data center costruiti in modo tradizionale.

Specialmente nelle economie in via di sviluppo, le implementazioni PFM stanno diventando sempre più frequenti perché permettono di ottenere rapidamente ulteriore capacità – anche nell'Edge – senza gli impedimenti di un processo di costru-

zione tradizionale e con una più efficace implementazione di sistemi, test e messa in servizio. Secondo gli analisti di 451 Research, il mercato dei data center PFM è destinato ad espandersi a un tasso annuo di crescita composto (CAGR) del 14,4 per cento nell'arco di cinque anni fino al 2021, quando raggiungerà i 4,4 miliardi di dollari.

Uno standard de facto

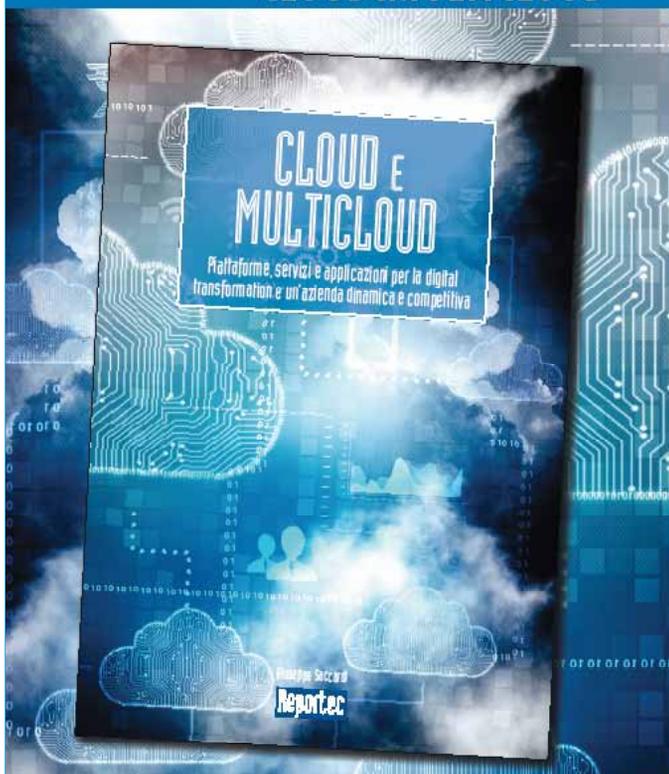
Va osservato che TIER Standard of Topology di Uptime Institute, osserva Vertiv, è lo standard de facto del settore per l'affidabilità e la resilienza dei data center e assicura ai clienti che i data center

certificati TIER operino in modo preciso e prevedibile in un'ampia gamma di condizioni operative, tra cui l'interruzione dell'alimentazione di rete.

L'Uptime Institute ha introdotto il proprio programma di design review TIER-Ready, che consente ai vendor PFM di fornire soluzioni in grado di raggiungere gli stessi livelli di affidabilità e resilienza già raggiunti dai migliaia di data center certificati TIER in tutto il mondo.

Il programma TIER-Ready snellisce poi il processo di certificazione TCCF riducendo i tempi di revisione ingegneristica richiesti di norma da ciascuna specifica installazione dei data center.

È disponibile il nuovo libro
CLOUD e MULTICLOUD



ORDINA SUBITO
LA TUA COPIA DEL
LIBRO
CLOUD e MULTICLOUD!

35 euro
(Iva e spedizione inclusa!)

chiamaci per ordinare
02.36580441
oppure scrivi a
info@reportec.it