Cloud & Business

n.93
Luglio/Agosto 2020

LA RIVISTA PER IL MANAGER CHE DEVE OTTIMIZZARE COSTI E PROCESSI

IN QUESTO NUMERO>>

DIGITALE, RESILIENZA ED EXPERIENCE: LA RIPARTENZA DELLE PMI

Affrontare il futuro per una PMI richiede che siano stabilite delle priorità e decisioni su dove e come investire. Un suggerimento su come agire è offerto da SAP

Ripartire dopo un evento grave come quello che sta coinvolgendo l'intero globo è sempre difficile. Un aiuto può venire dai suggerimenti di manager di aziende che quotidianamente hanno a che fare con i problemi connessi alla gestione di un'azienda. In proposito, abbiamo chiesto ad ***Adriano Ceccherini****,* ***Direttore Mercato PMI di SAP Italia e Grecia****, come sarebbe meglio affrontare i mesi che ci aspettano, soprattutto per una PMI.*

Adriano Ceccherini

«Nel mio ruolo - spiega Adriano Ceccherini - spesso mi sono trovato a dover analizzare le

Reportec Cloud&Business - N.93 Luglio-Agosto 2020 - società-editore: Reportec Srl (**www.reportec.it**) - Direttore responsabile: Giuseppe Saccardi. In redazione: Gaetano Di Blasio - Paola Saccardi - Immagini: Dreamstime.com

differenze di orientamento e approccio al digitale tra le imprese di grandi dimensioni e le PMI. Ovviamente risorse, competenze a disposizione di questi due cluster viaggiano su ordini di grandezza diversi, ma è anche vero che le PMI possono vantare dei vantaggi rispetto ai loro concorrenti più grandi. Possono sviluppare legami più stretti con clienti e dipendenti, possono adattarsi velocemente ai cambiamenti di sentiment del mercato, sviluppare prodotti innovativi in tempi rapidi, e modificare tempestivamente il modello di business in un'ottica di maggiore competitività. E il rapporto delle PMI con la tecnologia sta evolvendo per mantenere questi vantaggi inalterati.

Il digitale al servizio della resilienza

Durante e dopo la crisi COVID-19 le aziende hanno compreso l'importanza della tecnologia come una alternativa perseguibile per affrontare situazioni di emergenza, garantire la continuità del business, e in molto casi come un'opportunità per esplorare nuovi percorsi. Ad esempio, durante il lockdown la tecnologia ha permesso di mantenere i contatti, accorciare le distanze, promuovere e garantire educazione e formazione, realizzare progetti complessi da remoto, permettere alle aziende di rivedere i modelli di business sviluppando nuovi prodotti e servizi per sopravvivere.

L'attuale scenario economico potrebbe rappresentare un rallentamento alla crescita di molte PMI. Ad un certo punto, tuttavia, è necessario tracciare una strada da percorrere verso il recupero. Ma questa volta, tornare alla "normalità del business" non è un'opzione. Le nuove tendenze che richiedono resilienza, agilità e conoscenza istantanea stanno accelerando, facendo evolvere pratiche e processi consolidati, progettati principalmente per essere scalabili, automatizzati e garantire efficienza.

La prossima ondata di innovazione non si focalizzerà su rendere più veloci i processi esistenti. Al contrario, l'attenzione si concentrerà sulla capacità di un'azienda di agire senza indugio, rispondere a interruzioni e cambiamenti imprevisti quali modifiche nelle normative, indisponibilità delle risorse, carenza di approvvigionamento e picchi di domanda per prodotti che non erano considerati mission-critical una settimana fa.

Dal nostro osservatorio, con il COVID-19 stiamo assistendo ad esempio a un grande fermento, soprattutto verso sistemi ERP di nuova generazione, per massimizzare l'agilità di business, standardizzare i processi, accedere a dati certi in tempo reale e ridurre il time-to-value. La domanda delle PMI italiane si sta orientando sul poter disporre di un digital core affidabile, meglio in cloud, che agisca come cuore pulsante

dell'azienda e a cui processi come supply chain, produzione, e-commerce si possano integrare in modo semplice e naturale. Stiamo assistendo a una crescita di interesse per le nostre soluzioni di ERP in Cloud, che non vanno considerate solo come soluzioni ERP, ma soprattutto come la fonte per accedere a dati rilevanti di cui i manager hanno bisogno in tempo reale per crescere, pianificare e possibilmente anticipare le evoluzioni del mercato.

Focus sull'experience

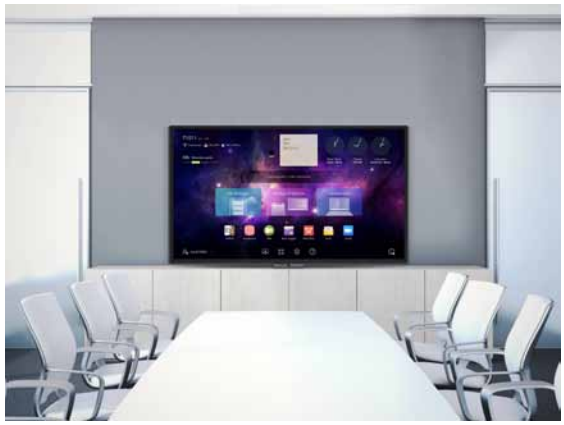
Le recenti disfunzioni operative e la volatilità dei mercati hanno ribadito l'importanza di servire efficacemente clienti, coinvolgere i dipendenti e stabilire rapporti di fiducia con i partner. Queste connessioni sono alla base della resilienza e dell'agilità delle aziende di più piccole dimensioni. Secondo una recente analisi che abbiamo svolto lo scorso aprile con Oxford Economics, intervistando 2.000 aziende PMI in 19 paesi emerge che le organizzazioni stanno adottando questo imperativo, citando la customer experience come una priorità fondamentale nei prossimi tre anni. Questo è vero sia a livello globale che italiano, dove circa il 40% dei rispondenti ha dichiarato che la customer experience rappresenta la prima area di intervento in questa fase di "ritorno alla normalità".

Per le PMI italiane la seconda area di intervento rientra nello stesso filone, e si concentra sul migliorare la capacità di attrarre nuovi clienti, mentre la terza area consiste nel minimizzare i rischi di business e di compliance. Infine un'altra area di forte interesse per le PMI italiane è quella di migliorare l'esperienza dei propri dipendenti (22%) e attrarre e fidelizzare nuovi talenti (21%). Migliori esperienze di clienti e dipendenti non derivano solo da una gestione oculata del business. Ogni funzione aziendale deve standardizzare i propri processi, migliorare la comunicazione e cercare nuovi modi per essere più efficiente, crescere e innovare. Questi interventi sono delle sfide per un'organizzazione perché il coordinamento tra le diverse funzioni è molto complesso. Basti pensare che spesso sono diverse le divisioni che si occupano di customer e employee satisfaction, ad esempio marketing, servizio clienti, direzione del personale e operation.

E' evidente a tutti, insomma, che nell'economia post-pandemica il successo del business per le PMI passa da agilità, focalizzazione sulle persone e utilizzo del potere dei dati. E come SAP siamo impegnati ad aiutare le aziende ad andare verso questa direzione e a funzionare sempre più come un'impresa intelligente per poter offrire ai loro clienti esperienze rilevanti e uniche, dove la tecnologia è invisibile e privacy, sicurezza e fiducia sono elementi certi».

di Giuseppe Saccardi

Con le lavagne interattive si collabora da remoto e nel cloud



Il sistema di videoconferenza integrato e con schermo antibatterico di BenQ abilita la collaborazione sicura e dinamica anche da remoto e nel cloud

La diffusione del lavoro a distanza, la ridefinizione degli spazi aziendali e la necessità di collaborazione tra gruppi di lavoro sono elementi chiave della trasformazione digitale in atto e aspetti imprescindibili per affrontare i momenti critici come quello che si sta vivendo.

Per fortuna, le soluzioni non mancano. Un esempio concreto dell'impegno dei produttori è offerto da BenQ Corporation, una multinazionale specializzata nella ricerca, nello sviluppo e nella produzione di tecnologie digitali.

La società è quotata tra i leader nello sviluppo di tecnologie di proiezione DLP (Digital Light Processing) ed ha a portfolio un'ampia gamma di display il cui obiettivo è di favorire la rivoluzione digitale in corso.

Alle soluzioni consolidate ha aggiunto di recente la nuova serie CP DuoBoard, costituita da display digitali componibili che, evidenzia **Giacomo Rocchi**, Sales and Marketing Director della filiale italiana, ha trasformato in soluzioni concrete quanto necessario per l'attuale trasformazione digitale delle aziende, predisponendo nello stesso tempo un contesto altamente sicuro per gli utilizzatori.

La salute innanzitutto

Per garantire la salute e ridurre al minimo i rischi connessi alla pandemia in corso, sia che vengano adottati per favorire il lavoro e la collaborazione dei team in ufficio o che questo avvenga da remoto, per ridurre l'impronta batterica e i conseguenti rischi di contagi i display della serie DuoBoard si avvalgono del sistema Healthcare+, una tecnologia ideata specificatamente per proteggere la salute del personale sul luogo di lavoro.

Healthcare+, oltre a includere la Smart Eye-Care Solution per la tutela del benessere oculare e un sensore di qualità dell'aria che monitora la quantità di CO2 nella stanza, è una tecnologia che comprende anche un rivestimento dello schermo resistente ai germi, costituito da uno strato nanoionico d'argento che elimina la maggior parte dei germi a contatto e ne previene la diffusione nell'ambiente circostante.

All-in-one per la video collaborazione professionale

Nella sua essenza, BenQ DuoBoard è una soluzione di video collaborazione con cui BenQ si è proposta di mettere a disposizione delle aziende e dei gruppi di lavoro locali o remoti una piattaforma che permetta di sfruttare tutte le possibilità offerte da una moderna sala riunioni, essere di ausilio alla creatività e favorire l'interazione e lo scambio di idee tra dipendenti e collaboratori. In particolare, integra in un solo prodotto tut-

te le diverse tecnologie comunemente utilizzate nelle sale meeting, quali monitor ad alta definizione, lavagna interattiva e un sistema per realizzare videoconferenze di qualità professionale. «Tramite un unico dispositivo multifunzione, diventa possibile realizzare riunioni altamente coinvolgenti e interattive, promuovere la creatività e migliorare la produttività, la partecipazione e l'interazione sinergica tra più persone sia in ufficio che da remoto», ha commentato Giacomo Rocchi.

Una suite per collaborare ovunque e nel cloud

Il motore di BenQ DuoBoard è costituito da Collaboration+, una suite di funzionalità progettate per ottimizzare l'efficienza, la produttività e il lavoro in team, sia locale che remoto. In particolare, ha evidenziato BenQ, la suite funzionale comprende:

- *Duo Boards*: permette di affiancare due display DuoBoard in modo da disporre di un unico e più ampio spazio di lavoro laddove serva estendere e migliorare la collaborazione tra più persone.
- *Duo Windows*: permette, tramite il display DuoBoard, di eseguire e visualizzare fianco a fianco due diverse applicazioni e/o sorgenti, in modo da favorire attività di tipo multitasking e la condivisione delle informazioni.
- *Duo OS:* consente di utilizzare contemporaneamente due sistemi operativi diversi (Android, iOS, macOS e Windows) su un unico display DuoBoard.
- *Duo Users:* è una funzione multi-touch che permette a più utenti di collaborare sulla medesima applicazione nello stesso momento.
- *EZWrite:* è una lavagna fruibile in cloud e da remoto che consente agli utenti di partecipare alle riunioni e di condividere le idee sulla lavagna tramite i propri dispositivi mobili.

Oltre che dalla suite Collaboration+, la qualità delle video conferenze tramite BenQ DuoBoard è assicurata dalla presenza di una videocamera integrata e da un set di microfoni di qualità professionale che riducono i rumori ed eliminano l'eco. Il BenQ Launcher consente poi agli utenti di iniziare le riunioni con un solo tocco.

Giacomo Rocchi - BenQ Italia

Flessibilità e sicurezza

Cloud e collaborazione remota sono due forti abilitatori della trasformazione digitale ma possono aprire la strada a rischi. Per evitarli, "la piattaforma è dotata in particolare della funzione DMS (Device Management Solution), che abilita il controllo centralizzato dei dispositivi BenQ e permette ai responsabili IT di gestire i diversi display installati anche da remoto, attivare o cancellare applicazioni", spiega Giacomo Rocchi.

L'AMS (Account Management System) è invece una funzionalità che permette al responsabile del servizio di gestire gli account multi-utente e le impostazioni personalizzate dei dispositivi. Una volta configurato, un utente può accedere al proprio profilo avvicinando al sensore di prossimità NFC (Near Field Communication) la propria card. Ad accesso avvenuto, sul display appare il desktop personalizzato con le applicazioni e i file e diventa possibile accedere allo spazio cloud personale senza bisogno di digitare ogni volta user name e password.

Per permetterne l'uso in contesti diversi, BenQ DuoBoard comprende i modelli CP6501K e CP8601K, rispettivamente con schermi di 65 e 86 pollici. Le dimensioni sono state definite con l'obiettivo di permettere ai dispositivi di adattarsi facilmente agli spazi disponibili, con la versione da 65 pollici che può essere utilizzata anche in verticale.

di Giuseppe Saccardi

Con la digital transformation dall'emergenza alla nuova normalità

Centro Computer sottolinea che i nuovi progetti sono sempre più mirati al supporto della trasformazione aziendale in atto e al crescente bisogno di smart working, mobility e cloud

Roberto Vicenzi - Centro Computer

L'emergenza da Covid-19 ha fatto registrare richieste straordinarie nell'ambito di due aree: smart working e servizi cloud, mentre a causa del lockdown sono risultati rallentati gli investimenti in data center, networking e stampanti multifunzione.

Questi sono i dati che si estrapolano esaminando i risultati finanziari del primo semestre di Centro Computer, società di consulenza attiva dal 1984 con sedi a Cento (FE), Faenza (RA), Milano, Modena, Padova e specializzata in prodotti, servizi e soluzioni ICT in aree strategiche per le imprese, come cloud, sicurezza, data center, fleet management e altro ancora. In particolare, l'indicatore delle nuove tendenze del mercato porta ad aver raggiunto a giugno una crescita di fatturato pari al +5,3% rispetto allo stesso periodo del 2019, un incremento dovuto essenzialmente all'aumento delle vendite di notebook e accessori, come ad esempio le soluzioni e i dispositivi per le videoconferenze, il software in cloud e servizi vari. Inoltre, la tendenza del lavoro in mobilità viene confermata anche dalla vendita incredibile di smartphone, un valore che si è attestato a +237%, rispetto al semestre precedente.

Centro Computer si è sempre distinta sul territorio per la capacità di offrire progetti ad alto tasso di innovazione, costruiti sulle esigenze dei clienti e oggi, più che mai, ritiene che le imprese debbano pensare a lungo termine, organizzandosi per essere più flessibili e sviluppando una vera cultura in ambito cloud e unified communications, ragionando sull'integrazione di tutte le forme di comunicazione aziendale in un unico sistema, che consenta di lavorare in modo semplice ed evoluto.

«L'emergenza sanitaria ha fatto comprendere in modo ancora più marcato alle imprese l'importanza della digital transformation. Il passo successivo per contrastare il periodo di recessione che vediamo all'orizzonte è quello di proseguire a investire in innovazione, uno dei pochi fattori in grado di ridurre al minimo la durata delle fasi di recupero caratteristiche di tutti i periodi di crisi. Solo così sarà possibile sia minimizzare l'effetto pandemia sulle aziende sia accelerare la trasformazione in imprese del futuro pronte ad affrontare la nuova normalità», ha osservato **Roberto Vicenzi**, Vicepresi-

dente di Centro Computer.
Centro Computer crede poi fortemente nella linea di business dedicata al Fleet - Mobility - Print Management, che integra i vantaggi dell'acquisto e della locazione operativa. Sono soluzioni che assicurano la garanzia di continuità dei servizi, conclude il manager, e sgravano l'azienda da tutte le problematiche di taglio logistico inerenti. La strategia finanziaria delle imprese, sarà quella di investire sempre di più sul "costo operativo" (con un canone annuale) rispetto al "costo capitale".

Collaborare da remoto in modo sicuro e garantito

Lo smart working è uno dei temi salienti della digital revolution, ma servono gli strumenti adatti e la garanzia di realizzarlo in modo sicuro

di Giuseppe Saccardi

Luigi Meregalli - CIE Telematica

Nello scenario che si prospetta per i prossimi mesi, a essere conservativi, saliente appare il tema del come lavorare in team quando i partecipanti sono distribuiti su più sedi o in mobilità o presso la propria abitazione, e quali strumenti lo rendono possibile.
Ma risolvere il problema dei dispositivi, dopo gli entusiasmi iniziali, può non essere sufficiente. Quella degli strumenti adatti , contribuisce al tema **Lugi Meregalli**, General Manager della società di ingegneria CIE Telematica (cietelematica.it), è di certo una condizione sine qua non, ma puntare solo su quello non basta. Assieme a un buon dispositivo serve anche quanto permette ai sistemi di collaborazione distribuiti di essere sempre operativi, ed esserlo in modo garantito, ed esenti da attacchi da parte di cybercriminali.

Se enunciare un principio è facile, i problemi con cui si scontrano i responsabili IT nel passare alla pratica nella identificazione e nella gestione di una soluzione di collaborazione tra team distribuiti, e con infrastrutture di comunicazione non sempre omogenee come capacità trasmissiva, sono tuttavia consistenti.
In primis c'è il fatto che sovente si dispone di personale di supporto limitato o non ancora formato sugli strumenti utilizzati, e poi la gamma di aspetti che devono essere considerati a corollario quali il come garantir la sicurezza remota, l'aggiornamento dei software, la manutenzione, la gestione, la garanzia del funzionamento e così via.
Apparati che smettono di funzionare nel mezzo di una conferenza, o una qualità della connessione insufficiente, oppure il mancato ag-

giornamento della sicurezza, sono aspetti che possono rapidamente far perdere i benefici di una evoluzione che ha permesso di affrontare l'attuale momento di criticità e lasciato intravvedere un nuovo modo di lavorare e cooperare, e più rispettoso dell'ambiente..

In sostanza, si rischia di far seguire a una fase di entusiasmo una fase di disillusione. Inevitabile o quasi, data la natura umana e delle aziende, che a quel punto scatti la ricerca del colpevole, che inevitabilmente tende sempre ad essere considerato il responsabile IT, al quale sino a poco prima si negavano le risorse necessarie.

Per superare questi problemi e il fatto che si è spesso restii ad affidarsi ai suggerimenti di un produttore per il timore di incorrere in un lock-in tecnologico, CIE Telematica ha sviluppato una proposta risultante da una analisi terza del mercato che si è concretizzata in un portfolio di prodotti e servizi che ritiene adeguati a rispondere alle sfide che si prospettano.

Cooperare in modo flessibile e nel cloud

Cominciando dallo smart working e dalla collaborazione, da una accordo con Lenovo che a sua volta ha in corso una partnership con Microsoft, ha identificato uno strumento adatto per l'ambito aziendale in Microsoft Teams, una piattaforma che permette di cooperare tramite chat, video meeting, file storage, abilita l'integrazione di applicazioni e che è disponibile in 26 lingue.

Aspetto saliente, osserva Meregalli, è che oltre a connettere in modo efficace gli utilizzatori in diverse modalità è una soluzione integrata anche con Microsoft Office 365 ed è integrato con app e servizi usati quotidianamente quali Word, Excel, PowerPoint, OneNote, SharePoint, Stream e PowerBI. In pratica si ha accesso a file e strumenti che abilitano ovunque l'usuale flusso di lavoro.

Semplificato, ha aggiunto Meregalli, e motivo della sua scelta, è anche l'editing simultaneo e in tempo reale con altri utenti di documenti, cosa che permette di evitare invii e reinvii di successive versioni via mail per la loro messa a punto.

L'importanza dei servizi di sicurezza

Il secondo aspetto a cui porre attenzione è, come osservato, quello della garanzia di funzionamento e di sicurezza della soluzione adottata. Le criticità derivano da diversi aspetti quali il dispositivo usato dagli utenti finali (aziendale o personale), i rischi connessi ai sistemi operativi dei dispositivi mobili, il malware e il phishing che hanno come obiettivo i social media e il rischio intrinseco all'utilizzo di software di terze parti.

La soluzione che CIE Telematica ha identificato e suggerisce nell'ambito delle proprie attività di società di ingegneria e in qualità di silver partner di Lenovo, è. il ricorso a ThinkShield, uno strumento sviluppato da quest'ultima e che è utilizzabile per proteggere dati, i dispositivi, la identità e le attività on-line.

I servizi di protezione estesa assicurati da ThinkShield derivano dalla considerazione che un'azienda non può permettersi di subire violazioni della protezione. ThinkShield rappresenta sotto questo punto di vista una piattaforma di protezione personalizzata e personalizzabile che ha l'obiettivo di protegge un'azienda nel suo complesso, dai dispositivi ai dati alle connessioni di rete, e dai criminali informatici sempre più agguerriti, anticipandone le mosse e bloccandone in modo preventivo e dinamico gli attacchi.

«Abbiamo verificato sul campo che Thinkshield è uno strumento estremamente efficace per la data security e la protezione dei dati, sia per

quanto concerne l'utilizzo che viene fatto di un pc che nelle modalità di accesso ad Internet, con in aggiunta la possibilità di riconoscere reti wifi affidabili a cui connettersi., e dotata di funzioni di autenticazione a più fattori ed encryption», ha evidenziato Meregalli.
Ideato per il supporto e la gestione del personale che lavora da remoto è anche il servizio Premier Support, sottoscrivibile anche per un solo anno, che prevede l'accesso all'help-desk per i prodotti della famiglia Think di Lenovo. Unico requisito è che il dispositivo deve essere coperto dalla garanzia Onsite. Tra quello che prevede vi e anche il supporto hardware e software , un singolo punto di contatto e la reportistica standard sui livelli di servizio.

Ottimizzare l'IT ibrido con i SystemInspection Service di Fujitsu e Finix

I servizi di discovery di Finix aiutano a definire lo scenario per la trasformazione data-driven analizzando la topologia dell' IT dall'edge al core fino al cloud

di Giuseppe Saccardi

Marcus Schneider - Fujitsu

Fujitsu ha presentato due nuovi servizi di valutazione che hanno l'obiettivo di permettere alle aziende di definire il proprio scenario di riferimento per una trasformazione data-driven.
A fronte di un costo fisso, le soluzioni di SystemInspection Service fanno leva su strumenti e capacità di analytics unificate per mappare l'architettura degli asset di dati fisici e logici presenti nell'intero ambiente IT ibrido.
Operativamente, scattano un'istantanea degli elementi di sistema esistenti a livello enterprise valutandone il grado di preparazione alla trasformazione digitale. Generano poi un inventario degli ambienti operativi SAP creando una visione olistica delle performance e dell'utilizzo delle risorse.
Fujitsu SystemInspection Service for Storage fornisce invece una visione centralizzata degli ambienti storage eterogenei - fisici e virtuali, residenti sia on-premises che nel cloud.
I nuovi SystemInspection Service complemen-

tano la gamma già esistente di servizi DataInspection e SystemInspection già a portfolio, che ampliano con strumenti per identificare metodi diretti utili a raggiungere performance migliori riducendo i costi, eliminando i colli di bottiglia prestazionali e migliorando l'utilizzo dei sistemi.
Le proposte Fujitsu SystemInspection Service sono peraltro parte di un più ampio portafoglio dedicato all'IT ibrido volto a fornire una chiara strategia per l'orchestrazione di mix di infrastrutture on-premises e cloud, sia privati che pubblici, con workload distribuiti in ambienti edge, core e cloud.
In Italia, le soluzioni Fujitsu SystemInspection Service e più in generale quelle dedicate all'IT ibrido sono distribuite da FINIX Technology Solutions.

«Gli ambienti IT ibridi innalzano i costi e la complessità costringendo i clienti a gestire tool specifici separati prodotti da vendor differenti. Con i due nuovi servizi Fujitsu dedicati agli ambienti IT ibridi siamo in grado di fornire un quadro complessivo, anche nel caso di installazioni complesse che abbracciano l'edge di rete, il core e il cloud. La particolare capacità di Fujitsu nell'analizzare in maniera indipendente dall'hardware interi ambienti SAP e fornire soluzioni correttive end-to-end per i data center mette a disposizione dei clienti roadmap tecnologiche che possono essere implementate nell'architettura di ciascun ambiente SAP», ha commentato **Marcus Schneider**, Head of Product Management Data Center Product Sales Europe di Fujitsu.

PARTNERSHIP

di Giuseppe Saccardi

IBM, Adobe e Red Hat assieme per migliorare la customer experience nel cloud

Le tre aziende hanno siglato una partnership per innovare la customer experience dando la priorità ai settori regolamentati che utilizzano il cloud ibrido

IBM, Adobe e Red Hat hanno annunciato una partnership strategica volta ad accelerare la trasformazione digitale e a rafforzare la sicurezza real-time dei dati delle imprese, con particolare attenzione a quelle che operano in settori maggiormente regolamentati.
Obiettivo della partnership è quello di agevolare le aziende nella capacità di offrire esperienze sempre più personalizzate e coinvolgenti, in grado di fidelizzare i propri clienti e, al contempo, di generare profitto.
La partnership si focalizzerà inizialmente su:

- *Flessibilità di adozione con Hybrid Cloud:* Adobe, IBM e Red Hat intendono agevolare la gestione e distribuzione di contenuti e risorse da parte delle imprese all'interno di qualsiasi ambiente cloud ibrido, dai multicloud pubblici ai data center on-premise.
- *Abilitazione di Adobe per i servizi finanziari:* Adobe entra nell'ecosistema di partner IBM

in qualità di partner strategico per l'offerta di soluzioni CX per IBM Cloud for Financial Services. In pratica, e tramite IBM Cloud for Financial Services, IBM potrà mettere a disposizione dei professionisti del settore Adobe Experience Manager, con l'obiettivo di rispondere alle loro necessità in termini di sicurezza, compliance normativa e offerta personalizzata ai clienti.

- *Servizi Adobe e IBM:* IBM iX, divisione di IBM Services dedicata al business design, estenderà l'offerta a tutte le principali applicazioni aziendali di Adobe. L'obiettivo è di consentire ai brand globali di accedere ai dati per progettare, implementare e personalizzare i progetti dei propri clienti.

«La realtà è che oggi le aziende di tutti i settori industriali operano in un mondo che pone l'esperienza di clienti e utenti al centro in cui è fondamentale il valore ottenibile dai dati grazie a tecnologie avanzate e flessibili che rispettano principi etici e regolamenti di settore - ha affermato **Bridget van Kralingen**, Senior Vice President di IBM Global Markets -. Questi principi sono al centro della nostra partnership - che racchiude l'esperienza marketing di Adobe, quella di IBM nel mondo industriale e di Red Hat nell'open innovation - volta ad offrire ai clienti la possibilità di utilizzare i dati in modo sicuro e di conseguire un vantaggio competitivo».

Nell'ambito della partnership IBM ha anche designato Adobe quale "Global Partner for Experience" e adotterà Adobe Experience Cloud e le relative applicazioni di classe enterprise per innovare il proprio marketing a livello globale.del settore tech.

IBM partner per la trasformazione digitale di doValue

Se dagli accordi tra fornitori di soluzioni IT ci si sposta sul piano delle partnership con clienti, IBM è stata scelta come partner da doValue per la trasformazione digitale del Gruppo.

Nello specifico, doValue, operatore nel Sud Europa per i servizi di credit management e real estate per banche e investitori, specializzata nella gestione e recupero di crediti deteriorati, ha scelto IBM come partner per l'innovazione tecnologica e la gestione dell'ICT e dei processi di back office delle attività italiane.

Attraverso la società controllata Dock Joined in tech (Dock), IBM svilupperà una *cognitive data platform*, tramite la quale doValue potrà supportare i propri clienti appartenenti alla filiera del credito fornendo loro servizi a valore aggiunto basati sui dati, dando così seguito alle iniziative recentemente annunciate in questo ambito.

In particolare, l'accordo prevede la cessione a Dock del ramo di azienda doSolutions, l'IT & Operations company del gruppo doValue, dedicato ai servizi informatici ed al Back Office. La rimanente parte del personale di doSolutions verrà successivamente integrata in doValue.

A partire dal 1° luglio 2020, Dock, tramite un accordo decennale avrà la gestione dell'infrastruttura IT, della sicurezza informatica delle applicazioni, dei processi di back office per il gruppo doValue.

A tale accordo saranno dedicate le risorse del ramo ceduto e alcune risorse di DOV per un totale di 138 persone, oltre alle risorse messe in campo da IBM e Dock.

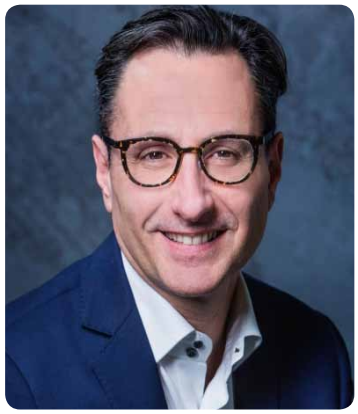
Il processo di internazionalizzazione e la crescente integrazione interna delle operation fra i diversi Paesi in cui il Gruppo doValue opera, impongono una razionalizzazione anche delle strategie e dei modelli operativi IT che, grazie all'impiego di tecnologie quali AI e multi-cloud, e all'automazione dei processi, permetterebbe di incrementare le performance operative e conseguire, al contempo, efficienze di costo ed economie di scala.

La partnership con IBM per il mercato italiano rappresenta un primo passo di questo percorso di integrazione tecnologica e consentirà a doValue, attraverso successive evoluzioni all'estero, di creare una piattaforma operativa di Gruppo comune.

di Giuseppe Saccardi

Pianificare la sicurezza per proteggere chi lavora da remoto

Lo smart working richiede un approccio proattivo e proiettato nel tempo per la sicurezza e la gestione dei dispositivi remoti. I suggerimenti di Qualys



Emilio Turani - Qualys

Per i team IT l'attenzione del 2020 avrebbe dovuto concentrarsi sulla trasformazione digitale. In un attimo le priorità sono mutate imponendo di fornire assistenza al lavoro a distanza. Per farlo i dipendenti devono accedere a Internet utilizzando dispositivi propri o pc aziendali che vanno costantemente protetti.

I dispositivi remoti non beneficiano però delle tecnologie di sicurezza implementate a livello centrale e diventa importante capirne lo stato al fine di rafforzarne la postura di sicurezza. Il problema più grande è l'identificazione e il controllo dei dispositivi che si connettono alla rete, le loro vulnerabilità e, cosa importante, il processo di patching di centinaia o migliaia di endpoint attraverso le Reti Virtuali Private e la loro limitata larghezza di banda.

Aziende come Microsoft e Adobe rilasciano le loro patch ogni mese ma nella situazione attuale la loro installazione non è semplice. Avere visibilità dei dispositivi è però prioritario e tramite servizi cloud i team IT dovrebbero poter visualizzare lo stato di ogni macchina usata dai dipendenti.

L'IT dovrebbe altresì poter definire le proprie regole sul patching e sulle priorità, in modo da classificare i nuovi problemi in base alla gravità, al rischio e al potenziale valore per i malintenzionati. Seguendo questo modello, ogni attività di patching potrà essere effettuata a distanza senza doversi affidare agli utenti. La sfida più grande per la sicurezza non è solo la configurazione del presente del lavoro a distanza, ma il prevedere ciò che accadrà nel futuro. Supportare lo smart working significa ottenere lo stesso grado di conoscenza delle risorse e di tutti i dispositivi di un'azienda nel corso del tempo, come avviene sulla rete aziendale.

È essenziale a tal fine comprendere le potenziali vulnerabilità, capire come possano essere corrette e come gestire la risposta per l'azienda nel suo complesso. E' un nuovo approccio, ma permette di mantenere sicuro il lavoro a distanza, rendendo l'ambiente di lavoro il più vicino possibile a quello aziendale.

Per rispondere a queste esigenze, Qualys, pioniere e fornitore leader di soluzioni di sicurezza e compliance basate sul cloud, ha adottato un approccio basato sull'offerta di VMDR, Vulnerability Management, Detection and Response, che permette di massimizzare le tattiche di sicurezza informatica di aziende di qualunque settore e dimensione. «Si tratta di una suite che consente un notevole salto di qualità ai programmi di gestione delle vulnerabilità e verifica della compliance - evidenzia **Emilio Turani**, Managing Director per Italia, South Eastern Europe, Turchia e Grecia di Qualys -. Il monitoraggio dell'infrastruttura individua le vulnerabilità in modo tempestivo ed efficace, rendendo più sicure le risorse esposte e consentendo di definire la priorità delle misure di risoluzione da adottare».

di Giuseppe Saccardi

Verso un retail sempre più contactless

Self-scanning e scan-and-go di Scandit abilitano un retail contactless e più sicuro nell'attuale contesto di emergenza sanitaria

La pandemia in corso sta imponendo profondi cambiamenti nel modo di lavorare e cooperare in azienda. Ma è soprattutto nel retail che sono richieste soluzioni che permettano di operare in sicurezza e rispettando le nuove normative.

Secondo Scandit, (scandit.com/retail) società quotata tra i leader nelle soluzioni enterprise di mobile computer vision e realtà aumentata, la pandemia da Covid-19 ha generato la necessità di un "retail contactless", e questo è il motivo per cui nell'ultimo periodo DO e GDO stanno accelerando l'adozione di soluzioni di self-scanning e di scan-and-go.

Mantenere la distanza dagli altri e sentirsi sicuri entrando in un negozio significa che i clienti possono utilizzare il proprio smartphone per scegliere, acquisire informazioni e acquistare i prodotti, mentre i dipendenti possono svolgere le proprie attività con un'app per smartphone.

La ricerca "Forging a New Future in Convenience Retail" di TWC ha evidenziato in proposito che la pandemia da Covid-19 ha creato un aumento della domanda di casse self-scan e di pagamenti contactless, con due terzi delle persone che accoglierebbero favorevolmente le casse self-scan o un'applicazione per scansionare i prodotti e pagarli.

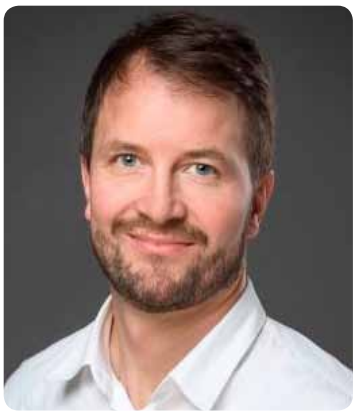
Shopping più veloce, più facile e frictionless

La promessa di uno shopping veloce, facile e "senza attriti" ha motivato numerose catene di supermercati a investire nello scan-and-go; tra queste ci sono 7-Eleven, Globus, Albert Heijn e Coop, solo per citarne alcune.

Con il giusto software di computer vision, qualsiasi smart device dotato di fotocamera può essere trasformato in uno scanner di barcode. I retailer utilizzano questa tecnologia per consentire ai clienti di leggere i codici a barre utilizzando il proprio smartphone e pagare la merce in un kiosk di self-checkout o attraverso l'app. L'azienda svizzera Valora ne è un esempio: il cliente inserisce il proprio ID nell'app per registrarsi ed entrare nel negozio, dove può fare acquisti grazie al self-scanning. In questo caso, per facilitare la registrazione, il software di scansione deve anche eseguire il riconoscimento del testo (OCR) e la verifica dell'ID, nonché la scansione dei codici a barre.

«I retailer hanno il dovere di salvaguardare i propri clienti e dipendenti, aiutandoli a svolgere il proprio lavoro tutelando la loro salute, attraverso processi contactless, che riducono al minimo ogni tipo di contatto. L'obiettivo è quello di farli sentire sicuri e protetti all'interno del negozio.

Credo che molti retailer pensino che l'emergenza Covid-19 e il distanziamento sociale non passe-



Christian Floerkemeier - Scandit

ranno nel breve periodo. Ciò significa che i supermercati vorranno pianificare le proprie attività tenendo presente questa nuova realtà. La semplicità e la velocità del mobile self-scanning e dello scan-and-go sullo smartphone di un cliente o di un dipendente, assicurano il mantenimento della distanza dagli altri e la tranquillità nell'entrare nei negozi», ha osservato **Christian Floerkemeier**, CTO & Co-Founder di Scandit.

Ridurre l'attesa, aumentare lo spazio, proteggere le entrate

Un obiettivo dei retailer è poi quello di ridurre i tempi di attesa per entrare nei punti vendita prima che i clienti decidano di recarsi altrove. L'obiettivo è quello di creare più spazio e ridurre il tempo che ogni cliente trascorre in negozio, e lo shopping tramite scan-and-go è di aiuto.

I tradizionali scanner comportano tuttavia un rischio sanitario per i clienti e un onere aggiuntivo per i retailer che devono gestirne l'igienizzazione. Spinti dalla domanda di uno shopping sicuro e senza contatto viene chiesto ai produttori, osserva Scandit, di aiutare i retailer a portare avanti i progetti esistenti e accelerare il roll-out delle app mobile per il self-scanning e lo scan-and-go utilizzando un software di scansione di codici a barre.

Segno del forte interesse è che alcuni dei clienti di Scandit hanno visto raddoppiare le transazioni all'interno del punto vendita tramite servizi di self-scanning e fatte con gli smartphone.

Il self-scanning è anche un modo efficace per aumentare la fidelizzazione. Un'esperienza di scansione efficace ed efficiente aiuta a risparmiare tempo e a rendere qualsiasi interazione il più possibile frictionless. In questo modo, si migliora la customer experience e, in ultima analisi, l'engagement.

In un settore sempre più basato sui dati, il self-scanning è anche una fonte di informazioni sul comportamento dei clienti. Monitorare l'utilizzo delle app insieme ai normali KPI del negozio permette di rilevare e misurare l'afflusso nel negozio, i tempi di attesa alla cassa, i modelli di acquisto, il valore della spesa, i ricavi, i costi e la soddisfazione del cliente.

Come iniziare

Maurizio Costa - Scandit

La consulenza da parte di esperti è importante per ottenere un'implementazione di successo del self-scanning. Come per qualsiasi altro servizio ai clienti, la user experience è fondamentale. Un ovvio fattore cruciale è la performance del software di scansione: deve funzionare fin dalla prima volta, ogni volta e su qualsiasi modello di dispositivo mobile utilizzato dai clienti.

I retailer dovranno accelerare la propria trasformazione digitale per competere con lo shopping online e soddisfare le nuove esigenze di sicurezza. In definitiva, la necessità di fondere il mondo fisico e quello digitale rimane più forte che mai nella nuova società contactless.

«In questo momento Scandit sta offrendo il proprio supporto ai retailer per accelerare e scalare le opzioni scan-and-go e click-and-collect per i clienti. L'evasione degli ordini effettuati con la scansione via smartphone è veloce, efficiente in termini di costi e contactless - e inoltre, è molto semplice da usare sia per gli addetti nei punti vendita che per i clienti», ha commentato **Maurizio Costa**, Sales Manager Italy di Scandit.

di Giuseppe Saccardi

Cloud e sicurezza non sempre vanno d'accordo

Il 70% delle aziende ha subito attacchi nel corso dell'ultimo anno. Lo evidenzia la nuova ricerca condotta dagli esperti di cybersecurity di Sophos

Secondo una recente ricerca svolta da Sophos, The State of Cloud Security 2020, quasi i tre quarti delle aziende (70%) ha subito un incidente di sicurezza che ha colpito il cloud nel corso dell'ultimo anno.

All'origine di questo preoccupante fenomeno gli attacchi ransomware e malware (50%), l'esposizione dei dati aziendali (29%), gli account compromessi (25%) e il cryptojacking (17%).

Inoltre, le aziende caratterizzate da ambienti multi-cloud hanno il 50% di possibilità in più di essere esposte a rischi informatici di quelle che si avvalgono di un solo cloud.

In questo quadro a tinte fosche, l'Europa, osserva Sophos, risulta l'area geografica meno a rischio e ciò sembra confermare la validità e l'efficacia della normativa GDPR. Ad aver subito il maggior numero di attacchi a livello cloud è invece l'India, che con il 93% di aziende colpite nel corso dell'ultimo anno rappresenta il dato più negativo.

«Il Ransomware si conferma la minaccia che più spesso mette a rischio il cloud: gli attacchi di questo tipo registrano particolare successo nel sottrarre i dati dal public cloud, come già evidenziato nella ricerca svolta da Sophos "State of Ransomware 2020" e forti di questa consapevolezza i cybercriminali stanno utilizzando questa tecnica anche per colpire ambienti cloud che, una volta compromessi, paralizzano le infrastrutture indispensabili, aumentando così le probabilità di ottenere il pagamento di un riscatto» spiega **Chester Wisniewski**, principal research scientist di Sophos. «Il recente sensibile incremento del ricorso al lavoro da remoto ha fornito ai cybercriminali l'occasione ideale per tentare di neutralizzare le infrastrutture cloud strategiche ed è preoccupante che molte aziende continuino a sottovalutare l'importanza del mettere al sicuro i dati in cloud e i workload. La sicurezza del cloud è una responsabilità condivisa e le aziende devono monitorare e gestire con estrema attenzione gli ambienti in cloud al fine di essere sempre un passo avanti rispetto agli intenti dei cybercriminali».

Dal porta dimenticata aperta entrano i cybercriminali

L'esposizione accidentale dei dati resta una vera piaga aziendale e la scorretta configurazione

del cloud è all'origine del 66% degli attacchi.
Gli errori di configurazione rappresentano ancora il canale di veicolazione principale per gli incidenti di sicurezza e sono ancora troppo diffusi se si considera la complessità insita nella gestione del cloud.
Un altro aspetto inquietante emerso dalla ricerca di Sophos riguarda i furti delle credenziali di accesso al cloud provider: il 33% delle aziende ha infatti dichiarato che è così che i cybercrminali hanno avuto accesso.
Ciò nonostante, solo un quarto delle aziende ritiene che gestire gli accessi agli account cloud sia una preoccupazione prioritaria.
I dati emersi da Sophos Cloud Optix (uno strumento che offre alle aziende funzionalità di analisi e visibilità ininterrotta necessarie per identificare, rispondere e prevenire le lacune di sicurezza e conformità che espongono i sistemi ai rischi) ha rivelato poi che il 91% degli account gode di privilegi di accesso e gestione non necessari e il 98% ha disattivato l'autenticazione multi-fattore sugli account dei provider del servizio cloud.

Lo scenario italiano

Tra il campione di 26 Paesi coinvolti in questa ricerca, l'Italia è quello ad aver registrato la percentuale più bassa di incidenti di sicurezza nel public cloud nel corso dell'ultimo anno: il 45% degli intervistati ha infatti confermato di aver dovuto far fronte a un incidente di sicurezza in tale ambito, contro il 75% del campione francese e il 61% di quello tedesco
Nonostante questo dato in parte rassicurante, ben il 97% degli intervistati italiani ha ammesso di essere preoccupato dai potenziali rischi in termini di sicurezza informatica quando si parla di Cloud.
All'origine della maggior parte degli incidenti di sicurezza (ben l'81%) vi è la configurazione scorretta del cloud che apre la porta agli attacchi. Piuttosto contenuto il dato che riguarda invece il furto delle credenziali, che è la causa del solo 17% dei casi di attacchi al cloud.

Cresce la consapevolezza dei rischi nel cloud

Nonostante dalla ricerca emergano molti dati ancora sconfortanti, va altresì segnalato che quasi tutti gli intervistati (il 98%) hanno ammesso di essere preoccupati per il loro attuale livello di sicurezza in-the-cloud, il che dimostra che si è raggiunta una maggiore consapevolezza dell'importanza di proteggere in modo adeguato questo specifico ambito dell'infrastruttura aziendale.
Il furto di dati è naturalmente in cima alla lista dei problemi di sicurezza per quasi la metà degli intervistati (44%); l'identificazione e la necessità di rispondere tempestivamente agli incidenti di sicurezza si posizionano secondo posto per il 41% degli intervistati.
Tuttavia, a conferma che ci sia ancora molta strada da fare, va segnalato che ancora oggi solo un intervistato su quattro considera la mancanza di competenze dello staff aziendale come una preoccupazione prioritaria.

di Giuseppe Saccardi

Più attenzione alla cybersecurity dei lavoratori da remoto

Cresce la consapevolezza dei rischi alla sicurezza anche se i comportamenti pericolosi rimangono molti. Trend Micro evidenzia come porvi rimedio

Lisa Dolcini - Trend Micro

Durante il "lockdown", il 73% degli italiani che ha lavorato da remoto ha sviluppato una maggior consapevolezza nei confronti della cybersecurity, ma i comportamenti a rischio sono ancora molti. Il dato emerge da una recente ricerca dal titolo "Head in the Clouds" commissionata da Trend Micro alla società Sapio Research. Ha coinvolto 13.200 lavoratori da remoto in 27 Paesi e in Italia il campione è stato di 506 dipendenti di aziende di diverse dimensioni e settore.

Lo studio, che aveva l'obiettivo di approfondire l'attitudine dei lavoratori da remoto nei confronti delle policy aziendali IT e di cybersecurity, ha rivelato che il livello di sicurezza oggi è alto più che mai.

Lo conferma, osserva **Lisa Dolcini**, Head of Marketing di Trend Micro Italia, il fatto che ben l'88% dei dipendenti italiani ha dichiarato di osservare attentamente le istruzioni del team IT e che l'86% è concorde nell'affermare che la sicurezza aziendale sia parte integrante delle responsabilità di ognuno. Inoltre, il 64% riconosce che l'utilizzo di applicazioni non ufficiali costituisce un serio rischio.

Riconoscere i rischi non per forza è sinonimo di comportamenti responsabili. A evidenziarlo il fatto che:

- Il 51% dei dipendenti utilizza applicazioni non ufficiali sui dispositivi aziendali e il 34% vi custodisce dati corporate.
- il 74% utilizza il computer aziendale per navigare a scopi privati.
- Il 37% accede a dati aziendali da un dispositivo personale, violando le policy di sicurezza.
- L'11% accede a siti hot con il PC aziendale e il 5% al dark web.
- Il 21% consente l'accesso al dispositivo aziendale a persone non autorizzate.
- I dati della ricerca evidenziano comunque la forte attenzione che viene posta al problema della security per quanto concerne il lavoro remoto e lo smart working.

«È incoraggiante vedere quante persone prendono seriamente i consigli del team IT e capiscono che la protezione della propria azienda sia anche una responsabilità individuale, anche se verrebbe da chiedersi perché gli altri non lo fanno - ha affermato Lisa Dolcini -, Le criticità sembrano però esserci quindi le consapevolezze sulla cybersecurity devono tradursi in com-

portamenti concreti. Le aziende devono tenere ben presenti le differenze all'interno della propria forza lavoro e insistere sulla formazione e sulla consapevolezza, in un momento in cui la cybersecurity è finalmente riconosciuta dai dipendenti come fondamentale».

Smart working sicuro nel cloud e ovunque

Se da un'analisi della situazione si passa a considerare come migliorare la postura aziendale in relazione alla tumultuosa trasformazione in atto, una considerazione di base da fare è che si parla di smart working, ma di fatto si tratta di home working, visto come traslazione della postazione di lavoro dall'interno all'esterno dell'azienda.

In sé, le pratiche per una corretta protezione non sono cambiate rispetto a prima e non cambiano con il lavoro da remoto. L'home working potrebbe però portare le aziende a rivedere le strategie al fine di fornire ai dipendenti delle connessioni più sicure. Quello che appare suggeribile, osserva Lisa Dolcini, è concentrare le proprie priorità su tre aspetti essenziali.

Proteggere il dato ovunque si trovi. I dati sono il capitale aziendale ed è compito dell'IT e del management fornire ai dipendenti i giusti dispositivi, gli strumenti e le corrette linee guida per l'utilizzo e le pratiche di smart working, oltre a fare tutto il necessario per mettere in sicurezza l'infrastruttura aziendali e i dispositivi dei dipendenti.

Proteggere l'infrastruttura. Il collegamento alla rete aziendale deve basarsi su VPN, che però garantisce la sicurezza nello scambio di comunicazioni ma non del loro contenuto. Per questo è importante installare sul dispositivo utente un software Antivirus che garantisca una protezione completa. Va anche verificato di aver installato tutti gli aggiornamenti sia del sistema operativo che dei programmi utilizzati, quali la suite di Office, il reader dei file pdf, il browser Internet e tutti i programmi che vengono utilizzati.

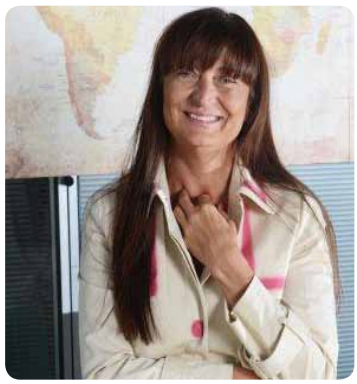
Proteggere il collegamento. Nel caso in cui si utilizzi un router commerciale, non gestito da un operatore telefonico, va verificato che il firmware sia aggiornato e la password non sia quella di dotazione. Ciò vale anche per la rete wi-fi. Vanno poi attivate le funzionalità di firewall, presenti di default, anche nei sistemi operativi che hanno una configurazione standard.

«Il lavoro da remoto è oggi un mezzo molto efficace a supporto della gestione dell'emergenza sanitaria. In una prima fase le aziende che non avevano previsto una situazione del genere, in cui migliaia di lavoratori hanno iniziato a lavorare contemporaneamente da casa, sono andate sotto stress, a causa di un'ampiezza di banda non sufficiente e l'impossibilità di garantire lo stesso livello di sicurezza ai dispositivi che si connettevano dall'esterno della rete aziendale. Sicuramente hanno sofferto maggiormente le aziende con infrastrutture on-premise, mentre quelle che erano più avanti nella trasformazione digitale e avevano adottato soluzioni cloud sono state in grado di gestire la situazione in maniera più reattiva. Passata questa prima fase, dove le aziende hanno sistemato o semplicemente integrato l'infrastruttura esistente, ci troviamo ora in una seconda fase, che vedrà molto probabilmente il consolidamento del lavoro da remoto come normale abitudine lavorativa. È quindi un'ottima occasione per approntare le giuste procedure ove non ancora fatto, per garantire la sicurezza dell'infrastruttura», osserva Lisa Dolcini.

di Giuseppe Saccardi

I data center richiedono innovazione e nuovi standard

La realizzazione di data center basati su moduli prefabbricati è guardata con crescente attenzione e Vertiv ritiene che diventeranno i nuovi standard



Cristina Rebolini - Vertiv Italia

Quando si parla di data center è opportuno distinguere tra le diverse tipologie esistenti. In particolare, prefabbricati e modulari sono metodologie distinte, ma i dati di mercato indicano che l'adozione dei cosiddetti data center prefabbricati modulari (chiamati anche PFM), che combinano entrambe le tecniche, sono in rapida crescita.

Secondo gli analisti di settore di 451 Research, evidenzia in proposito **Cristina Rebolini**, Commercial, Industrial and Enterprise Sales Director di Vertiv (www.vertiv.it) in Italia, il mercato dei data center PFM si sta espandendo, ed entro il 2021 raggiungerà un tasso di crescita annuale cumulativo (CAGR) del 14,4%.

La ragione di questa crescita è legata essenzialmente alle implementazioni a basso rischio e ad alto valore aggiunto, con il vantaggio di una consegna più rapida e un'installazione in loco più facile.

Ma la nuova tecnologia, spiega Rebolini, introduce un divario di conoscenza e un rischio percepito dell'ignoto: cosa intendiamo quando diciamo prefabbricati e modulari, e quali vantaggi assicurano alla costruzione, al funzionamento e alla ottimizzazione di strutture critiche come i data center?

L'impatto dell'Edge Computing

La crescita esponenziale della Digital Transformation aggiunge a quelle usuali la preoccupazione di come gestire l'imprevedibile crescita della domanda pur rimanendo flessibili per il futuro.

I casi d'uso nel settore delle applicazioni di Edge Computing richiedono potenzialmente un grande numero di data center medio-piccoli (o addirittura micro) per gestire i carichi di lavoro associati a un'esplosione della domanda legata ad esempio all'IoT.

Le implementazioni in un sito Edge possono poi spaziare da un impianto da 5MW in città a un singolo rack posizionato vicino a un'antenna 5G sul tetto di un edificio.

Far fronte a queste innovazioni che vanno dal core all'Edge con approcci convenzionali è quasi impossibile. Gli approcci tradizionali, come il processo di costruzione "stick-build", hanno rappresentato la scelta scontata per molte organizzazioni semplicemente perché non c'era alcuna alternativa praticabile.

Tuttavia, i metodi tradizionali si sono rivelati in molti casi inefficienti in quanto non sono stati in grado di rispondere ai requisiti di sviluppo accelerato delle organizzazioni più dinamiche, spes-

so non prevedendone un'adeguata crescita.
«In un tale scenario - osserva Rebolini -, metodi prefabbricati e/o modulari sono sempre più la scelta degli operatori dei data center per un approccio integrato e scalabile. Questo perché la progettazione, la configurazione e l'integrazione delle varie componentistiche direttamente a livello di fabbrica permettono di ottenere un'integrazione più stretta tra i sistemi, migliorandone la gestione e rendendo più lineari i processi».

Il perché di un data center prefabbricato e modulare

Ciò che rende attraenti i data center PFM è il fatto che sono delle soluzioni che includono l'intera gamma delle unità necessarie per gestire la potenza elaborativa del data center, dai singoli componenti ai sistemi più complessi, compreso le infrastrutture elettriche e termiche, software e servizi di controllo e gestione, oltre a impianti secondari come illuminazione, protezione antincendio, sicurezza fisica e sistemi anti allagamento.
I vantaggi dei PFM includono in pratica un progetto su misura del cliente, tempi di installazione più veloci, la possibilità di scalare ed espandere la capacità in base alla domanda, prestazioni ottimizzate dei componenti con una visione olistica del sistema e controlli di qualità elevati.
E non ultimo, osserva Rebolini, il fatto di poter trovare un'applicazione che spazia dal core fino all'Edge di un'infrastruttura IT.
A livello costruttivo, i moduli prefabbricati comprendono data center e altre strutture critiche che sono pre-ingegnerizzate con sistemi assemblati, integrati e testati in un ambiente di fabbrica per ridurre i tempi di implementazione in loco e migliorare la prevedibilità delle prestazioni sia in termini di pianificazione sia di costi.
Per l'espansione di strutture pre-esistenti e retrofit, sono previste inoltre soluzioni fondanti che spaziano da rack chiusi singoli a sistemi multirack più grandi, mentre, nel caso delle nuove costruzioni, consentono alle organizzazioni di portare nuove capacità più velocemente e possono essere facilmente scalabili.
I metodi modulari progettano il piano di crescita nella soluzione fin dall'inizio. Un data center PFM è progettabile su misura per adattarsi al clima, al profilo tecnologico, alle applicazioni IT e agli obiettivi di business di un progetto, sfruttando al tempo stesso la velocità e l'economia della progettazione modulare e della prefabbricazione.
«Le tecniche di integrazione modulare combinate con il processo di prefabbricazione off-site si traducono nel concreto in una struttura che risulta allo stato dell'arte, integrata e con un costo complessivo inferiore rispetto ad una struttura simile che faccia ricorso a pratiche costruttive tradizionali», spiega Rebolini.

Dalla teoria alla pratica

Un esempio specifico di questa tecnologia in azione, osserva Rebolini, è fornito dalla famiglia Vertiv SmartMod™, una gamma di prodotti configurabili, ordinabili come moduli prefabbricati per aggiungere nuovo spazio ai data center, con un numero significativamente inferiore di attività di installazione in loco rispetto ai data center costruiti tradizionalmente.
L'approccio "plug and play" che li caratterizza è stato ideato al fine non solo di minimizzare i tempi per l'avviamento e la messa in funzione (da settimane o mesi a pochi giorni, evidenzia Rebolini), ma anche di ridurre le potenziali problematiche di qualità, in quanto i componenti sono pre-integrati e pre-testati off-site. Inoltre,

Data center modulare
di Vertiv Italia

nel caso di una distribuzione di più unità o in più sedi, avere layout e sistemi comuni semplifica le attività di manutenzione e funzionamento.
Oltre a SmartMod, concepito per alloggiare apparecchiature IT in un sistema autonomo, Vertiv ha reso disponibile anche il modulo di potenza Power Module. L'involucro del Vertiv Power Module, trasportabile e resistente alle intemperie, protegge i componenti interni tra cui l'UPS ad alte prestazioni Liebert EXL S1 e le batterie.
Inoltre, il sistema di Thermal Management Liebert PDX, specificatamente indicato per Power Module, ha anche la funzione di garantire che l'apparecchiatura mantenga condizioni operative ottimali in modo da prolungarne la durata.
Come per l'unità SmartMod, Power Module è fornito con un condensatore per esterni a microcanali Liebert MC pre-integrato, cosa che evita l'esigenza di dover installare sistemi di raffreddamento esterni in loco e permette di ridurre i tempi di avviamento dei sistemi.

Data Center PFM in field: il caso T-Systems

Un esempio realizzativo dove i data center modulari mostrano la loro validità è quanto realizzato da T-Systems. La società, per rispondere alle esigenze dei clienti, ha avuto la necessità di fondere requisiti diversi con l'obiettivo di ottenere disponibilità, affidabilità, sicurezza, scalabilità, sostenibilità e, non ultimo, una rapida implementazione.
Dopo un'approfondita analisi, la realizzazione modulare in container prefabbricati si è rivelata essere l'opzione più adatta per garantire rapidamente ed efficacemente l'elevata scalabilità atta a favorire future fasi di espansione e investimenti pianificati.
Progettato ad hoc e costruito nello stabilimento dedicato alle soluzioni modulari integrate di Vertiv in Croazia, e trasferito poi a Barcellona (Spagna), il data center di T-Systems è formato da 38 moduli integrati che ospitano centinaia di rack Knürr, molteplici unità di Thermal Management Liebert e sistemi di alimentazione AC Chloride. L'infrastruttura modulare include l'isolamento, la protezione antincendio, il monitoraggio e il controllo di sicurezza degli accessi.
Mentre in fabbrica venivano costruiti i container, il sito veniva preparato con le opere civili per accogliere l'installazione finale. Successivamente sono stati consegnati i moduli integrati secondo una precisa tabella di marcia, assemblati e collegati a tutti gli impianti elettrici, meccanici e idraulici. Al termine, la struttura si è presentata come un edificio tradizionale, sia dall'esterno che dall'interno, comprese, per esempio, sale riunioni, corridoi e passaggi sopraelevati per accedere a tutte le aree dell'infrastruttura.