Cloud & Business

n.70
Aprile 2018

LA RIVISTA PER IL MANAGER CHE DEVE OTTIMIZZARE COSTI E PROCESSI

IN QUESTO NUMERO

COVER STORY

LA TRASFORMAZIONE DIGITALE AVANZA CON IL CLOUD

Cloud e digital transformation sono un connubio sempre più stretto per le nuove strategie IT e per esternalizzarne in modo sicuro la complessità

La trasformazione digitale si conferma come un potente motore per lo sviluppo industriale e dei servizi del sistema paese. E' quanto raccontano anche i dati che emergono da una recente ricerca: The Digital Transformation PACT, che ha esaminato le performance delle aziende nei confronti dei quattro elementi strategici necessari per potersi trasformare digitalmente: Persone, Azioni, Collaborazione e Tecnologia (PACT).

Il campione italiano (per il 56% degli intervistati) ha messo in evidenza, ha osservato Fujitsu, sponsor della ricerca, come nelle loro organizzazioni la tecnologia digitale venga utilizzata non solo a livello di processi e funzioni aziendali, ma anche al fine di crearne di nuovi, da affiancare a quelli esistenti, non ancora coinvolti e interessati dalla digitalizzazione.
Principale driver della trasformazione digitale si evidenziano essere i clienti (per il 39% degli in-

Reportec Cloud&Business - Numero 70 - Aprile 2018 - Registrazione al tribunale n°574 del 5 Novembre 2010 -
Tutti i marchi sono di proprietà delle relative società- Editore: Reportec Srl (www.reportec.it) - Direttore responsabile: Giuseppe Saccardi - In redazione: Gaetano Di Blasio - Grafica: Paola Saccardi - Immagini: Dreamstime.com

Reportec

tervistati), seguiti a breve distanza da partner e terze parti (35%) e, non meno significativo, i concorrenti (33%).

Il ruolo delle tecnologie dal cloud alla security

E sotto il profilo tecnologico cosa si prospetta? Nei programmi degli intervistati, evidenzia la ricerca Fujitsu, nei prossimi 12 mesi ci sono progetti che riguardano, non sorprendentemente dato anche l'impatto del GDPR, i sistemi di sicurezza informatica (59%), l'Internet of Things (51%) e il cloud computing (43%), visto come strumento per esternalizzare la crescente complessità dell'IT e accelerare l'adozione di nuove tecnologie senza dover ricorrere a cospicui investimenti in Capex.

Relativamente al tema della sicurezza informatica, il 95% afferma che questa è fondamentale per supportare il successo finanziario della propria organizzazione nei prossimi 10 anni. In egual misura - 95% - vengono citati anche big data e analytics.

Se la tecnologia ha di certo un ruolo importante, un pari valore lo ha il fattore umano. Il gap di competenze interne si è infatti evidenziato come uno dei maggiori ostacoli per affrontare uno dei temi salienti della trasformazione digitale e della sua proiezione in uno scenario aperto e globale sempre più basato sulla mobility e il cloud: la cybersecutity e come garantirla.

Quello della sicurezza cibernetica e la protezione di applicazioni, dati e dispositivi di utente è un tema di primo piano e di importanza strategica per la propria organizzazione: lo afferma il 68% del campione italiano. Pur con qualche minimale resistenza e titubanza nell'affrontare il problema, la maggior parte non sta a guardare e il 91% dichiara di stare lavorando per attrarre e disporre di maggiori competenze digitali.

Un punto molto condiviso è che l'aggiornamento non basta e la capacità di saper attrarre e reclutare le persone diventa cruciale (37% del campione). Ad esempio, l'85% dei manager ritiene che entro il 2020 l'Intelligenza Artificiale (AI) nelle sue varie implicazioni inciderà sulla tipologia di competenze necessarie per la propria organizzazione, tanto che il 93% di essi si sta muovendo per far fronte a questa necessità e il 91% ammette che saper attrarre personale 'native digitali' sarà vitale per il successo della sua azienda nei prossimi tre anni.

L'importanza di una chiara strategia e collaborazione

Per avere successo deve essere chiaro dove andare e come giungervi. In pratica, serve una chiara e perseguibile strategia. La strategia è alla base del successo di un progetto di trasformazione digitale e il 92% del campione italiano dichiara di averne una ben definita, grazie anche al coinvolgimento diretto del top management (94%); questo però non preclude l'esistenza di ciò che va sotto il nome di "Shadow IT", ovvero

l'esistenza di cosiddetti progetti ombra, avviati senza un'approvazione organizzativa esplicita.
Si tratta di progetti che per i quasi due terzi (62%) del campione costituiscono un serio problema per la loro organizzazione, anche se il 59% dichiara che spesso sono l'unico modo per provare ad ottenere un'innovazione significativa.
Qualunque siano gli obiettivi, la co-creazione si prospetta come la chiave del successo. In generale, le organizzazioni italiane appaiono aperte a un mondo collaborativo: il 58% sta implementando o sta pianificando progetti di co-creazione in cui lavorano a stretto contatto con un'altra organizzazione per fornire innovazione digitale.

Di certo si tratta di un cambiamento significativo nel panorama nazionale dove la predominanza di piccole e medie aziende a conduzione padronale aveva dato origine a un approccio che aveva sempre evidenziato una ridotta se non nulla propensione alla collaborazione con l'esterno e la difficoltà ad inserirsi n una filiera produttiva.
Laddove questa barriera è stata rimossa i partner preferenziali sono esperti di tecnologia, scelti dal 53% del campione, start-up (46%) o altre organizzazioni (45%), anche e indicativo del cambiamento di mentalità in atto dello stesso settore (31%).
Ma come rispondono le aziende ai diversi problemi esposti dalle aziende coinvolte nella trasformazione? Vediamo alcuni casi di aziende impegnate in diversi settori dell'IT.

Cloud più facile con l'Iperconvergenza

Trasformazione e digitalizzazione richiedono, come osservato, tecnologie di nuova concezione. Un esempio è quanto sta accadendo con le soluzioni riferite come iperconvergenti, uno dei modi studiati per semplificare lo sviluppo di infrastrutture cloud ibride o multi-cloud, ideate anche per rispondere alla necessità di trattare crescenti volumi di dati, in cloud o on-premise.
L'approccio proposto da NetApp per affrontare una digital transformation centrata sui dati, è costituito da NetApp HCI (NetApp Hyper Converged Infrastructure), una piattaforma che copre sia le esigenze delle applicazioni business on-premise che nel cloud ibrido, in modo da coniugare l'esigenza di mantenere pieno controllo della parte IT con i benefici e la flessibilità assicurata dal cloud.
NetApp HCI si basa su un software, Data Ontap, omogeneo su tutta la sua linea di prodotti, on premise o nel cloud, che garantisce la portabilità dei dati ed applicazioni da e verso il cloud in modo trasparente, e su un hardware che utilizza in modo estensivo tecnologie di storage Flash che si caratterizzano per elevata velocità e bassi consumi. Alle caratteristiche fisiche si abbinano funzioni che garantiscono la sicurezza del dato e la produttività delle applicazioni all'interno dell'intera organizzazione.
NetApp HCI costituisce in pratica una soluzioni per data center di prossima generazione che semplifica e accelera l'implementazione delle applicazioni. Ad esempio, è possibile eseguire applicazioni multiple con livelli prestazionali ga-

rantiti e far leva su una flessibilità, una scalabilità e un'automazione elevata.
Per far fronte alla gestione di volumi di dati la cui crescita e le cui dinamiche non sempre sono facilmente prevedibili la soluzione NetApp si basa sulla tecnologia storage flash SolidFire, che fornisce la sicurezza indispensabile al fine di consolidare i diversi carichi di lavoro generati dalle applicazioni, di scalare senza sprecare risorse e garantire le performance richieste dalle applicazioni di nuova concezione.
La soluzione comprende in un'unica architettura building block indipendenti che forniscono le risorse di calcolo, di storage e di connettività.
L'unità minima è composta da due blocchi di calcolo e quattro di storage in modo da costituire sin dall'entry level una soluzione ridondata. L'espansione può poi avvenire con moduli storage e di calcolo o con solo storage o solo calcolo a secondo che serva più capacità storage o computazionale.
La soluzione, basata su SolidFire, ha commentato Patano, senior manager systems engineer di NetApp, permette in sostanza alle organizzazioni di sfruttare appieno le potenzialità della propria infrastruttura grazie alla possibilità di semplificare la gestione e di scalare autonomamente e in modo flessibile le risorse.

La soluzione per HCI di NetApp

Sviluppata avendo in mente le esigenze di ambienti cloud, infrastrutture web, database e di consolidamento del workload, NetApp HCI si integra facilmente con le soluzioni dei principali partner, come quelle di Commvault, Intel, MongoDB Enterprise, Veeam e VMware.

Data Intelligence e cloud la chiave per il business

L'importanza di un cloud in grado di trattare volumi crescenti di dati è alla base della vision anche di un'altra azienda impegnata nel facilitare la trasformazione digitale, Hitachi Vantara, dato che però va raccolto, protetto, analizzato e fruito al fine di produrre valore per le aziende, aziende che devono affrontare numerose sfide sia sul piano del mercato che della concorrenza.
Il volume di dati che si generano e la possibilità di far leva su di essi, osserva **Marco Tesini,** country manager di Hitachi Vantara in Italia, ha ridotto le barriere e aperto spazi che nuove aziende si stanno approntando a riempire a scapito degli incumbent abituati ad avere rendite di posizione. E' una sfida che il mercato sta affrontando e che Hitachi Vantara si è proposta di supportare incrociando due vettori chiave della trasformazione in atto: il primo è la enorme crescita dei dati e il secondo è l'esigenza di semplificazione al fine di gestire in modo efficace questa mole di informazioni.
Per fronteggiare la crescita esponenziale del volume dei dati l'azienda ha ampliato l'offerta storage ed ha integrato in Hitachi Vantara due aziende. La prima, Pentaho, è specializzata negli analytics, la seconda, Insight Group, nello sviluppo di piattaforme per l'IoT. Di fatto, con queste due organizzazioni si è proposta di assumere il ruolo di attore principale del Gruppo Hitachi nel favorire il processo di trasformazione digitale, in primis nel Gruppo e poi nel mercato.
In maggi l'azienda ha anche a piano il rilascio di soluzioni Storage che risponderanno alle esigenze relative ad ambienti ibridi o nel cloud e permetteranno di disaccoppiare il software dall'hardware. Saranno soluzioni storage, ha spiegato Tesini, dotate in maniera nativa di applicazioni derivate dal mondo IoT, in grado di auto ottimizzarsi e con un up-time garantito del 100%, do-

Marco Tesini - Hitachi Vantara

tate anche di funzionalità di data protection e containers ready.
Peraltro, ha evidenziato il manager, per una azienda che volesse esternalizzare la complessità dell'IT tutto quello che fa parte del portfolio di soluzioni un cliente lo può acquisire come preferisce: in modalità Capex, Opex o "as a Service".

Convergenza e flash per data center cloud-ready

Impegnata nel rilascio di soluzioni atte a favorire l'adozione di nuove architetture pronte per il cloud e più semplici da gestire è anche un altro dei big dell'IT, Fujitsu. La società ha di recente annunciato che ha disponibile la soluzione NFLEX Converged Infrastructure, una piattaforma sviluppata e commercializzata congiuntamente con NetApp.
Obiettivo dell'iniziativa, ha spiegato l'azienda, è stato quello di eliminare la complessità insita nell'implementazione e nella gestione di ambienti applicativi virtualizzati all'interno dei data center, nel cui ambito NFLEX si prefigge di costituire per medie e grandi aziende una soluzione infrastrutturale semplice da installare ed esercire e "ready to use".
A livello di architettura e gestione NFLEX Converged Infrastructure si caratterizza per un dimensionamento a moduli del sistema, un singolo punto di contatto unificato per l'assistenza da parte di Fujitsu e NetApp e una sua gestibilità integrata. Una volta in opera, la soluzione pre-configurata permette, ha spiegato Fujitsu, di ridurre i costi di implementazione e funzionamento e supportare la crescita del business tramite la possibilità di scalare la capacità storage e/o di calcolo in base al workload da supportare mediante "expansion pack" preconfigurati .
Il core della soluzione è costituito dai nuovi server Fujitsu Primergy CX400 M4 e il suo utilizzo è suggerito laddove si deve aumentare le prestazioni e la produttività del data center mettendo a disposizione servizi IT di maggior valore e a costi contenuti.
Obiettivi perseguiti dal progetto sono stati la facilità di utilizzo e una semplificazione dell'esperienza end-to-end dei clienti a partire dal momento stesso dell'acquisto. Un approccio, ha commentato Fujitsu, che si applica anche a tutte le fasi di installazione e gestione operativa fino al supporto di sistema.
Nel pensare al cloud non si deve però fare l'errore che fanno molti. In genere, mette in guardia **Bruno Sirletti**, Presidente e AD di Fujitsu Italia, si è portati a pensare che con il cloud tutto sia diventato più semplice. In realtà con il cloud le cose si sono complicate e questo perché la sua diffusione ha fatto sì che il CIO di un'azienda abbia perso in parte il controllo di quanto è installato in azienda. E' il concetto di "shadow IT", dovuto al fatto che ad esempio il responsabile marketing può comprare all'insaputa del reparto IT un servizio cloud di terzi perché rientra nei suoi limiti di spesa. Per il CIO dunque diventa difficile sapere esattamente cosa c'è in azienda e quello che ne risulta è un aumento della

Bruno Sirletti - Fujitsu Italia

complessità gestionale. Per rimediare a questo impasse Fujitsu ha sviluppato un nuovo servizio di Hybrid IT dedicato al la gestione di ambienti multi cloud.

La sicurezza per il cloud diventa adattativa

Un aspetto fortemente correlato al cloud e alla trasformazione digitale è la crescente esigenza di sicurezza, sia in termine di approccio da adottare che di soluzioni atte a garantirla a device e utenti.

La trasformazione digitale fa si, osserva **Emiliano Massa**, AVP Sales South EMEA di Forcepoint, che gli utenti IT possano accedere ed interagire con i dati aziendali, spesso critici, attraverso una miriade di sistemi, applicazioni e dispositivi. Quello che è suggeribile è quindi, piuttosto che concentrarsi sulla costruzione di muri più grandi e spessi, enti ed aziende si concentrino sul come ottenere una migliore visibilità di cosa accade nella propria infrastruttura, fisica o virtuale, e da questo trarre informazioni che permettano di migliore la sicurezza e prevenire gli attacchi, o, bloccarli sul nascere.

Per proteggere dati e applicazioni in uno scenario complesso come quello attuale Forcepoint ha concretizzato un approccio riferito come "Human Point System", che consiste nel mettere a fattor comune quanto inerente le esigenze di sicurezza di utenti, dati e rete, sia in cloud che a livello di singolo dispositivo.

Emiliano Massa - Forcepoint

L'approccio comprende capacità integrate che forniscono controllo e visibilità dettagliate su identità, attività e intenti dell'utente che accede e opera nella rete IT attraverso installazioni cloud, applicazioni e reti distribuite complesse. In pratica, l'obiettivo perseguito consiste nel supportare ad alto livello enti ed organizzazioni nel proteggere in modo efficace utenti e dispositivi in un mondo digitale del quale non sempre è possibile garantire il completo controllo.

Se poi ci si proietta più avanti nel tempo, in futuro, è fondamentale, suggerisce il manager, che le organizzazioni implementino soluzioni di sicurezza intelligenti integrate che forniscano visibilità sul comportamento degli utenti, insieme a programmi di sicurezza informatica definiti in modo preciso e puntuale. Comprendendo l'accesso ai flussi di dati, è possibile aumentare l'efficacia della sicurezza. Analizzando ed identificando comportamenti normali e anomali degli utenti, è poi possibile ridurre la complessità e concentrarsi sugli eventi che contano veramente.

L'analisi comportamentale mette al sicuro gli end-point

Cloud, mobility e digitalizzazione sono i punti chiave per avere successo in un mercato estremamente dinamico ed esigente, ma sono fattori che quando messi a fattor comune espongono a crescenti rischi.

Quello della Cyber Security e, del suo rapporto con il cloud e la mobility, evidenzia **Antonio Pusceddu**, Country Sales Manager per l'Italia di F-Secure, è un problema che coinvolge in modo trasversale qualsiasi settore industriale, pubblico e dei servizi e che vede crescere costantemente le minacce, sia in termini quantitativi che qualitativi.

I fattori sono numerosi e tra questi i principali sono il numero crescente di dispositivi interconnessi, con l'esigenza di proteggere gli end-point e il crescente ricorso al cloud come mezzo per esternalizzare la complessità dell'IT. A questo, per quanto concerne l'Industry 4.0 e gli ambienti

Antonio Pusceddu - F-Secure

privati e pubblici Smart, si aggiunge il problema di come garantire la sicurezza di una trasformazione digitale che porterà in breve tempo ad avere miliardi di dispositivi IoT interconnessi.

Identificare una soluzione, o un prodotto non è però sufficiente, o almeno, non lo è da solo, serve una visione di ampio respiro e approcci del tutto nuovi.

Quello che necessita e la strada che ha intrapreso F-Secure, evidenzia Pusceddu, è di ricorre a strumenti che sfruttano l'human behaviour, l'analisi comportamentale, il tutto inserito in una visione olistica, e che permettano di meglio prevenire ed individuare gli attacchi, nonché ricorrere a soluzioni come quelle che ha sviluppato di Managed Detection & Response, di Endpoint Detection & Response nonché di Incident Response Services.

Sono servizi che nello specifico eroga tramite team di esperti che permettono ad un'azienda o a una PMI di essere protetta senza doversi dotare di conoscenze che sono sempre più difficili da perseguire anche per chi ha ampie disponibilità di budget, e praticamente fuori dalla portata del bilancio di qualsiasi PMI.

Mettere al sicuro dati, infrastruttura e applicazioni

Quando si parla di trasformazione digitale il pensiero corre al cloud ma più un sistema si estende e si accresce di componenti più diventa insicuro. Con il crescere dell'automazione aziendale cresce infatti anche il rischio e i costi conseguenza di un fuori servizio, per quanto possa essere temporaneo.

In parallelo all'automazione quello che si rende necessaria, osserva **Albert Zammar**, Regional Vice President della Southern EMEA Region di Veeam, è anche una soluzione che faccia fronte ai momenti critici che possono verificarsi e se questi proprio non possono essere evitati, si preoccupi d i ricreare in tempi rapidi e con un elevato automatismo le usuali condizioni operative.

Quello di ripristinare le condizioni di lavoro, di rendere di nuovo disponibili dati e applicazioni, e di farlo in pochi minuti, è il compito che si è assunta Veeam Software con il rilascio della soluzione Veeam Availability Platform.

Nella sua essenza, si tratta di una suite di prodotti software progettati per garantire ad un'azienda la continuità operativa in modo da permettere, rispondendo a stretti requisiti SLA e con rapidi tempi di recovery dei fuori servizio o di perdita di dati, di trarre il massimo dei benefici dagli investimenti che un'azienda fa in server, storage e servizi cloud nel corso di una trasformazione digitale. Tre i punti salienti e critici che la soluzione affronta.

Il primo è la continuità non stop delle operazioni business: l'obiettivo è perseguito mediante funzioni che assicurano il recupero praticamente istantaneo delle applicazioni e dei dati, sia che risiedano on-premise che in un cloud ibrido.

Albert Zammar - Veeam

Il secondo è l'agilità nella trasformazione digitale dell'azienda: l'obiettivo è perseguito mediante funzioni che facilitano la

migrazione da una architettura on-premise ad una ibrida multi-cloud, nonché la gestione integrata e centralizzata del sistema che ne risulta.
Il terzo è l'analitica e la visibilità dell'IT: fornisce viste approfondite e dettagliate di cosa avviene nel sistema IT e dei suoi dati al fine da facilitarne la gestione, ottimizzare le prestazioni applicative e perseguire gli obiettivi di compliance normativa, come previsto anche dal GDPR.
I tre obiettivi sono perseguiti mediante una serie di componenti che coprono esigenze di "always-on" in ambienti Microsoft sia on-premise che nel Cloud, di disponibilità di dati e applicazioni in Cloud come ad esempio in AWS o Office 365, o di orchestrazione delle risorse nell'ambito di piani di Disaster Recovery.
Un elemento chiave per una trasformazione digitale efficace e sicura è poi Veeam Availability Orchestrator, che nell'ambito della Veeam Availability Platform ha l'obiettivo di permettere alle aziende di garantirsi la Business Continuity e la conformità ai requisiti di Disaster Recovery (DR).

Un marketplace per una sicurezza più rapida ed efficace

Per facilitare l'adozione di soluzioni di sicurezza e permettere alle aziende di individuare quella più adatta alle proprie esigenze, e di farlo senza doversi disperdere su più siti, CiberArk, società specializzata nelle soluzioni per la sicurezza nell'accesso degli utenti privilegiati, ha annunciato nel corso della recente RSA Conference 2018 svoltasi a San Francisco, la disponibilità del CyberArk Marketplace, un ampio portfolio di soluzioni allestito per rendere sicuro l'accesso degli utenti privilegiati a prescindere dal contesto di fruizione.
Dal punto di vista del suo utilizzo, CyberArk Marketplace ha l'obiettivo di costituire una piattaforma trusted a disposizione dei clienti che hanno la necessità di trovare rapidamente e installare soluzioni integrate con la soluzione CyberArk Privileged Account Security , disponibile da parte di CyberArk e dai suoi partner.
In pratica, le organizzazioni aziendali, ha osservato l'azienda, possono far leva sui prodotti disponibili nel marketplace per rendere più sicuro l'accesso ai dati sull'intero loro stack tecnologico, incluso la security, l'IT operation, il Cloud, DevOps o il software attinente i processi di automazione robotica.

Adam Bosnian - CyberArk

Nel costruire ed espandere progressivamente il marketplace, ha osservato l'azienda specializzata nella sicurezza degli utenti privilegiati, verrà mantenuto un approccio basato sul concetto di community, con il contributo da parte della CyberArk Alliance, dei partner e delle altre entità che collaborano con l'azienda al fine di migliorare la sicurezza e l'efficienza operativa dell'IT.
Il marketplace di CyberArk, ha commentato Adam Bosnian, executive vice president, global business development di CyberArk, riflette in pratica la filosofia che una effettiva sicurezza è una sorta di gioco di squadra e che è necessario disporre di un ambiente dinamico che indirizzi le priorità delle aziende per quanto concerne il risk management e le priorità connesse alla compliance, mettendoli in condizione di massimizzare gli esistenti investimenti in sicurezza ed estendere velocemente e facilmente quegli investimenti al fine di indirizzare nuove minacce e nuovi casi di utente man mano che vengono rivelati.

La fibra di Interoute serve il nuovo portale unificato del Vaticano

La rete in fibra ottica di Interoute ha permesso di accrescere le capacità e i servizi della digital transformation del Vaticano

Simone Bonannini - Interoute

Interoute, operatore proprietario di una piattaforma di servizi cloud globale, ha annunciato che la propria rete in fibra ottica supporta il lancio del nuovo portale online della Segreteria per la Comunicazione del Vaticano www.vaticannews.va. Il portale ingloba i tradizionali canali di comunicazione (radio, tv e casa editrice) in un punto di accesso unitario, per rispondere alle esigenze della missione della Chiesa a fronte delle sfide dell'ambiente digitale contemporaneo.

Il nuovo sito permetterà, questo l'obiettivo, di trovare facilmente le informazioni desiderate, mettendo a disposizione degli utenti contenuti multimediali, multi-device e multiculturali.

«Il ripensamento del sistema comunicativo della Santa Sede è passato attraverso un cambio tecnologico importante perché il mondo del web, quello del broadcasting e quello dell'editoria potessero fondersi in un'unica realtà. A fianco del portale avremo altri servizi e stiamo anche pensando ad altri progetti per distribuire contenuto multimediale di qualità direttamente agli utenti, come documentari o altre produzioni importanti. La rete in fibra di Interoute è la base tecnologica per abilitare questo progetto all'avanguardia", ha commentato Francesco Masci, a responsabile della Direzione Tecnologica della Segreteria per la comunicazione della Santa Sede.

L'accesso diretto alla dorsale digitale di Interoute, con la sua struttura in fibra ottica, è la chiave di colta del progetto, da qui anche il nome che è stato, "Backbone".

Il progetto ha visto una stretta collaborazione degli esperti del Vaticano e Interoute, al fine di trovare le soluzioni migliori anche in ambiti molto vincolanti. Il progetto, infatti, ha comportato anche la posa di cavi nel sito religioso, culturale, e artistico senza tema di smentita il più importante del mondo.

«Siamo stati onorati di mettere a disposizione tutta la nostra decennale esperienza. Interoute ha costruito l'infrastruttura di backbone che in Europa abilita la digital transformation di grandi organizzazioni con presenza globale. Grazie all'esperienza del nostro team tecnico, che ha cablato una delle reti più estese d'Europa, abbiamo maturato il know how e la competenza per affrontare questo progetto, unico nel suo genere, rispettando i tempi di consegna e i vincoli imposti dal patrimonio artistico culturale del sito», ha dichiarato Simone Bonannini, Vice President of Southern Europe, CEE e MEA di Interoute.

CLOUD SANDBOX PERMETTE UNA RAPIDA RISPOSTA ALLE MINACCE

Kaspersky Cloud Sandbox, attraverso una macchina virtuale, consente di testare manualmente e automaticamente nel cloud i file sospetti

Come conseguenza delle principali fughe di dati del 2017 che hanno visto sfruttare le vulnerabilità di software legittimi, la necessità di tecnologie avanzate di rilevamento non è mai stata così evidente. Per aiutare le imprese a migliorare le proprie procedure di indagine e risposta alle minacce complesse, Kaspersky Lab ha avviato un nuovo servizio chiamato Kaspersky Cloud Sandbox che, proprio perché basato sul cloud, ha l'obiettivo di fornire alle aziende l'opportunità di avvalersi delle sandbox senza dover supportare investimenti in hardware.

La soluzione è disponibile su abbonamento all'interno del Kaspersky Threat Intelligence Portal. In sostanza, Cloud Sandbox permette agli utenti di "far detonare" i file sospetti in un ambiente virtuale ricevendone un report sulle attività dei file, ed è stata progettata per migliorare l'efficienza dell'incident response e delle indagini forensi di sicurezza informatica senza rischi per i sistemi IT dell'azienda.

Il problema, evidenzia Kaspersky, è che per indurre i malware a rivelare il proprio potenziale nocivo, le tecnologie sandbox devono includere tecniche anti-evasione avanzate. Un programma dannoso, sviluppato per operare su un determinato ambiente software, non si eseguirà su una macchina virtuale "standard" e probabilmente si distruggerà senza lasciare tracce. Per evitarlo, Kaspersky Cloud Sandbox applica diverse tecniche di emulazione delle attività degli utenti – come il clic sul tasto Windows, lo scroll dei documenti e specifici processi di routine che possono indurre il malware a esporsi – di randomizzazione dei parametri dell'ambiente utente, e altre ancora.

Una volta che un campione di malware inizia a condurre le proprie attività distruttive, entra in gioco un'ulteriore tecnologia di Cloud Sandbox. Ad esempio, quando un documento Word inizia a comportarsi in modo sospetto come eseguire comandi Shell o installare payload, questi eventi vengono registrati nel logging di Cloud Security che dispone di funzionalità in grado di rilevare una vasta gamma di attività nocive, incluse registrazione e modifica di DLL e chiavi di registro, invio di richieste HTTP e DNS anomale, creazione, eliminazione e modifica di file.

Il cliente riceve quindi un report con grafici riassuntivi dei dati e screenshot.

«Kaspersky Cloud Sandbox è un servizio unico di analisi approfondita dei file, che consente ai ricercatori di sicurezza IT e ai team SOC ti ottenere informazioni importanti sul comportamento dei file senza rischi per l'infrastruttura IT», ha commentato il rilascio del nuovo servizio cloud Nikita Shvetsov, Chief Technology Officer di Kaspersky Lab.

MAIL E SOCIAL PROTETTI CON LA SICUREZZA PEOPLE-CENTRIC

Proofpoint ha annunciato nuove soluzioni per applicazioni cloud, email aziendale e social media che incrementano visibilità e protezione

Ryan Kalember - Proofpoint

Proofpoint ha annunciato la disponibilità di quattro nuove soluzioni di sicurezza people-centric pensate per aiutare le imprese a operare anche al di fuori del perimetro aziendale, ad esempio nel cloud.

Le soluzioni, ha spiegato l'azienda, hanno lo scopo di fornire una maggiore visibilità sul principale vettore di rischio - le persone - e comprendono Proofpoint Cloud App Security Broker (PCASB), 360 Degree Email Fraud Protection, Threat Response Auto-Pull (TRAP) Abuse Mailbox Monitoring e Executive and Location Threat Monitoring per i social media e i canali del dark web.

«I cybercriminali mirano sempre più spesso alle persone, non alle infrastrutture, e il passaggio al cloud cambia il modo in cui le organizzazioni devono proteggersi», ha commentato il rilascio dei prodotti Ryan Kalember, senior vice president Cybersecurity Strategy in Proofpoint. «L'annuncio odierno sottolinea il nostro continuo impegno volto a salvaguardare le imprese dalla minaccia più grande – le persone – difendendo, evitando e rispondendo agli attacchi in uno scenario in costante evoluzione. Investiamo il 20% del nostro fatturato in ricerca e sviluppo, una cifra ben al di sopra della media del settore e queste innovazioni ne sono il frutto».

Le soluzioni, che danno una protezione e una visibilità che si proietta oltre il tradizionale perimetro aziendale comprendono:

- Proofpoint Cloud App Security Broker (PCASB) permette ai team di sicurezza di adottare soluzioni cloud con fiducia. Protegge le organizzazioni da minacce avanzate, condivisione accidentale di dati sensibili e i rischi di compliance nel cloud..
- Proofpoint 360 Degree Email Fraud Protection protegge dipendenti, clienti e partner dalle frode via email. Potenziamento della soluzione Proofpoint Email Fraud Defense, la nuova funzionalità 360 Degree dà visibilità sulle minacce email – indipendentemente dalla tattica impiegata o dalla persona colpita.
- Proofpoint Threat Response, è una piattaforma di automazione e orchestrazione della sicurezza per garantire analisi e risposte rapide e automatiche per email che gli utenti segnalano come potenzialmente malevole.
- Proofpoint Executive and Location Threat Monitoring; fornisce una situational awareness ai team di sicurezza esplorando il mondo digitale, studiando milioni di pagine web e siti social ogni giorno.

CON SAP IL DIGITAL MANUFACTURING VA NEL CLOUD

Dall'esperienza nell'IIoT, nell'analisi predittiva e nella supply chain, è derivata la soluzione che consente alle aziende manifatturiere di implementare tecnologie di Industry 4.0 nel cloud

SAP SE ha annunciato il rilascio di SAP Digital Manufacturing Cloud, una sua nuova soluzione ideata per aiutare le aziende a ottimizzare le prestazioni, migliorare la qualità e l'efficienza della produzione e garantire maggior sicurezza per i lavoratori. Basandosi in particolare sull'esperienza nell'Industrial Internet of Things (IIoT), nell'analisi predittiva e nella supply chain, la soluzione si propone di consentire alle aziende manifatturiere di implementare tecnologie di Industry 4.0 nel cloud.

Peraltro, la nuova soluzione cloud estende e completa il portafoglio di produzione digitale di soluzioni on-premise di SAP ed è disponibile in diversi bundle per supportare aziende di varie dimensioni sia in ambito industria discreta che di processo, sia fornendo un aiuto ai differenti ruoli all'interno delle organizzazioni.

I clienti possono scegliere tra la soluzione SAP Digital Manufacturing Cloud for execution, che fornisce tutte le soluzioni manufacturing del portfolio cloud, o la soluzione SAP Digital Manufacturing Cloud for insights, focalizzata sulla gestione delle prestazioni e sulla qualità predittiva.

«Le aziende nell'era di Industry 4.0 richiedono soluzioni intelligenti, interconnesse e predittive», ha commentato Bernd Leukert, Member of the Executive Board of SAP SE, Products & Innovation. «Le nostre soluzioni per il mondo manufaturing in cloud aiutano i clienti a sfruttare l'Industrial Internet of Things connettendo macchinari persone e operazioni attraverso una supply chain digitale estesa e integrando direttamente la produzione con le operazioni di business».

La nuova offerta cloud include:

- SAP Digital Manufacturing Cloud for execution: destinata alle linee di produzione comprende funzionalità di personalizzazione industrializzata "lot-size-one" e di produzione senza carta. Integra i sistemi aziendali con le linee di produzione, consentendo la visibilità a livello di componenti e materiali per installazioni singole e globali.
- SAP Digital Manufacturing Cloud for insights: abilita la gestione delle prestazioni centralizzata e basata sui dati.
- Qualità predittiva: supporta nell'ottenere le visioni dettagliate necessarie per conformarsi alle specifiche dei processi e semplificare la gestione della qualità.
- Network di produzione: fornisce una piattaforma collaborativa basata su cloud integrata con le soluzioni SAP Ariba che collega i clienti con i manufacturing service provider, come i fornitori di servizi di stampa 3D e di stampa con computer numerical control fornitori di materiali, produttori di apparecchiature originali (OEM) e società di certificazione tecnica.

LA CHIAVE PER PROTEGGERSI DAGLI ATTACCHI DDOS È LA FLESSIBILITÀ

A10 Networks ha sviluppato una soluzione per garantire un IT "always-on" alle aziende che non possono permettersi un'interruzione dei propri servizi

Alberto Crivelli - A10 Networks

A10 Networks, azienda specializzata in Application Visibility Performance and Security, al fine di garantire un IT sempre attivo, ha sviluppato un portfolio di soluzioni basate sul software A10 DDoS Protection Cloud, il cui compito è di rilevare e mitigare gli attacchi denial of service distribuiti (DDoS).

A10 Networks, che ha una presenza globale con oltre 6.000 aziende clienti, è attiva anche in Italia con una base installata che comprende soprattutto società nelle aree Telco, PA ed Industry.

In particolare, l'offerta DDoS Protection Cloud permette alle organizzazioni che utilizzano il web per il business, di proteggersi dagli attacchi DDoS con soluzioni basate sia su componenti software che su appliance. Le soluzioni sono fruibili tramite la "no licensing policy", un approccio flessibile che prevede il solo prezzo per l'acquisizione iniziale della soluzione ed i canoni annuali di manutenzione ed aggiornamento, e permette al cliente di attivare funzionalità addizionali senza ulteriori investimenti.

«I nostri clienti sono molto soddisfatti della nostra proposta – ha sottolineato Alberto Crivelli, Country Manager di A10 Networks Italia -, la strategia di A10 Networks basata sulla "no licensing policy" permette ai clienti di adattare l'utilizzo delle apparecchiature alle esigenze dei business che spesso si modificano con il passare del tempo e l'evolvere delle architetture. Capita spesso infatti che apparati acquisiti per una specifica funzione vengano di seguito utilizzati in maniera molto differente da come si era immaginato al momento dell'acquisto».

Quello della protezione DDoS è un ambito della sicurezza ancora poco noto, rispetto ad altri ambiti e soluzioni, ed è di conseguenza anche la parte più scoperta e vulnerabile in azienda. Tradizionalmente le soluzioni atte a contrastare questi attacchi erano però rivolte soprattutto al mercato dei Carrier e delle maggiori imprese ed è questa limitazione che A10 Networks ha voluto rimuovere rendendola alla portata della media impresa italiana. «Gli attacchi DDoS sono imprevedibili e sempre più complessi e le aziende hanno bisogno di strumenti di difesa smart e scalabili, per poter adottare strategie di protezione dagli attacchi DDoS in continua evoluzione. Punto cardine della protezione è la visibilità, A10 networks propone per questo strumenti di analisi molto potenti al fine di automatizzare il più possibile la protezione e rendere visibili I tentativi di attacco», ha spiegato Crivelli. A10 Networks sta inoltre sviluppando la propria rete di partnership e la community a livello internazionale, ad oggi dispone di 40+ alliances di livello globale tra cui Verisign.

EQUINIX SUPPORTA IL SERVIZIO CLOUD PARTNER INTERCONNECT DI GOOGLE

La collaborazione di Equinix e Google dà alle aziende ampie possibilità di interconnessione su Google Cloud Platform

Equinix, azienda attiva nel settore delle interconnessioni di rete e dei data center, ha annunciato il supporto a Google Cloud Partner Interconnect, un nuovo servizio di Google Cloud che consente ai clienti di connettersi a Google Cloud Platform da qualsiasi luogo tramite i propri partner. Equinix ha anche annunciato l'espansione della connettività privata al servizio cloud Dedicated Interconnect di Google alle aree metropolitane di Stoccolma, Sydney e Monaco, portando così a 20 il numero totale di mercati in cui Google ha implementato il proprio servizio Dedicated Interconnect nei data center Equinix International Business Exchange.

Con l'aumento delle opzioni di accessibilità e connettività a Google Cloud Platform, Equinix si è proposta di consentire alle aziende di accrescere le proprie opportunità di interconnessione e di scalare le proprie attività digitali attraverso un data center dinamico e una piattaforma di interconnessione.

Il quanto al servizio Partner Interconnect, si tratta di un nuovo prodotto della famiglia Google Cloud Interconnect volto a dare l'opportunità ai clienti di implementare Google Cloud Platform abilitando la connettività tramite i canali partner, tra cui Equinix Cloud Exchange Fabric, una piattaforma on-demand che consente di connettersi a qualsiasi altro cliente da qualsiasi location Equinix.

In pratica, ha osservato la società, espande le opportunità di mercato per i clienti che cercano una connettività diretta a Google Cloud Platform. Oltre a sfruttare un modello di utilizzo on-demand, le aziende che implementano Partner Interconnect saranno anche in grado di scegliere tra una varietà di velocità di interfaccia sub-rate, da 50 Mbps a 10 Gbps.

Lo scorso settembre, Google aveva già annunciato Dedicated Interconnect, un servizio che fornisce una connettività a velocità più elevata e a costi inferiori rispetto alla VPN ed è una soluzione proposta per connettere i data center on-premise con il cloud. «Fornendo l'accesso ai servizi cloud Dedicated Interconnect e Partner Interconnect di Google ed espandendo queste offerte in più mercati in tutto il mondo, stiamo aiutando le aziende a sfruttare la rete di Google e ad accelerare le loro strategie di cloud ibrido a livello globale. Con maggiori opzioni di connettività e una maggiore accessibilità a Google Cloud, Equinix offre ai clienti la possibilità di fare le loro scelte per soddisfare le esigenze di interconnessione e creare facilmente il cloud che desiderano», ha commentato Brian Lillie, Chief Product Officer, Equinix.

SERVIZI GRATUITI METTONO AL SICURO CERTIFICATI DIGITALI E ASSET CLOUD

Qualys ha annunciato due servizi gratuiti per l'inventario e l'assessment dei certificati SSL/TLS esposti a Internet, e CloudView per l'inventario del cloud pubblico

Schermata di CloudView

Qualys, fornitore di soluzioni di sicurezza e compliance basate su cloud, ha annunciato due servizi gratuiti: CertView e CloudView, entrambi basati sulla Qualys Cloud Platform.

I due servizi hanno l'obiettivo di consentire alle aziende di migliorare la visibilità dell'IT e supportarle nel compilare su base continua l'inventario e la valutazione dei certificati digitali, dei workload e dell'infrastruttura cloud.

"CertView e CloudView estendono il campo di azione della Qualys Cloud Platform alle aziende di tutto il mondo, aiutandole a individuare e a monitorare i loro certificati digitali e a compilare un inventario completo delle risorse nel cloud pubblico. Queste funzionalità sono cruciali per aiutare i CIO e i CISO ad adottare strategie più proattive per proteggere i dati critici nella delicata fase di trasferimento verso il cloud", ha commentato l'annuncio Philippe Courtot, Presidente e CEO di Qualys.

Nello specifico dei servizi, CertView consente di compilare un inventario, di valutare i certificati e le relative configurazioni SSL/TLS sottostanti e di rilevarne le vulnerabilità su tutte le risorse che interagiscono con l'esterno, nell'ottica di prevenire inattività ed interruzioni, mitigando i rischi associati all'uso di certificati e configurazioni SSL/TLS scaduti o vulnerabili. Tra le funzionalità comprende l'Individuazione e l'inventario dei certificati, rating delle configurazioni TLS, monitoraggio continuo, report e dashboard

CloudView permette invece di migliorare la visibilità topologica dell'IT e ottenere informazioni sullo stato di sicurezza e conformità della loro propriainfrastruttura di cloud pubblico per i principali provider come Amazon Web Services (AWS), Microsoft Azure e Google Cloud. Tra le funzionalità comprende individuazione e inventario delle risorse, ricerche per attributi e rilevazione dei bucket di archiviazione non sicuri, le istanze non governate e quelle programmate per essere cancellate. Il servizio è offerto gratuitamente per un massimo di tre account per ogni piattaforma di cloud pubblico.

E anche possibile aggiornare la sottoscrizione al servizio aggiungendo le app Qualys Cloud Inventory (CI) e Cloud Security Assessment (CSA) che includono il monitoraggio continuo della sicurezza, individuazione delle cause degli incidenti e protezione .

RICOH AMPLIA L'OFFERTA DI SERVIZI CLOUD PER LA DIGITAL TRANSFORMATION

I nuovi servizi IT rispondono alle esigenze del mercato in ambito Workplace & Mobility, Data Center & Infrastructure, Information Management & Business Intelligence

Ricoh ha ampliato la propria offerta IT Services per l'area EMEA con nuovi servizi e soluzioni a supporto delle aziende che operano sia a livello nazionale che internazionale. Il nuovo portfolio copre tre aspetti chiave della trasformazione digitale:

- Workplace & Mobility: comprende soluzioni volte al miglioramento della produttività e della flessibilità aziendale.
- Data Center & Infrastructure: abilita la trasformazione e gestione delle infrastrutture IT critiche.
- Information Management & Business Intelligence: è relativo all'analisi dei dati al fine di migliorare le decisioni.

Oltre alla tradizionale infrastruttura on-premise, la nuova proposta include anche l'opzione Ricoh Cloud Service Management pensata per supportare le aziende con soluzioni di cloud pubblico e ibrido. Si tratta di servizi che si basano su tecnologie di nuova generazione caratterizzate, ha evidenziato Ricoh, da elevati standard di sicurezza.

«L'offerta IT Services di Ricoh si fonda sull'evoluzione delle esigenze del mercato. Ciò che distingue la proposta Ricoh da quella della concorrenza è la nostra capacità di supportare le aziende con servizi globali, mantenendo però allo stesso tempo flessibilità e agilità grazie a strutture locali. La nostra offerta per il Digital Workplace risponde alla necessità delle imprese di lavorare in modo smart e di aumentare l'efficienza. Dalla piccola azienda alla multinazionale, gli IT Services di Ricoh sono sviluppati per aiutare le organizzazioni ad utilizzare al meglio le risorse a loro disposizione», ha commentato Alberto Mariani, Director of IT Services EMEA, Ricoh Europe.

Peraltro, va osservato che il mercato degli IT Services non è nuovo per Ricoh perché da diversi anni svolge attività e servizi connessi alla trasformazione e alla gestione di ambienti di lavoro e delle infrastrutture IT. E' su questa basa che cala l'ampliamento dell'offerta che ha annunciato, vista come un passo successivo della sua evoluzione volta a fornire soluzioni e servizi per rendere il business dei clienti più rapido, smart e sicuro.
inaugurazione

Un esempio dell'impegno che profonde per supportare i clienti e per aumentare l'efficacia dei servizi Data Centre & Infrastructure, è dato dalla inaugurazione avvenuta lo scorso ottobre di un Service Operation Centre a Varsavia con l'obiettivo di offrire supporto e servizi innovativi, tra cui monitoraggio, gestione e sicurezza per proteggere i sistemi dei clienti h24.

IL VOIP E LA UC NEL CLOUD RICHIEDONO PERSONALE

Per l'ICT aziendale è in corso una migrazione sul cloud che coinvolge non solo l'office automation ma anche i sistemi UCC. 3CX mette in guardia dai problemi organizzativi

La soluzione di video comunicazione 3CX Webmeeting

Secondo le analisi effettuate da Namertes Research, negli Stati Uniti il passaggio al cloud coinvolgerebbe il 44% circa delle aziende con un tasso di crescita del 20% previsto entro fine 2018. Sebbene in Italia i dati si attestino su valori assoluti inferiori del 30% circa rispetto al tasso registrato oltreoceano, la percentuale delle aziende che migra al cloud risulta addirittura maggiore.

Un dato che si spiega con il fatto che la banda larga e ultralarga, pur scontando una ritardata diffusione nel nostro Paese, negli ultimi mesi ha registrato un incremento superiore alla media.

Ciò comporterà di conseguenza una maggiore diffusione e fruibilità dei servizi di comunicazione unificata in cloud, con particolare riferimento ai servizi di video conferenza web.

Sorprendentemente, le aziende che passano al Cloud vedono però aumenti nel proprio organico IT piuttosto che diminuzioni, sempre secondo i dati di Nemertes.

Le organizzazioni che si spostano verso il cloud hanno visto, al termine del processo, una riduzione degli impiegati dedicati a tempo pieno all'assistenza tecnica, riduzioni tuttavia più che compensate dagli aumenti del personale (+6%) responsabile della gestione delle relazioni con i fornitori di tecnologia, della formazione tecnica e dello sviluppo ed integrazione nell'ambito del comparto IT.

La più vasta area di crescita del personale riguarda i ruoli di promozione, formazione e responsabilizzazione nell'utilizzo dei nuovi e innovativi strumenti di produttività offerti dalla migrazione verso il cloud, specie nell'ambito delle telecomunicazioni. Il motivo, spiega 3CX, lo si trova nel fatto che le soluzioni UC di nuova generazione cambiano le metriche di successo delle aziende determinando un aumento della produttività e del tasso di ritorno degli investimenti.

Quello che si evince è che le aziende pensano sempre più al personale IT non come centro di costo, ma come mezzo per raggiungere gli obiettivi aziendali. Il personale IT, esterno o interno, deve essere però in grado di garantire che il processo in atto consenta di adottare nuove funzionalità che aggiungano valore alla conduzione delle attività quotidiane.

La buona riuscita di una strategia di digitalizzazione e transizione al cloud dipende quindi, in primo luogo, dalla volontà e dalla consapevolezza della dirigenza di voler migliorare o addirittura rivoluzionare i propri processi comunicativi e produttivi.

La seconda variabile è legata alle competenze dei consulenti IT. Per le PMI il ruolo dell'UC Manager sarà, quasi sicuramente, esternalizzato nella fase iniziale. Solo successivamente sarà possibile trasmettere tali competenze direttamente degli impiegati interni.

SEMPRE PIÙ "ALWAYS-ON" PER IL MONDO ENTERPRISE

Albert Zammar - Veeam Software

L'Hyper-Availability Platform di Veeam ha registrato un'accelerazione, con oltre 150.000 download di Veeam Availability Suite Update 3 dal suo lancio. Molto positivi i risultati finanziari

Veeam Software, fornitore di soluzioni di Intelligent Data Management per la Hyper-Available Enterprise, ha annunciato i risultati finanziari del primo trimestre 2018.

Nel trentanovesimo trimestre consecutivo di crescita delle vendite, Veeam, guidata in Italia da Albert Zammar, Regional Vice President della Southern EMEA Region di Veeam, ha registrato una crescita annuale degli ordini pari al 21%, con 12.000 nuovi clienti che hanno portato la base totale a toccare le 294.000 unità, e ad una crescit annua degli ordini ricevuti da clienti del settore Enterprise del 58%.

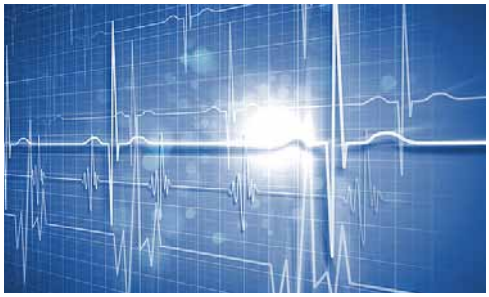
«La nostra missione è di essere il fornitore di riferimento di soluzioni per la gestione intelligente dei dati, con l'obiettivo di permettere alle aziende clienti di operare con successo in un mondo in cui è indispensabile la Hyper-Availability dei dati», ha commentato Peter McKay, Co-CEO e President di Veeam. «Oggi, grazie alla più completa piattaforma di Hyper-Availability per la protezione di qualsiasi dato, applicazione o architettura cloud, affianchiamo circa 300.000 clienti nel passaggio dal vecchio mondo– fatto di backup sporadici e recuperi rischiosi dei dati – ad una nuova era in cui i dati sono disponibili in sistemi intelligenti e automatizzati che si estendono in tutta l'azienda».

I risultati ottenuti, ha evidenziato la società, sono la conseguenza di investimenti significativi realizzati nei team di progettazione e sviluppo, l'estensione delle attività di marketing e branding, lo studio di nuovi programmi ed iniziative per supportare i nostri partner e, non ultimo, il focus sul mercato delle grandi aziende.

Un ruolo importante nella strategia di mercato di Veeam lo ricoprono le alleanze strategiche. Ad esempio, le opportunità congiunte di Veeam con HPE sono cresciute del 148 percento a seguito della partecipazione di Veeam al programma HPE Complete, che consente ai clienti di acquistare le soluzioni Veeam e HPE direttamente da HPE e dai suoi rivenditori. Per quanto concerne la sua alleanza con Cisco, nel primo trimestre, a seguito della disponibilità delle soluzioni Veeam sul listino globale Cisco, le trattative Veeam e Cisco sono cresciute del 299 percento su base trimestrale. Non ultimo, va considerato che Veeam è anche stata inclusa nel listino globale NetApp , cosa che prevedibilmente contribuirà ad aumenterà ulteriormente la presenza della società nel mercato delle grandi aziende.

Sul piano del portfolio e dei servizi offerti, un contributo significativo alla crescita della società è dovuto al programma Veeam Cloud & Service Provider (VCSP), che continua la sua crescita e ha registrato un incremento annuale del 38%.

A RISCHIO ATTACCO GLI OSPEDALI NEL MONDO



Una ricerca Trend Micro ha esaminato le vulnerabilità delle strutture sanitarie e ne evidenzia le lacune nella sicurezza. Cloud e dispositivi i punti critici

La tecnologia è il cuore pulsante di ogni struttura medica moderna. I progressi in campo cloud, IoT e digitale aiutano le organizzazioni sanitarie a migliorare enormemente la qualità dei servizi offerti ai pazienti e i dati sanitari sono la spina dorsale di protocolli di cura sempre più complessi e in evoluzione. Ma se i pazienti sono in buone mani i loro dati, anche riservati, sembrano esserlo decisamente di meno.

Trend Micro, insieme a HITRUST, ha esaminato il settore delle strutture sanitarie nel suo ultimo report "Securing Connected Hospitals". Il dato più allarmante è che sono almeno 80.000 i sistemi a rischio violazione, negli ospedali di tutto il mondo. Inoltre, all'interno delle organizzazioni è stato riscontrato un preoccupante divario tra la percezione dei rischi e la realtà.

I responsabili IT delle strutture mediche devono infatti comprendere meglio e mitigare le nuove minacce cyber. La ricerca svela che i sistemi a rischio violazione espongono gli ospedali ad attacchi DDoS, malware e violazioni di dati.

Gli attacchi DDoS sono la minaccia più seria, seguita dai ransomware. Gli attaccanti che vanno tenuti in maggior considerazione sono i Cyber Criminali organizzati, poiché i dati medici hanno un grande valore all'interno dei mercati underground e per la loro natura privata e sensibile possono essere utilizzati anche per ricatti e frodi, oltre che per la compilazione e vendita di database.

Un'area importante che le organizzazioni sanitarie dovrebbero proteggere, suggerisce Trend Micro, è anche quella della supply chain. La maggior parte delle violazioni sono infatti associate a fornitori e partner. Basti pensare a tutti i fornitori di servizi cloud o IT, ma anche a quelli di apparati medicali e dispositivi mobili. Molto spesso infatti, sono i dispositivi elettromedicali, quelli meno protetti, a essere sfruttati per infiltrarsi nella rete.

Che fare per migliorare la sicurezza? Trend Micro suggerisce alcune regole:

- Identificare e rispondere velocemente alle violazioni di dati
- Contenere le violazioni alla sicurezza e fermare la perdita di dati sensibili
- Prevenire gli attacchi, mettendo al sicuro tutti i dispositivi che possono essere sfruttati come punti di ingresso
- Fare tesoro delle lezioni imparate, per rafforzare le difese e impedire il ripetersi degli incidenti

Da un punto di vista tecnologico, bisogna applicare tecnologie di crittografia per proteggere i dati sensibili, vulnerability scanning, segmentazione delle reti, patch management, IPS/IDS, rilevamento delle violazioni e soluzioni anti-malware.