Cloud & Business

n.80
Aprile 2019

LA RIVISTA PER IL MANAGER CHE DEVE OTTIMIZZARE COSTI E PROCESSI

IN QUESTO NUMERO>>>

COVER STORY

LE NUOVE FRONTIERE DELL'IT CON IL CLOUD IBRIDO

di Giuseppe Saccardi

Le soluzioni Nutanix per il cloud ibrido facilitano il passaggio al cloud, rimuovono gli ostacoli per la gestione, abilitano la mobilità e migliorano i costi aziendali

Alberto Filisetti - Country manager di Nutanix Italia

Reportec Cloud&Business - Numero 80 - Aprile 2019 - 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

Che lo si ami o lo si detesti, il cloud sta avendo un grande impatto sull'IT in azienda. Se questa è la sensazione non ci si è però resi pienamente conto di quanto fosse forte il suo effetto fino a quando non si sono analizzati i risultati di una ricerca su ciò che sta accadendo nel mercato dell'enterprise cloud.

Condotto da Vanson Bourne per conto di Nutanix, lo studio ha raccolto dati molto interessanti da circa 2.300 aziende di tutto il mondo. I risultati sono espliciti: oltre un terzo (36%) dei workload aziendali è già in cloud e la maggior parte delle aziende intervistate si aspetta che questo dato cresca rapidamente per arrivare ad oltre la metà dei workload in cloud entro l'ormai prossimo 2020.

Ma non solo. Le aziende cercano sempre più spesso di distribuire le applicazioni tramite un mix di cloud pubblico e privato.

Circa il 18% degli intervistati ha già adottato questo tipo di approccio misto, percentuale che tenderà a incrementare più del doppio nel corso dei prossimi due anni. L'approccio ibrido diventerà quindi, con tutta probabilità, il modello di implementazione IT di riferimento.

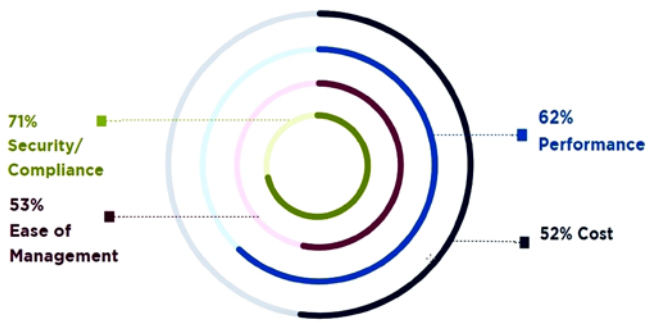
L'approccio ragionato al cloud ibrido

Le ragioni del passaggio a un mix di cloud sono chiare. In sostanza, le aziende stanno sperimentando i benefici del cloud pubblico (scalabilità on-demand, risparmio grazie a un approccio pay per use e così via) e, allo stesso tempo, sono consapevoli del fatto che non tutti i cloud sono uguali. Infatti, allocare tutte le applicazioni in un unico posto potrebbe essere controproducente.

La vecchia trappola del così detto vendor lock-in, a tutta evidenza, è ancora lì che attende i più incauti e questo è il motivo per cui in tanti adottano un approccio all'IT molto più incentrato sulle applicazioni.

Di conseguenza, scelgono il luogo migliore per ogni applicazione che distribuiscono, sia esso un cloud pubblico o privato, invece che uniformarsi a un unico cloud e adattarvi le applicazioni.

Molti vorrebbero anche poter spostare i carichi di lavoro tra i cloud per ragioni sia tecniche che finanziarie, ecco perché gli intervistati da Vanson Bourne, assegnano alla mobilità una priorità maggiore rispetto ai costi e alle problematiche di sicurezza.



I fattori che determinano dove far girare le applicazioni (Vanson Bourne)

Come rendere efficiente il modello ibrido

Purtroppo, evidenzia **Alberto Filisetti**, Country Manager di Nutanix Italia, si è ben lontani dall'essere in grado di trasformare l'aspirazione ad una libera circolazione delle applicazioni. Innanzitutto perché non tutti i cloud sono uguali, a cui si aggiunge un'altra constatazione emersa dallo studio condotto da Vanson Bourne: una reale mancanza di personale con le competenze necessarie per concretizzare tale ambizione.

Sebbene poi tecnologie come container, microservizi e API contribuiscano a rendere le applicazioni molto più portabili, le funzionalità di implementazione, monitoraggio e gestione non si sono evolute di pari passo, finendo con l'enfatizzare la carenza di competenze.

Il risultato finale è una mancanza di visibilità nel momento in cui le applicazioni vengono distri-

buite su un mix ibrido di cloud. E se a tale mix si aggiunge un'infrastruttura tradizionale on-premise, diventa ancora più difficile avere visibilità su cosa stia succedendo non solo in termini di prestazioni e disponibilità, ma anche di sicurezza e conformità.
Detto altrimenti, se non è possibile vedere un'applicazione su ogni cloud che "tocca", non è possibile gestirla o correggerla quando qualcosa va storto. Inoltre, diventa molto più difficile garantirne conformità, la disponibilità e, mancando la visibilità dei diversi cloud, non è possibile automatizzare i processi tra di essi.
Gli strumenti per la gestione ibrida del cloud
E' evidente che qualcosa andava fatto e, in questo senso, ci sono tecnologie e soluzioni in fase di sviluppo in grado di fornire la auspicata visibilità tra i cloud. Tre funzionalità, osserva Filisetti, sono particolarmente utili:

- Strumenti di analisi avanzata in grado di comprendere le peculiarità tecniche, finanziarie e di governance dei cloud pubblici per permettere ai team IT di scegliere la "sistemazione" migliore per le proprie applicazioni. Sono strumenti che possono anche indicare ai manager che tipo di investimenti hanno fatto, a che punto sono e come stanno performando rispetto a metriche concordate che possono poi orchestrare la migrazione verso un nuovo cloud o un'istanza di prodotto in base alle esigenze di business.
- Servizi di disaster recovery (DR) in cloud per proteggere le applicazioni e i dati aziendali critici. Identificato da Gartner come uno dei requisiti IT "tecnologicamente più noiosi", il DR tra cloud è sempre più complesso ma, se eseguito correttamente, ha il potenziale per risolvere tutta una serie di problemi di disponibilità.
- Strumenti e tecnologie di rete cross-cloud in grado di gestire la connessione tra applicazioni attraverso cloud, istanze di servizi e prodotti di vendor diversi, identificare colli di bottiglia e potenziali vulnerabilità e avviare iniziative correttive.

«La distribuzione di questi e altri strumenti di gestione del cloud ibrido sarà tutt'altro che semplice e richiederà una maggiore cooperazione tra i vendor cloud e i service provider. Tuttavia, a fronte di un crescente numero di aziende che sta passando a un modello ibrido, è nell'interesse di tutti lavorare in sinergia. E' giunto il momento di unificare i cloud e fornire la visibilità, le tecnologie e gli strumenti necessari per sfruttare al meglio questa interessante modalità di fornire e gestire l'IT enterprise» ha osservato Filisetti.

Cloud ibrido e l'impatto sui servizi finanziari

Un caso particolare è costituito dal settore del Finance, abituato storicamente a basare il proprio IT su data center e reti di proprietà.
Nella ricerca "Enterprise Cloud Index" di Nutanix, volta a capire la propensione e l'attitudine verso il cloud per i servizi finanziari, sono stati valutati i piani specifici di adozione di cloud privati, ibridi e pubblici da parte del mercato finance.
Secondo lo studio, il settore finanziario supera altri settori nell'adozione del cloud ibrido con una penetrazione attuale del 21% rispetto alla media globale del 18,5%.
Il motivo risiede nel fatto che le società di servizi finanziari si trovano ad affrontare sfide importanti a causa dell'esigenza di snellire le IT operations e allo stesso tempo offrire un'esperienza diversificata ai propri clienti, sfruttando le nuove tecnologie come ad esempio la blockchain.
Questa rivoluzione, definibile come FinTech, combinata ai crescenti oneri di conformità normativa, privacy dei dati e problematiche di sicurezza, sta spingendo i CIO a trasformare radicalmente le fondamenta tecnologiche dei propri

Istituti.
Dai risultati dell'indagine emerge, inoltre, che gran parte delle organizzazioni finanziarie sta ancora affrontando con fatica il processo di modernizzazione di architetture e processi IT ormai obsoleti, con una conseguente inefficacia operativa e una potenziale vulnerabilità nel subire violazioni dei dati.
Il report evidenzia, infatti, che i servizi finanziari si appoggiano a data center più tradizionali rispetto ad altri settori, con una penetrazione del 46%.
In sostanza, nonostante la loro evoluzione sul fronte del cloud ibrido, le organizzazioni finanziarie hanno livelli di utilizzo del cloud privato inferiori a qualsiasi altro settore, con una penetrazione del 29% rispetto alla media del 33%.
Come e più di altri settori, anche quello dei servizi finanziari ritiene la sicurezza e la conformità elementi chiave nel valutare dove eseguire i carichi di lavoro. Ma non è solo questione di riorganizzazione dei data center esistenti. Altri punti sono emersi di interesse per il Finance. In particolare:

- La mobilità delle applicazioni tra gli ambienti cloud, con la capacità di spostare app e carichi di lavoro da un'infrastruttura cloud privata a una pubblica e viceversa, in base al tipo di carico di lavoro o all'esigenza del business, beneficiando al tempo stesso di gestione e operations unificate. Significativo è che ben il 63% degli intervistati del settore finanziario considera "essenziale" la mobilità delle applicazioni tra gli ambienti cloud.
- Miglior controllo delle spese nel cloud ibrido, derivante dalla possibilità di avere sotto controllo la propria spesa IT. In generale, le organizzazioni che utilizzano il cloud pubblico gli dedicano il 26% del loro budget IT annuale, percentuale che si prevede salga al 35% nel giro di due anni. Già oggi, peraltro, oltre un terzo delle aziende (36%) che utilizza il cloud pubblico ha dichiarato di sforare il budget assegnato e in questo il finance non è molto diverso, con il 33% degli intervistati che ha ammesso di aver superato il budget a disposizione.
- La carenza di competenze costituisce una barriera all'adozione del cloud ibrido. Sebbene l'88% degli intervistati abbia dichiarato di aspettarsi un impatto positivo sul proprio business dall'utilizzo del cloud ibrido, le competenze in materia sono alquanto scarse nelle aziende IT, con un livello di inadeguatezza al secondo posto solo dopo Intelligenza Artificiale e Machine Learning (AI/ML).
-

La fiducia complessiva di un settore sempre molto attento ma critico nei confronti dei cambiamenti è comunque elevata. Il 91% delle società di servizi finanziari intervistate ha dichiarato che il cloud ibrido è il modello IT ideale. Questa fiducia nel cloud e il fatto che il settore abbia un livello di adozione del cloud ibrido superiore rispetto agli altri settori, è probabilmente dovuto alla riconosciuta necessità di un processo di trasformazione digitale.

La situazione del cloud in Italia

Se quella descritta è la situazione emersa in EMEA su un campione di 900 aziende in 9 nazioni, come si presenta il cloud in Italia? Tutto sommato mostra un concreto dinamismo in quanto l'Italia ha superato la media su un certo numero di punti, in particolare per quanto riguarda l'ubicazione della maggior parte dei carichi di lavoro, che sono oggi molto inferiori nei data center tradizionali rispetto alla maggior parte degli altri Paesi e molto di più in cloud privati e ibridi.
Rispetto ai suoi omologhi a livello globale e regionale in EMEA, l'Italia gestisce attualmente un numero significativamente inferiore di carichi di lavoro nei data center tradizionali (24%), signifi-

cativamente maggiore nei cloud privati (49%) e ibridi (24%), e notevolmente inferiore in molteplici cloud pubblici (3%)..

Se poi le aziende italiane seguiranno i piani indicati, il loro utilizzo dei data center tradizionali scenderà ben al di sotto delle medie, mentre il loro utilizzo di servizi di cloud ibrido, privato e pubblici supererà moderatamente le medie.

Dall'analisi emerge poi che si assisterà ad un marcato spostamento dell'Italia dai tradizionali data center in 12 - 24 mesi, quando l'utilizzo diminuirà di tre volte. I cloud ibridi e l'utilizzo di più cloud pubblici prenderanno il sopravvento, dato che l'uso del cloud ibrido in Italia raddoppierà e l'utilizzo del multicloud aumenterà più di sette volte nello stesso periodo. Questo a scapito del ricorso al cloud privato e di un singolo cloud, che diminuirà della metà o più.

Enterprise Cloud OS, la piattaforma Nutanix per il multicloud

L'esigenza di ecosistemi per il cloud ibrido

La complessità nell'approntare una soluzione ibrida che soddisfi le varie esigenze, dalle economiche alle applicative, non può che essere affrontata con un forte connubio, osserva Filisetti, tra aziende fornitrici di soluzioni cloud.

Un esempio è quello tra Nutanix e Hewlett Packard Enterprise (HPE), che hanno dato il via a una collaborazione globale volta a fornire una soluzione integrata di cloud ibrido as a Service (aaS).

La soluzione si basa sul software Nutanix Enterprise Cloud OS e il suo hypervisor AHV integrato e gratuito, reso disponibile tramite HPE GreenLake.

L'approccio permette alle aziende di poter disporre di un cloud ibrido che può essere gestito in toto da HPE, ridurre in modo significativo il TCO e assicurare un time-to-value più rapido.

L'operazione trae la sua genesi, ha osservato Filisetti, dalla considerazione che le aziende subiscono una pressione costante per innovare e accelerare il processo di trasformazione digitale. Tuttavia, gli approcci tradizionali in atto relativi all'IT ibrido presentano molte sfide, tra cui sistemi complessi che richiedono personale numeroso per gestire le IT operations, aumento dei costi operativi e delle licenze software, oltre alle preoccupazioni relative al vendor lock-in. Il risultato è mancanza di flessibilità in un mondo che richiede invece ampia scelta e agilità nonché un forte dinamismo.

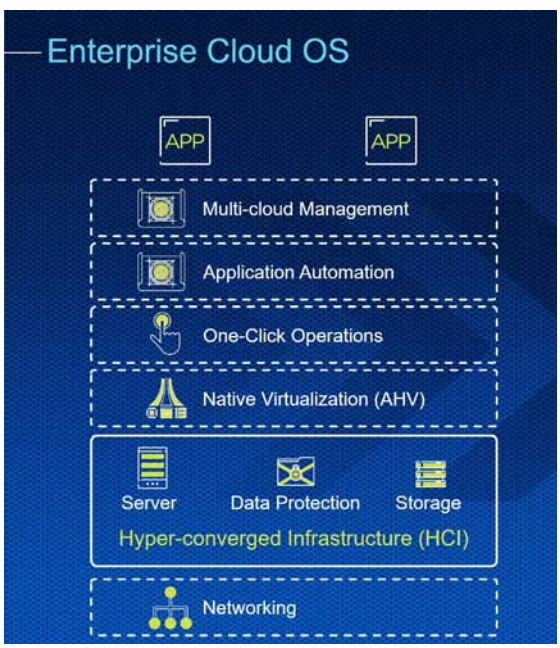
La partnership tra Nutanix e HPE si propone di rispondere a tali sfide e fornire un'alternativa interessante e funzionale atta a ridurre i costi e la complessità.

Nel suo insieme la proposta combinata ha l'obiettivo primario di fornire un'infrastruttura cloud ibrida del tutto gestita, resa disponibile in modalità "as a Service" e distribuita nei data center dei clienti o in strutture coabitative.

Non ultimo, osserva l'azienda, la combinazione di GreenLake con il software Nutanix Enterprise Cloud OS si prospetta ideale per le aziende che desiderano utilizzare la soluzione Nutanix, in-

clusa la sua tecnologia hypervisor AHV, per supportare carichi di lavoro mission-critical e applicazioni big data, carichi di lavoro virtualizzati di primo livello quali SAP, Oracle e Microsoft, oltre al supporto per applicazioni big data virtualizzate, come Splunk e Hadoop. Tra i benefici:

- Riduzione dei costi delle operations, delle spese in conto capitale e dei costi per l'assistenza e i servizi professionali: In base a una ricerca IDC commissionata da Nutanix sul software per l'iperconvergenza dell'azienda, i clienti beneficiano di una riduzione del costo delle operations stimabile nel 60% in 5 anni.
- Innovazione e time-to-value rapido: passando a un modello aaS per l'IT, viene abilitata una produttività superiore, diminuito l'onere dell'assistenza sul personale delle IT operations e ridotto fortemente il tempo necessario per distribuire i progetti IT.
- Scelta e semplicità: è possibile far leva su un hypervisor integrato e gratuito tramite un'offerta aaS, e sfruttare la semplicità d'uso "single-click" di Nutanix per distribuire e scalare carichi di lavoro virtualizzati. La tecnologia Nutanix, osserva Filisetti, può ridurre del 61% il tempo che il personale IT dedica alla distribuzione, gestione e supporto rispetto all'infrastruttura tradizionale, permettendo la distribuzione dei servizi HPE GreenLake in modo più rapido ed efficiente.



Lo stack Enterprise Cloud OS di Nutanix

Va poi osservato che HPE GreenLake è una soluzione aaS per l'IT on-premise di ultimissima generazione che può essere fruita con modalità di pagamento variabili in funzione dell'effettivo utilizzo misurato del carico di lavoro o delle risorse, in modo scalabile rispetto alle richieste di capacità dei clienti, e con gestione e supporto di livello enterprise.

Il parere degli analisti

La corrispondenza dell'approccio Nutanix alle esigenze delle aziende ha trovato riscontro nelle valutazioni degli analisti.

La società è stata posizionata da Gartner tra i Leader nel Magic Quadrant per le infrastrutture iperconvergenti del mese di novembre 2018.

Nutanix ritiene che il proprio posizionamento come Leader per la seconda volta consecutiva sia una chiara conferma della sua continua posizione di rilievo nel mercato e della vision nel fornire una reale esperienza di cloud ibrido, volta a consentire ai team IT di fornire applicazioni su più piattaforme senza problemi.

«Oggi, le aziende hanno bisogno di un ambiente cloud realmente ibrido e iperconvergente che sia invisibile all'organizzazione ma che offra un'esperienza fluida tra cloud pubblici e privati. Con il software Nutanix Enterprise Cloud OS, i clienti possono concretizzare i benefici di semplicità, agilità e consumo frazionato dell'IT offerti dal cloud pubblico, con il controllo e la sicurezza necessari nel data center aziendale», ha commentato Filisetti.

NON RALLENTANO LE MINACCE DEGLI HACKER PER L'IOT

Preoccupanti i dati di un report di F-Secure che rivela un aumento di attacchi e minacce che prendano di mira dispositivi IoT

L'esplosione attesa e in parte in atto dell'internet of things si è dimostrata controversa a causa delle misure di sicurezza insufficienti in molti di questi dispositivi connessi a internet.
In proposito una conferma dell'assunto è offerta da un report del fornitore di cyber security F-Secure, che evidenzia che le minacce e il numero di attacchi continuano a crescere, pur basandosi su punti deboli della sicurezza già noti, come software non aggiornati e password deboli.
Il report, che usa dati raccolti e analizzati dai Laboratori di F-Secure, sottolinea che le minacce che prendono di mira i dispositivi connessi a Internet stanno iniziando a moltiplicarsi più rapidamente che in passato.
Il numero di minacce IoT osservato è pressoché raddoppiato nel corso dello scorso anno, passando dal 19 precedente a 38. Per fortuna, si fa per dire, ma mai contare troppo su di essa, molte di queste minacce usano ancora tecniche conosciute e prevedibili per compromettere i dispositivi.
Le minacce che prendono di mira credenziali deboli o quelle predefinite fornite dal produttore, oppure le vulnerabilità non risolte, o tutte queste insieme, hanno costituito l'87% delle minacce osservate.
Tom Gaffney, F-Secure Operator Consultant ha dichiarato in proposito che i maggiori produttori di dispositivi IoT o ad essi assimilabili stanno prestando più attenzione alla sicurezza che non in passato, ma c'è un gran numero di dispositivi di numerosi produttori che non offrono molto in termini di sicurezza e privacy agli utenti finali.
"I grandi come Google e Amazon hanno fatto passi da gigante nei loro prodotti per la smart home grazie all'enorme sostegno di hacker etici come il nostro Mark Barnes, che ha eseguito il primo proof of concept per l'hacking di Echo nel 2017," ha spiegato Gaffney. "Ma per anni i produttori hanno rilasciato sul mercato prodotti senza pensare molto alla sicurezza, quindi molti dispositivi 'smart' in circolazione sono vulnerabili ad attacchi relativamente semplici."
Le minacce IoT sono state riscontrate raramente prima del 2014, si spiega nel report. Ma ciò è cambiato con il rilascio del codice sorgente per Gafgyt, una minaccia che ha preso di mira una varietà di dispositivi IoT, inclusi i dispositivi BusyBox, le telecamere a circuito chiuso (CCTV) e molti registratori video digitali (DVR).
Nell'Ottobre 2016, Mirai, che è stato sviluppato dal codice di Gafgyt, è diventato il primo malware IoT a raggiungere notorietà a livello globale quando la sua massiccia botnet è stata utilizzata per lanciare uno dei più grandi attacchi denial-

of-service distribuiti nella storia.
Il codice di Mirai è pubblico "per scopi di Ricerca/Sviluppo IoC" dal 2016. Originariamente, utilizzava 61 combinazioni univoche di credenziali utilizzate per le infezioni.
Nel giro di tre mesi, quel numero era proliferato a quasi i 500 ed è prevalente come famiglia di malware. Circa il 59% del traffico di attacco rilevato dai server honeypot di F-Secure nel 2018 ha preso di mira le porte Telnet esposte, con tentativi di Mirai di diffondersi.
Secondo **Jarno Niemela**, F-Secure Labs Principal Researcher, la causa principale di molti problemi IoT inizia con le supply chain dei produttori.
«La maggior parte dei vendor di dispositivi rilasciano kit di sviluppo software per i chipset che utilizzano nelle loro smart camera, smart appliance e altri dispositivi IoT. Ecco da dove vengono le vulnerabilità e altri problemi» spiega Niemela. «I produttori di dispositivi devono iniziare a chiedere di più in termini di sicurezza da questi fornitori e anche essere pronti a rilasciare aggiornamenti e patch non appena disponibili».

RETE PIÙ SICURA E DANNI DIMOSTRABILI CON LA NETWORK FORENSIC

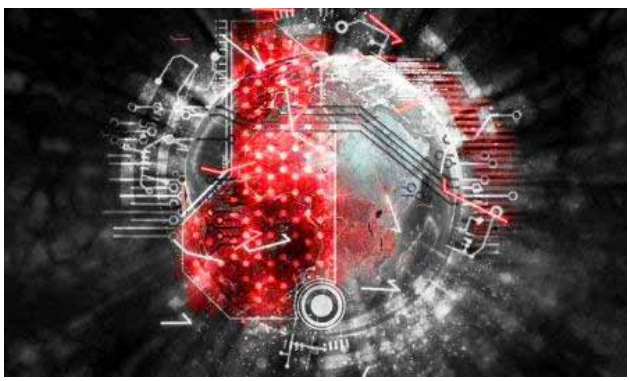
La network forensic assicura numerosi vantaggi, funzionali ed economici. Li illustra Gabriele Zanoni, Senior Systems Engineer di FireEye

Gabriele Zanoni di FyreEye

È un dato di fatto che la maggior parte dei sistemi di allarme domestici viene acquistata dopo aver subito un'effrazione. Il che equivale a chiudere la porta della stalla dopo la classica fuga del bestiame.
Non è parimenti una sorpresa e che anche la maggior parte delle aziende applichi lo stesso processo decisionale per le proprie reti, anche se con una scala diversa.
La maggior parte della spesa per la sicurezza, evidenzia **Gabriele Zanoni**, Senior Systems Engineer di FireEye, viene infatti destinata a misure preventive, come firewall e gateway web sicuri, ma la realtà è che le violazioni nelle rete continuano ad accadere con numeri notevoli, nonostante l'ammontare consistente di euro investiti in queste soluzioni, pur valide ma sempre meno efficaci.
Per peggiorare le cose, aggiunge l'azienda, il dwell time medio di una intrusione, e cioè il

tempo che trascorre prima che sia scoperta e rimossa, è attualmente di 78 giorni. Questo significa che gli attaccanti rimangono nelle reti aziendali per più di due mesi.

La domanda da porsi a questo punto è se una persona accetterebbe o meno che un ladro intrufolatosi nella sua abitazione e possa rimanerci tutto questo tempo? La risposta è di certo no e per questo semplice motivo il fattore "tempo" è essenziale quando si tratta di una violazione.



Provare e comprendere l'accaduto con la Network Forensic.

Come per qualsiasi intrusione in una proprietà privata o pubblica, possedere delle prove sul fatto accaduto è la chiave per comprendere l'evento sgradito, in che modo si sia verificata, cosa è stato trafugato e infine trovare il rimedio migliore per evitare che accada nuovamente.

Questo è il motivo per cui disporre di una soluzione di network forensics, osserva FireEye, è importante.

Ma di cosa si parla? In pratica, la network forensic è simile a un sistema di registrazioni a circuito chiuso. Consente di disporre della registrazione di tutto il traffico di rete in modo che quando si verifica una violazione i team di sicurezza possano consultarla immediatamente e retrocedere nel tempo. Disporre di un sistema di registrazione del traffico della rete consente in sostanza di ridurre il "dwell time" e identificarne l'impatto sui dati risultati compromessi,

Ma quali sono i benefici derivanti dal disporre di una soluzione di network forensics? Cinque i più importanti:

Eliminazione de gli angoli ciechi della rete. Dà la possibilità di registrare rapidamente tutto il traffico di rete. Significa avere una soluzione in grado di registrare il traffico ad alte velocità senza perdere l'integrità dei dati. Dopo tutto, non si può fermare ciò che non si vede.

Prove quando servono. Fornisce risposte a domande su chi ha fatto irruzione, che cosa hanno toccato, cosa si sono lasciati alle spalle, cosa è stato rubato, quali altri sistemi sono stati compromessi.

Sicurezza a un livello più elevato. Fornisce, tra le altre, indicazioni e "racconta" come si è verificata la violazione, dove è andato l'aggressore, quali sistemi e/o endpoint sono stati compromessi

Risposta ottimizzata agli incidenti. Fornisce garanzie su ciò che è effettivamente accaduto e su informazioni su come rispondere aiutando nel determinare quindi la gravità di una violazione.

Recupero semplificato. Permette di richiedere il risarcimento danni per le investigazioni o per altre finalità assicurativi dimostrando i danni effettivi e le perdite dovute agli attacchi informatici.

«Ogni rete aziendale è soggetta ad attacchi e violazioni. La storia, anche recente, dimostra che non basta concentrare tutti gli sforzi sulle misure preventive, in quanto è sufficiente una sola vulnerabilità, non solo tecnica ma anche logica, per entrare nella rete aziendale e fare danni. Detto questo è chiaro, conoscendone i notevoli vantaggi, che una soluzione di network forensics deve essere un must have per ogni azienda», ha commentato Gabriele Zanoni, Senior Systems Engineer di FireEye.

COME AFFRONTARE LA SFIDA DELLA SICUREZZA NEL CLOUD IN CINQUE PASSI

La protezione, la conformità e la capacità di integrare soluzioni di sicurezza per carichi di lavoro in sede e in cloud, sono tra le sfide per la sicurezza aziendale

Liviu Arsene di Bitdefender

Sebbene il cloud possa offrire vantaggi significativi, osserva Liviu Arsene, Global Cybersecurity Analyst di Bitdefender, le aziende devono tuttavia essere consapevoli delle problematiche legate alla sicurezza quando pianificano una strategia cloud-first.

Alcune di queste sfide non riguardano solo la protezione e la conformità, ma anche considerazioni operative, come la capacità di integrare soluzioni di sicurezza per i carichi di lavoro in sede e in cloud, di applicare policy di sicurezza coerenti in tutto il cloud ibrido e di automatizzare il rilevamento delle macchine virtuali (VM) per garantire visibilità e controllo sull'infrastruttura dinamica. Vediamo cosa suggerisce il manager.

1. Mettere in equilibrio protezione e conformità

Le violazioni più recenti, dovrebbero spingere i responsabili dell'azienda a pensare oltre la conformità. Oltre a rischiare più sanzioni, mettono a rischio anche la loro reputazione. Le normative di conformità tendono ad essere considerate come opzioni di sicurezza minime di base.

Tuttavia, una protezione completa comporta l'implementazione di più livelli di sicurezza progettati per aiutare i team IT e di sicurezza a ottimizzare le operazioni, rendere più visibili le minacce e accelerarne il processo di rilevamento prima che si verifichi una vera e propria violazione.

2. Integrare la sicurezza dei carichi di lavoro on-premise e nel cloud

Le soluzioni di sicurezza tradizionali possono, nella migliore delle ipotesi, offrire soluzioni distinte per i carichi di lavoro on-premise e in cloud, ma corrono comunque il rischio di creare problemi di visibilità e di gestione.

Nel peggiore dei casi, la stessa soluzione di sicurezza tradizionale viene distribuita su tutti i carichi di lavoro in cloud e locali – creando seri problemi di prestazioni per questi ultimi.

È importante, evidenzia il manager, che le aziende integrino una soluzione di sicurezza creata per modellare automaticamente il proprio agent di sicurezza in base al compito da svolgere, a seconda che il carico di lavoro sia on-premise o in cloud, senza influire sulle prestazioni o compromettere le funzionalità di sicurezza.

virtuali e di applicare le policy di sicurezza conseguentemente, senza costringere i team IT e quelli di security ad assegnare manualmente le policy a nuovi carichi di lavoro.

Considerando la flessibilità del cloud ibrido in termini di endpoint (fisici e virtuali) e di infrastruttura (on-premise e in cloud), è importante, suggerisce Liviu Arsene, che la soluzione di sicurezza garantisca la stessa elasticità e consenta alle aziende di godere appieno dei vantaggi di queste infrastrutture senza sacrificare prestazioni, fruibilità e sicurezza.

3.Distribuire policy coerenti se il cloud è ibrido

Le aziende devono comprendere che la distribuzione di policy di sicurezza in infrastrutture ibride può risultare problematica, soprattutto in assenza di una console di sicurezza centralizzata in grado di trasmettere senza soluzione di continuità tali policy a tutti gli endpoint e i carichi di lavoro.

È importante applicare automaticamente policy di sicurezza di gruppo alle macchine virtuali di nuova generazione, in base al loro ruolo all'interno dell'infrastruttura.

Ad esempio, i server virtuali di nuova generazione dovrebbero aderire immediatamente alle policy specifiche del gruppo, così come le VDI di nuova generazione, e così via. In caso contrario, le conseguenze potrebbero essere disastrose, in quanto rimarrebbero senza protezione contro le minacce e gli aggressori per tutto il periodo in cui sono operativi.

4. Rilevamento automatico delle VM

Le aziende dovrebbero prendere in considerazione l'adozione di soluzioni di sicurezza in grado di automatizzare il rilevamento delle macchine

5. Infrastruttura dinamica sotto controllo

Una piattaforma di sicurezza integrata può aiutare i team IT e di sicurezza a risparmiare tempo, offrendo al contempo funzioni di automazione della sicurezza che accelerano la capacità di identificare con precisione i segnali di una violazione dei dati.

Nel complesso, riassume il manager, e ci trova di certo d'accordo, affrontare le sfide relative alla sicurezza sul cloud è un lavoro costante e continuo che richiede che i team IT e a quelli dedicati alla sicurezza siano vigili e, allo stesso tempo, adottino gli strumenti di sicurezza e automazione più corretti che possano contribuire ad alleggerire una parte dei loro oneri operativi. Lavorare insieme per trovare le giuste soluzioni, assicura a entrambi i team di ottenere quello di cui hanno bisogno. È proprio la collaborazione tra questi due team, conclude Arsene, che garantisce la protezione dell'intera infrastruttura, indipendentemente da carichi di lavoro on-premise o sul cloud.

MANUFACTURING, ATTENZIONE AL RISCHIO CYBER

Cresce l'attenzione del manifatturiero per la cybersecurity. I servizi gestiti di sicurezza di alto livello sono fondamentali

Axitea, Security Provider italiano, ha richiamato l'attenzione sull'importanza della cybersecurity anche per le aziende che operano nel settore manifatturiero, e in generale industriale.
Il recente rapporto Allianz Risk Barometer 2019, evidenzia **Marco Bavazzano**, CEO di Axitea, ha in proposito posto in luce come in Italia i principali rischi percepiti siano l'interruzione di attività (al 1 posto con il 47% delle risposte), le minacce cyber e le catastrofi naturali, entrambi al secondo con il 38% delle risposte.
Se due elementi su tre possono apparire naturali in ottica aziendale, il report conferma che il rischio da cyberattacco è diventato una delle principali preoccupazioni anche per le imprese industriali.
Già nel 2010 la diffusione di Stuxnet (virus informatico appositamente creato e diffuso dal Governo statunitense in collaborazione col governo israeliano con lo scopo di sabotare la centrale nucleare iraniana di Natanz) aveva evidenziato la vulnerabilità dei sistemi di controllo industriale, anche quelli protetti tramite il completo isolamento da Internet.
Ancora oggi però, molte aziende manifatturiere ritengono che i propri sistemi di controllo industriale siano sicuri proprio per via dell'isolamento fisico e/o logico dalla rete dei sistemi informativi o per la diffusione di sistemi operativi diversi dal più vulnerabile Windows.
In realtà, mette in guardia il manager, i casi di attacco contro i sistemi di controllo industriale sono continui e costanti da diverso tempo.
Nonostante i principali siano probabilmente riconducibili ad azioni state-sponsor e diretti verso target di rilevanza nazionale, la diffusione del malware impiegato ha impattato molte aziende del tutto estranee all'obiettivo specifico.
Ciò avviene perché un malware, una volta rilasciato, si diffonde in modo incontrollabile attraverso molteplici vettori secondari causando danni significativi.
«Per questo motivo è necessario che tutte le aziende dotate di sistemi di controllo implementino un modello di business resilience che comprenda anche la gestione del rischio cyber - suggerisce Bavazzano -. Una componente fondamentale del modello è la capacità di rilevazione tempestiva degli eventi di sicurezza significativi, al fine di attuare un contrasto efficace e immediato alla propagazione per ridurre l'impatto degli incidenti».
«In una tale situazione dove l'esperienza conta molto, il ricorso a Security provider qualificati in grado di fornire servizi di Security Operation Center "as a service" può essere la scelta ottimale per molte realtà impossibilitate a sostenere in proprio gli ingenti investimenti necessari per dotarsi delle tecnologie, delle competenze specialistiche e degli aggiornamenti continui che consentono una gestione efficace (ossia proattiva) delle minacce».

EXCLUSIVE NETWORKS E NOZOMI INSIEME PER LA SICUREZZA INDUSTRIALE

Siglato un accordo che aggiunge al portafoglio Cybersecurity e Cloud Transformation del VAD le soluzioni di Nozomi per il settore industriale

Exclusive Networks, distributore a valore aggiunto (VAD), ha annunciato un nuovo accordo di distribuzione con Nozomi Networks, società specializzata in soluzioni di cybersecurity industriale e sede nella Silicon Valley.
Nata nel 2013 su iniziativa di due giovani italiani, Andrea Carcano e Moreno Carullo, Nozomi sviluppa soluzioni per rilevare minacce informatiche e difendere impianti e infrastrutture industriali e laintegrazione IT/OT. Supporta, inoltre, oltre 250mila dispositivi nei settori delle infrastrutture critiche, dell'energia, manifatturiero, minerario, dei trasporti e delle utility.
Sono diversi. osserva Exclusive Network, gli attacchi nel mondo industriale, casi come quelli subiti da Renault e Nissan, che hanno visto bloccati ben cinque plessi produttivi, o l'incidente in Ucraina in ambito ICS (Industrial Control Systems), dove sono stati inviati comandi per la disattivazione dell'elettricità in una grande città creando un blackout di due ore.
Attacchi di questo tipo non hanno il solo scopo di recuperare informazioni preziose, ma anche quello di creare disagi a infrastrutture critiche e mettere a rischio l'incolumità delle persone.

I temi di sicurezza per i sistemi industriali non possono quindi avere lo stesso approccio e metodologia utilizzata per l'Information Technology.
In un tale contesto, dove i criteri da rispettare sono la Disponibilità e l'Integrità in primis, poi la Riservatezza, sono indispensabili soluzioni tecnologiche che garantiscano la protezione di sistemi che devono essere "sempre accessi" e prevedere tempi di ripartenza "pari a zero".
Per fare security in ambito industriale, in sostanza, si rivela indispensabile utilizzare un approccio mirato e unico per la gestione di impianti IT e OT.
Molto spesso il mondo ICS viene attaccato sfruttando le vulnerabilità IT, che in seguito hanno impatto sui sistemi SCADA (Supervisory Control And Data Acquisition).
Nozomi, evidenzia Exclusive Networks, si colloca in questo settore in modo dedicato ed altamente specialistico con competenze tecnologiche per proteggere le applicazioni OT in reti di automazione, controllo e telecontrollo dai rischi informatici nell'industria e nelle infrastrutture critiche.

"Il mercato industriale è in continua evoluzione, gli impianti produttivi sono sempre più digitali e interconnessi – ha commentato Luca Marinelli, Managing Director Exclusive Networks Italia – L'Italia è il secondo paese manifatturiero

in Europa (dato CSC 2017 – Centro Studi Confindustria), ciò significa un rapido e profondo cambiamento per le infrastrutture critiche e di produzione con una prevedibile crescente domanda di soluzioni per la sicurezza. Accordi di distribuzione, come quello con Nozomi, si inseriscono pienamente nella mission di Exclusive di creare il VAD specialista globale più grande al mondo per la Cyber e Cloud Transformation. In particolare, questa nuova partnership con Nozomi permetterà a Exclusive di consolidarsi in un settore, quello industriale, in cui la cybersecurity ha un forte impatto, permettendo ai partner di ampliare la propria offerta indirizzata ad un settore in forte crescita, dove competenze e soluzioni specifiche permettono di affrontare l'importante sfida nel garantire un efficace livello di sicurezza all'interno delle infrastrutture".

"La sensibilità su tematiche di sicurezza OT è in continua crescita in modo trasversale sul mercato abbracciando ogni tipologia di azienda che opera con dispositivi SCADA – ha aggiunto Sergio Leoni, Regional Sales Director Nozomi – L'accordo di distribuzione con Exclusive Networks si inquadra in questo contesto in piena crescita come elemento di spinta, coesione e fulcro della preparazione dei partner, fornendo valore, competenza tecnica sulla tecnologia, fornitura di prodotti, know-how di integrazione ed approfondimento per i clienti ma soprattutto esperienza in un contesto in pieno e repentino sviluppo".

CORETECH RILASCIA LA BETA DI SYGMA CONNECT

CoreTech rilascia la beta pubblica di Sygma Connect per provarla gratuitamente almeno sino a fine Maggio

Il provider milanese di soluzioni tecnologiche, CoreTech, ha annunciato il rilascio della beta pubblica diSygma Connect, la soluzione per il controllo remoto per Windows, Linux e Mac OSX. È un prodotto realizzato da CoreTech che vuole essere un'alternativa low cost alla nota soluzione di connettività remota Teamviewer.

Dopo quasi 2 mesi di beta privata, che ha visto un nutrito numero di tester con oltre 65.000 minuti di sessione, ora è possibile installare Sygma Connect e provarlo gratuitamente almeno sino a fine Maggio, fa sapere la società.

Roberto Beneduci, CEO di CoreTech, ha commentato la novità: «Sono molto orgoglioso di questo progetto, tutto italiano, che mi ha visto coinvolto in prima persona a fare test notte e giorno da quasi un anno a questa parte. Non ho scritto una riga di codice, ma è figlio mio. Non sono la Mamma, però sono il Papà. La mia indole da tecnico, la mia voglia di capire ogni virgola del progetto che è stato sviluppato da Zero senza utilizzare VNC o derivati… Insomma, non ha prezzo far nascere un prodotto e vedere che ci sono altri che lo usano».

Sygma Connect verrà presentata ufficialmente in occasione della quarta edizione del CoreTech Summit 2019, che si terrà il 10 maggio presso il Royal Garden Hotel di Assago (MI). L'evento è indirizzato a Managed Service Provider, Cloud Solution Provider e professionisti che operano nel settore IT come system integrator, rivenditori, consulenti, sysadmin, devops, web master.

PARTNERSHIP STRATEGICA PER LE RETI E IL CLOUD DEL FUTURO TRA SIRTI E ADVA

Sirti e ADVA sostengono e rafforzano i progetti di cloud transformation ad alto contenuto tecnologico di operatori e aziende

Sirti Digital Solutions, la Business Unit di Sirti specializzata nella system integration, networking, SDN/NFV, cybersecurity, Cloud e Data Center, ha siglato un'alleanza strategica con ADVA, azienda multinazionale attiva nelle tecnologie di cloud interconnection (Open Optical Networking WDM) e cloud access (Carrier Ethernet e NFV), con l'obiettivo di sostenere progetti di cloud transformation ad alto contenuto tecnologico.

La partnership strategica nasce con l'assegnazione a Sirti da parte di TIM della progettazione e delivery di sistemi WDM ADVA per le sue reti regionali di trasporto ottico ad altissima velocità.

«Quello che stiamo annunciando oggi non è una mera alleanza; è l'intento condiviso di aiutare i fornitori di servizi e le imprese in tutta Italia a sfruttare le loro reti per cogliere nuove opportunità di business e offrire un maggiore valore ai loro clienti. È questo impegno che entusiasma entrambi i nostri team», ha commentato **Marcello Forti**, Vice Presidente delle vendite italiane, ADVA. «Insieme, supporteremo i nostri clienti a compiere il prossimo passo fondamentale nella trasformazione digitale dei propri processi e non c'è mai stato un momento più critico per farlo. La nostra tecnologia di rete aperta e sicura, combinata con l'esperienza ICT di Sirti, consentirà ai nostri clienti di crescere nel modo più scalabile, sicuro e flessibile possibile».

La collaborazione è derivata da una visione condivisa su due dei più rilevanti trend innovativi del mondo delle reti: network virtualization e intelligent edge.

«In Sirti Digital Solutions siamo costantemente impegnati nella ricerca di soluzioni tecnologiche d'eccellenza che riducano la complessità dei big data e che permettano di alleggerire il traffico sulle reti geografiche che collegano i data center alla periferia. In questo senso l'alleanza con ADVA è per noi un asset che aumenta il valore della nostra offerta, rendendola più distintiva e competitiva. Le tecnologie innovative di ADVA, inoltre, abilitano ad un nuovo approccio integrato all'Internet of Things, spostando l'intelligenza e le analisi sui dispositivi perimetrali. Questo ci consente di migliorare le prestazioni e la sicurezza delle reti dei nostri clienti e di offrire loro un importante vantaggio competitivo», ha commentato l'accordo siglato **Benedetto Di Salvo**, Vice Presidente della BU Digital Solutions di Sirti.

BT COLLABORA CON LA NATO PER LA DIGITAL TRANSFORMATION

I servizi forniti da BT si aggiungono ed integrano quelli attualmente erogati alla NATO di connettività globale

BT ha annunciato l'ampliamento della gamma di servizi che fornisce alla NATO a supporto delle operazioni globali dell'alleanza militare. L'annuncio fa seguito alla firma di un nuovo accordo triennale con la Communications and Information Agency (NCI) della NATO per servizi di supporto del valore di 5,9 milioni di euro.

Una connettività sicura e affidabile integrata da nuovi servizi di supporto è alla base della trasformazione digitale della NATO. BT connette più di 70 basi internazionali della NATO, compresi siti dislocati nei 29 paesi membri dell'Alleanza e oltre. L'aggiunta dei servizi di supporto di rete di BT all'Agenzia consente alla NATO di implementare nuove soluzioni all'interno dell'ambiente dinamico in cui opera.

«La Digital Transformation è un driver strategico per le organizzazioni multinazionali. Come molti dei nostri clienti globali, la NATO si trova a dover operare in un contesto dinamico, in cui cerca di sfruttare gli strumenti e le tecnologie digitali più recenti per migliorare le sue performance. Grazie alla nostra rete globale e sicura e alla nostra esperienza di fornitore affidabile di governi, agenzie internazionali e multinazionali, BT ha tutte le carte in regola per supportare la NATO in un mondo sempre più digitale», ha commentato l'annuncio **Bas Burger**, CEO di Global Services, BT

RINNOVATO IL PROGRAMMA PER I PARTNER DI VERTIV

Il nuovo programma VPP aiuta i partner nel soddisfare le richieste dei clienti per l'edge computing e la digitalizzazione

Vertiv, società che realizza e fornisce hardware, software e servizi di diagnostica e monitoraggio per le applicazioni mission critical, ha annunciato il nuovo programma di canale Vertiv Partner Programme. Alla base del programma tre iniziative principali: un nuovo piano di incentivi, un portale rinnovato per i partner e un portfolio più ampio per far crescere i reseller e i distributori in Europa, Medio Oriente e Africa (EMEA).

La strategia del vendor vuole consentire ai propri partner di soddisfare le richieste dei clienti in termini di edge computing, digitalizzazione e altre tendenze che stanno interessando il segmento del data center e maniera più ampia l'IT.

Per questo Vertiv nel corso dell'ultimo anno ha investito nella ricerca continua e approfondita per definire i quattro archetipi principali di edge computing e identificare i casi d'uso più consolidati per il 5G, che rappresentano secondo la società le opportunità commerciali più immediate per il proprio ecosistema di partner.

Un ulteriore vantaggio del programma di Vertiv è il nuovo EMEA Vertiv Incentive Programme (VIP), che consente ai reseller Authorised e Silver di guadagnare automaticamente punti bonus e monetizzare rapidamente i premi. Gli incentivi includono anche nuovi sconti per i reseller Gold e Platinum.