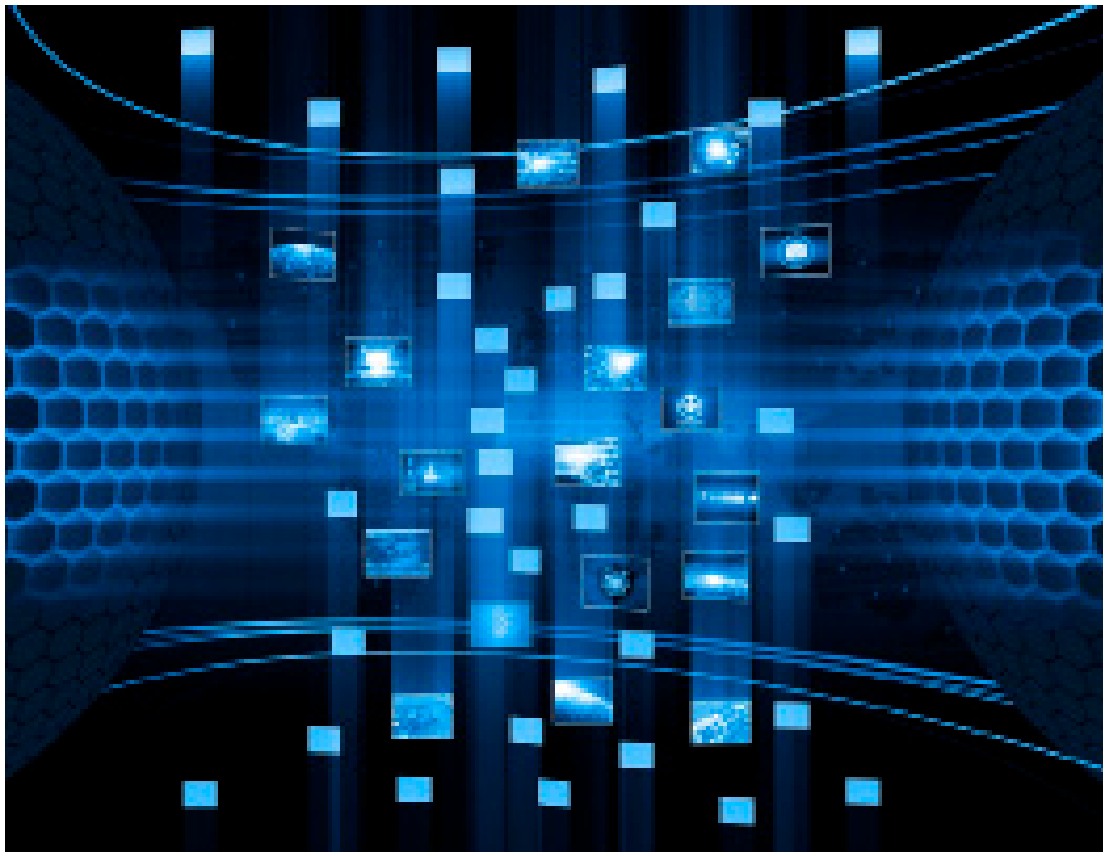
Cloud & Business
LA RIVISTA PER IL MANAGER CHE DEVE OTTIMIZZARE COSTI E PROCESSI
56
Maggio 2016

IN QUESTO NUMERO

Reportec

Come proteggere i dati nel cloud ibrido

La complessità del business complica la protezione dei dati da cui dipende. Una risposta per una business continuity rapida ed efficace viene dal cloud ibrido



Il Cloud si evidenzia sempre più come uno strumento per elaborare, salvare e fruire dei propri dati. Anche quando questo approccio non fa parte in modo esclusivo della strategia di archiviazione e di data recovery di un'azienda e del suo reparto IT, pur tuttavia è un approccio che permette di far fronte ad esigenze improvvise in attesa che le procedure di procurement interno di nuovo storage facciano il loro corso.

In sostanza, con il costante aumento del volume e del valore strategico dei dati, si ricorre sempre più spesso al cloud per soddisfare le esigenze di archiviazione e gestione dei dati. Le ragioni di una tale scelta sono ben individuate e possono essere riassunte nel fatto che i servizi cloud sono in grado di fornire livelli di flessibilità e scalabilità senza precedenti, consentendo allo stesso tempo di risparmiare sull'hardware e su altri costi invece associa-

ti a soluzioni on-premise, dalle esigenze di gestione a quelle di procurement, manutenzione, protezione, espansione o aggiornamento delle release software.

Ma come per tutte le cose esiste sempre il rovescio della medaglia: il backup e l'archiviazione dei dati nel cloud presenta le sue sfide, soprattutto per le aziende che non dispongono di uno staff IT consistente.

In linea generale si può affermare che i dati rappresentano il bene principale di un'azienda, ma proprio per questo motivo devono essere attentamente protetti da alterazioni, disastri, perdite o furti esterni o interni. Ma non si tratta solo di conservare.

Nell'economia digitale dove una informazione può perdere rapidamente il suo valore di mercato o strategico nel giro di un breve periodo di tempo, i dati devono essere facilmente accessibili da parte del personale autorizzato per consentire ai dipendenti di essere produttivi e, se la funzione lo richiede, essere disponibili e altamente interattivi verso e dai clienti.

La complicazione dei dati nel cloud

Una cosa però emerge, e cioè che le aziende di qualunque dimensione archiviano i propri dati in più luoghi. Tra questi il proprio Data Center, server fisici e virtuali, archivi off-site, cloud storage anche su diversi operatori, computer connessi in rete, dispositivi mobili e servici quali Dropbox. Non ultimo, le aziende stanno evolvendo verso una distribuzione dei carichi di lavoro su ambienti misti, incluso in questo applicazioni fisiche e virtuali e dispositivi mobili. Tutto ciò ha un forte impatto sia sull'IT interno che sui fornitori d servizi

"In qualità di esperti IT, oggi il lavoro è più impegnativo a causa del maggiore volume di dati archiviati in più luoghi; inoltre dovete tenere traccia di dove si trovano tutti i vostri dati e assicurarvi che questi siano protetti in qualunque moment,", evidenzia ad esempio Frank Jablonski, Vicepresidente marketing di Acronis.

Frank Jablonski

Come accennato, ogni medaglia ha il suo rovescio e certe volte questo rovescio riserva cattive sorprese. Per i responsabili IT che gestiscono ad esempio le reti di piccole e medie imprese, tentare di gestire e mettere al sicuro i dati in più luoghi utilizzando soluzioni multiple-point può trasformarsi velocemente in una attività frustrante che richiede molto tempo.

"Le soluzioni single-point tendono a funzionare su un particolare carico di lavoro o su un particolare tipo di carico di lavoro. Queste eseguono il backup solo di server fisici o solo di server virtuali. Ma la maggior parte delle aziende possiede un ambiente misto. Hanno server fisici, server virtuali e possono persino avere diversi tipi di server virtuali – un fornitore di servizi cloud può infatti utilizzare Microsoft Hyper-V, un altro Red Hat Enterprise Virtualization o Citrix XenServer", nota Jablonski.

In sostanza, la cosa si presenta complicata e in mancanza di una piattaforma singola in grado di fornire un controllo e una gestione unificata il reparto IT può incontrare forti difficoltà nel soddisfare i requisiti dell'azienda in relazione alla protezione base dei dati. In caso di incendio, alluvione, interruzione prolungata dei servizi di rete o violazioni della sicurezza di grave entità, un backup e una protezione inadeguati dei dati possono portare anche al fallimento di un'azienda che non sia in grado di recuperare o ripristinare velocemente il funzionamento dei sistemi IT.

Il solo utilizzo del backup su cloud può poi complicare l'accesso ai dati, la protezione e il backup dei dati poiché questi vengono archiviati in un sito remoto gestito da terzi e collegato tramite una rete. In caso di interruzione della rete i dati risultano inaccessibili, a meno

Palm Secure

che non siano stati salvati on-premise, in un centro dati o in qualche altro archivio locale come un dispositivo o la postazione di lavoro di un dipendente.

Non ultimo aspetto da considerare, un'azienda che utilizza solo l'archiviazione su cloud si affida in gran parte ad una terza parte che protegge fisicamente i suoi dati. I Service Level Agreement possono specificare livelli di protezione dati e uptime del cloud promessi, ma difficilmente questi sono garantiti.

Come proteggere i dati nel cloud ibrido

Per garantirsi la protezione dei dati archiviati in più luoghi localmente e in remoto le aziende possono adottare una soluzione basata su cloud ibrido in grado di copiare i dati da e su diversi ambienti cloud, sia in siti locali che remoti, Pc o server virtuali. Tramite il backup automatico su più siti diventa in sostanza possibile salvaguardare i dati lasciandone però l'accesso sicuro a dipendenti, partner, clienti e applicazioni.

In essenza, una piattaforma per la protezione dei dati deve permettere di recuperare i dati e ritornare rapidamente operativi sia che si tratti di un foglio di lavoro accidentalmente cancellato, una connessione caduta verso il fornitore di servizi Internet che ospita o gestisce il proprio sito web o del cloud recovery di un intero database a seguito di un evento catastrofico.

Agli eventi naturali o dovuti a guasti tecnologici se ne aggiungono poi altri, ancor più pericolosi: gli attacchi cibernetici.

Il problema è che un ecosistema altamente digitalizzato e interconnesso presenta molti vantaggi, ma attira anche l'attenzione indesiderata di molti cyber criminali che tentano di rubare informazioni. Per questo, la sicurezza dei dati in un ambiente ibrido dovrebbe comprendere una tecnologia di cifratura per proteggere questi dati da attenzioni non gradite.

Una protezione dati efficace comprende anche la protezione delle identità delle persone associate ai dati della propria azienda. Questo può essere effettuato archiviando le informazioni su chi ne è il proprietario separatamente dai dati rilevanti connessi, impedendo così ad un hacker di collegare dati bancari o finanziari ad un nome. In molti casi, la protezione dei dati implica anche la garanzia che l'azienda soddisfi gli standard di privacy e conformità dei dati, tema questo centrale per le assicurazioni sanitarie, le quali sono chiamate a soddisfare requisiti di privacy dei dati dei pazienti nazionali.

È una protezione che deve partire dal dispositivo usato per accedere ai dati o alle stesse aree riservate, la sala server, o il data center stesso. Lo stesso dispositivo usato dal personale IT per accedere al sistema di gestione da remoto dovrebbe essere altamente protetto, oltre gli usuali sistemi di password.

Una soluzione in proposito, evidenzia Fabrizio Falcetti, Business Program Manager di Fujitsu Italia, l'ha ad esempio sviluppata Fujitsu e si chiama Palm Secure.

Fabrizio Falcetti

È un dispositivo che può essere usato per controllare in modo sicuro l'accesso a un'area o disponibile in modo nativo in un Pc o in un notebook di fascia business e che permette di rilevare la configurazione venosa (attiva, per ulteriore maggior sicurezza) della mano. Ed è una funzione che interviene a livello BIOS, e quindi impedisce anche l'accesso al sistema operativo.

Dalla cifratura alla rilevazione sicura dei diritti di accesso le soluzioni quindi ci sono. Basta metterle in atto. ❋

INTEROPERANO 3CX HOTEL MODULE E PROTEL PMS

3CX ha annunciato che il proprio centralino basato su software 3CX Phone System è interoperabile con la piattaforma di applicazioni per la gestione alberghiera di protel

La società protel è un'azienda che dal 1994 produce software PMS (acronimo di Property Management System, che corrisponde a software di gestione alberghiera). L'offerta comprende ora anche protel Air, una piattaforma cloud SaaS con cui gli hotel possono gestire prenotazioni, assegnazioni di camere e altri aspetti inerenti le attività alberghiere.

La programmazione multifunzione dei pernottamenti di protel Air consente di prenotare o modificare la prenotazione delle camere e di accedere in modo diretto ai dati relativi agli ospiti. Se, ad esempio, un ospite cambia stanza, protel Air modifica automaticamente tutti i dettagli rilevanti tra cui lo stato della camera e i dati per la fatturazione. In questo contesto di utilizzo,

evidenzia 3CX, il modulo per hotel di 3CX fornisce l'integrazione tra il sistema di gestione alberghiera protel e il centralino 3CX Phone System. Quest'ultimo è un centralino IP basato su software che opera con i più noti sistemi operativi e quindi di facile gestione e manutenzione. La soluzione di UCC comprende un set funzionale per le Unified Communication, è stata sviluppata con l'obiettivo di consentire di ridurre i costi delle comunicazioni, aumentare la produttività e facilitare la mobilità del personale. In pratica, assicura allo staff la fruibilità di tutte le funzioni per le comunicazioni attraverso il software PMS, da cui riceve le informazioni che trasmette in tempo reale a telefoni IP o smartphone.

"La versatilità del 3CX Phone System è ora accessibile a tutti gli utenti del PMS della protel. Lo staff alberghiero potrà consultare informazioni e comunicare in tempo reale, quando e dove occorre", ha commentato Nick Galea, CEO di 3CX.

3CX e protel integrati

Lo staff ha accesso alle funzioni tramite una interfaccia web tramite la quale, in combinazione con il sistema telefonico, ha la possibilità di i gestire le diverse attività alberghiere. A livello di sistema integrato i profili degli ospiti sono collegati al numero della camera e al rispettivo telefono. In questo modo, qualora un ospite chiami la reception, il personale saprà esattamente con chi sta parlando invece di vedere esclusivamente il numero della stanza.

L'interazione diventa così più amichevole. Personale e management potranno salutare gli ospiti chiamanti rispondendo loro chiamandoli per nome. Qualora un ospite desideri non essere disturbato, basta che lo indichi premendo un pulsante sul telefono, il personale potrà consultare tale informazione in qualunque momento, prima di bussare alla porta.

Anche le informazioni in merito alla gestione delle camere sono collegate al telefono e allo scambio di informazioni tra le due soluzioni. Ad esempio, il personale addetto alle pulizie ha la possibilità di notificare lo staff tramite messaggistica istantanea se le stanze sono state liberate o pulite e tale informazione viene registrata nel sistema. Facilitata anche la mobilità del personale all'interno della struttura alberghiera. Tramite il client per smartphone di 3CX, gli impiegati dell'hotel possono essere raggiunti ovunque si trovino. ✱

É PIÙ SEMPLICE MITIGARE GLI ATTACCHI DDOS

Arbor Networks ha incrementato la scalabilità per mitigare gli attacchi DDoS e ridurre i tempi e la complessità operativa per farlo

Appliance Arbor per bloccare gli attacchi

Arbor Networks ha annunciato potenziamenti all'interno del proprio portfolio di soluzioni di mitigazione degli attacchi DDoS per reti di imprese e fornitori di servizi. Sono sviluppi volti a permettere una miglior gestione e ridurre la complessità nel contrastare gli attacchi DDoS di nuova concezione.

I nuovi sviluppi sono conseguenza del fatto, ha spiegato l'azienda, che sotto la spinta dell'utilizzo delle tecniche di riflessione/amplificazione, le dimensioni degli attacchi DDoS stanno crescendo a ritmo sostenuto. Secondo il Worldwide Infrastructure Security Report di Arbor, l'attacco più significativo riscontrato nel 2015 dalle imprese interpellate è stato della portata di 500 Gbit/s, quindi di 50 volte superiore rispetto a quelli riscontrati nel decennio scorso.

Appliance Arbor per bloccare gli attacchi

Inoltre, gli attacchi DDoS mirano ora non solo all'ampiezza di banda della connessione, ma anche ai vari dispositivi che costituiscono l'infrastruttura di sicurezza, tra cui gli apparati IPS/Firewall, come pure a un'ampia varietà di applicazioni su cui fa affidamento l'impresa, come HTTP, HTTPS, VoIP, DNS e SMTP. La protezione DDoS costituisce in pratica un aspetto fondamentale della continuità del servizio.

Nello specifico, Arbor è partita dalla creazione della sua tecnologia Cloud Signaling per sviluppare nuove funzionalità di mitigazione chirurgica che possano essere basate automaticamente o manualmente sulla strategia di mitigazione preferita dall'impresa. In particolare, l'Arbor APS 5.9 può avviare in cloud una mitigazione chirurgica per il traffico che è oggetto di attacchi in corso, senza interferire con il traffico normale degli host o dei servizi che non sono sotto attacco attivo. Ciò contribuisce a garantire la disponibilità di siti Web, applicazioni e infrastrutture riducendo il tempo di mitigazione degli attacchi DDoS.

Pur esistendo la capacità di automatizzare la mitigazione chirurgica in cloud, gli utilizzatori possono comunque vedere lo stato di mitigazione attiva nell'interfaccia utente che fornisce informazioni approfondite in tempo reale, come pure i report a seguito degli incidenti, che evidenziano tutti i dettagli dell'attacco e le misure adottate per mitigarlo.

Nuovi report presentano, aggiunge l'azienda, un riepilogo di elevato livello sulle attività dannose e il traffico normale nel corso del tempo, incluso il volume di traffico ispezionato e trasmesso o bloccato in quanto dannoso, come pure le minacce in uscita rilevate e bloccate. ❋

L'IT DIVENTA COMPONIBILE

Andrea Massari, country manager di Avnet TS Italia illustra cos'è e perchè è importante una "composable infrastructure"

Quando si pensava di aver finalmente sotto controllo infrastrutture convergenti, piattaforme convergenti e iper-convergenti improvvisamente si inizia a parlare di infrastrutture componibili. Ma di cosa si tratta? Cerchiamo di capirlo meglio con l'aiuto di Andrea Massari, country manager di Avnet TS.

Andrea Massari

Con l'infrastruttura convergente, spiega il manager, ci si riferisce in genere a uno stack integrato di elaborazione, storage e networking con un piano di gestione unificata. Gli esempi includono soluzioni di alcuni dei vendor distribuiti in Emea come Cisco FlexPod, HPE Converged Systems, NetApp, VCE Vblock e molti altri. Si tratta di soluzioni che possono essere integrate direttamente dal produttore o assemblate dal VAR o distributore (compreso Avnet) prima della distribuzione.

È però molto più di un semplice esercizio di 'confezionamento', perché i sistemi convergenti accelerano e semplificano la progettazione, l'approvvigionamento, la distribuzione e la gestione delle infrastrutture dei data center. Si sta parlando naturalmente di grandi sistemi: server blade, fabric switch e storage array. Questi sono progettati per fornire la potenza e la scalabilità necessari per eseguire qualsiasi carico di lavoro, virtualizzato o fisico che sia.

Ma in questo scenario, un paio di anni fa, sono andati apparendo i sistemi iper-convergenti, sistemi a nodo singolo che possono essere raggruppati insieme per creare pool di calcolo e di storage. Si tratta di sistemi software defined per combinare processori e dischi all'interno di ogni nodo nei cluster di calcolo e di storage. Sono progettati per ottenere velocità e semplicità di utilizzo, per essere implementati e ampliati in pochi minuti, semplicemente aggiungendo un altro nodo al cluster. Essendo hypervisor-dipendente, sono infrastrutture che sopportano solo i carichi di lavoro che possono essere virtualizzati.

Dentro una infrastruttura componibile

Ora, cos'è l'infrastruttura componibile? L'infrastruttura componibile, osserva Massari, rappresenta l'innovazione più significativa apparsa nello spazio convergente, perlomeno da quando sono entrate in scena le iper-convergenti, e rappresenta la più grande innovazione fino ad oggi.

Si potrebbe dire che l'infrastruttura componibile rappresenta un'architettura di data center con la velocità e la semplicità di una iper-convergente ma abbastanza flessibile per sostenere qualsiasi carico di lavoro (virtualizzato, fisico, containerizzato).

Si tratta in sostanza di una architettura unificata comprendente pool disaggregati di elaborazione, storage e struttura di rete, tutti controllati da un singolo piano di gestione. Tutte le risorse sono software defined, indipendentemente da dove si trovano gli switch o quale sia lo chassis che ospita le CPU e i dischi, ed è possibile comporre e ricomporre queste risorse in base alle singole esigenze.

Si tratta di pool di risorse fluidi, che possono essere forniti in modo indipendente e riallocati a volontà per sostenere qualsiasi carico di lavoro. Questa modalità viene spesso denominata "infrastructure as code." Si immagini di poter organizzare l'infrastruttura di data center come se si trattasse di rack di processori, rack di storage, rack di infrastruttura di rete (Ethernet, Fibre Channel, iSCSI, FCoE) che possono essere gestiti

in maniera flessibile e utilizzati come pura capacità in base alle esigenze dei carichi di lavoro, a prescindere dal fatto che tali carichi di lavoro siano virtualizzati o fisici.

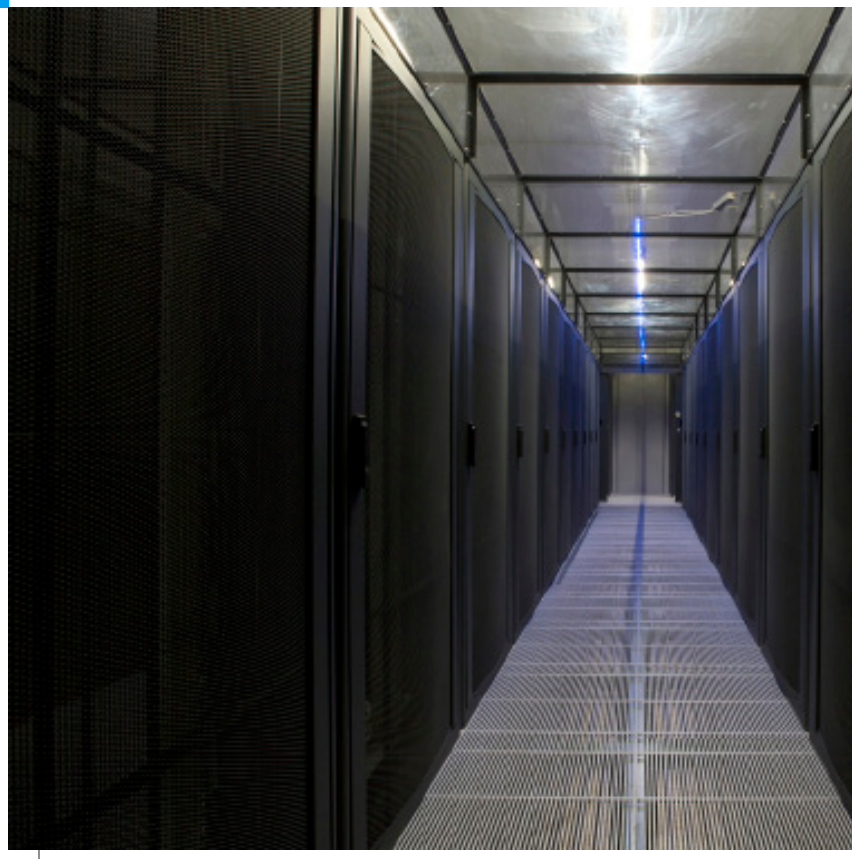
I vantaggi del componibile

Qual è dunque il vantaggio e perché ora? L'infrastruttura componibile promette di aumentare notevolmente l'efficienza a l'agilità dei data center. Questo perché l'infrastruttura componibile consente di creare una singola architettura di data center in grado di supportare i requisiti delle applicazioni aziendali tradizionali, fornendo al contempo la velocità e la flessibilità per supportare le richieste di nuovi progetti e applicazioni in una modalità agile e on-demand.

Quindi aspettiamoci, osserva Massari, nei prossimi mesi molto interesse intorno alle infrastrutture componibili. Si è appena all'inizio, e di certo non è difficile essere d'accordo. Peraltro, alcuni dei player chiave dell'infrastruttura sono già al lavoro sulla prossima fase di innovazione componibile, ad esempio per separare il complesso processore/memoria per consentire pool fluidi di memoria che possono essere forniti in modo indipendente dal processore. *

PER I SERVIZI CLOUD SERVE UNO STORAGE AD ALTISSIMA AFFIDABILITÀ

Nuovi modello di business hanno comportato per Genesys Informatica la ricerca di un approccio scalabile allo storage. La risposta nello storage FAS di NetApp



Gli operatori nel campo del service si trovano sempre più a dover fare i conti con la sicurezza e la realizzazione di soluzioni atte a garantire un elevatissimo standard per quanto concerne la business continuity. Anche chi ha già da tempo intrapreso questa strada si trova a dover fare i conti con ambienti applicativi e clienti sempre più esigenti e a voler dare loro una rapida e consistente risposta.
Un esempio di azienda che ha fatto della continuità operativa uno dei suoi aspetti salienti su cui investire è Genesys Informatica, società fiorentina presente da quasi 30 anni nell'ambito dei servizi di Information Technology. L'azienda opera con il marchio Hosting Solutions e la mission di rappresentare il punto di riferimento nel mercato dell'hosting.
L'infrastruttura tecnologica di Hosting Solutions è costituita da un complesso insieme di sistemi la cui connessione permette l'erogazione di numerosi servizi in sicurezza. L'infrastruttura si basa su 4 data center, di cui due di proprietà a Firenze e due in co-location a Roma e Catania.
Per ottimizzare l'efficienza e l'affidabilità tutti i servizi vengono erogati da server fisicamente distinti, in modo che ciascuno sia destinato alla gestione di una sola tipologia di dati e di richieste (web hosting, posta elettronica, database, storage).

Tecnologia per un nuovo modello di business

Le esigenze di un nuovo modello di business basato sui dati ha comportato per l'azienda un approccio sostanzialmente nuovo allo storage, alla cui base c'è un'integrazione di hardware a elevate performance con software scalabile e adattivo per lo storage. E' una combinazione che non si limita a supportare i carichi di lavoro già in essere, ma è anche in grado, ha spiegato l'azienda, di adattarsi e scalare rapidamente per essere utilizzato con nuove applicazioni e modelli IT in evoluzione.
Genesys Informatica, ha spiegato Alessio Fanfano, Marketing&Sales dell'azienda disponeva di storage, sempre di fascia enterprise, *"È utilizzato per offrire ai clienti principalmente servizi di hosting, poi cloud computing, server virtuali e quant'altro. Essendo un Internet Service Provider l'infrastruttura storage è una parte assolutamente fondamentale e deve garantire standard di disponibilità e affidabilità il più elevati possibile. Oltre a questo lo storage deve essere indipendente dai server"*.
Vediamo come tutto questo è stato ottenuto.

La soluzione in campo

Per quanto concerne lo storage Genesys Informatica disponeva già da qualche anno di soluzioni storage di NetApp, ovvero

FAS8060

un FAS3140 in dismissione e un FAS3240, sistemi all'epoca stand alone, sui quali poggiava una serie di servizi (hosting, e-mail e buona parte del private cloud).

"Dopo avere valutato un upgrade del sistema, abbiamo avviato una selezione tra varie aziende. Alla fine la scelta è caduta su NetApp perché abbiamo ritenuto che i suoi prodotti all'avanguardia rispondessero pienamente alle nostre esigenze presenti e future e offrissero caratteristiche per noi fondamentali, quali il supporto del protocollo NFS (Network File System)", ha illustrato Fanfano. "A questo punto ci siamo rivolti al system integrator Ergon, un partner 'di fiducia' con il quale collaboriamo ormai da diversi anni".

Il primo passo è stato quello di affiancare un FAS3250 con sistema operativo C-dot Cluster Data ONTAP e la migrazione in cluster del FAS3240. Al variare del business (acquisizione nuovi clienti e aggiunta di servizi) si sono create nuove esigenze legate in gran parte alle prestazioni e l'infrastruttura - FAS3250 + FAS3240 - si è rivelata inadeguata.

Quindi, come secondo step, è stata aggiunta una macchina FAS8060, in sostituzione della FAS3240, e ricreato il cluster con quattro nodi (FAS8060 + FAS3250). Il tutto sfruttando le potenzialità del software NetApp Data ONTAP, che ha permesso di non creare disservizi.

I miglioramenti ottenuti per servizi e sicurezza

"Per quanto riguarda l'hosting, in particolare, abbiamo un'architettura separata e i dati risiedono, non sui dischi del server stesso, ma sul sistema NetApp con il protocollo NFS, lo standard più utilizzato per l'accesso ai dati condivisi. In pratica il server è usato esclusivamente come risorsa computazionale, mentre tutta la parte storage è affidata alle soluzioni NetApp che sono più affidabili rispetto ai dischi all'interno della macchina", spiega Alessio Alfano. "Questo ci garantisce una notevole flessibilità, grazie al fatto di poter ampliare lo storage senza aggiornare o incrementare la parte server. Tra le altre caratteristiche per noi importanti, gli snapshot a caldo e ad alta velocità che permettono di acquisire una copia del volume di dati in pochi secondi: se, per esempio, un cliente dovesse 'perdere' la posta elettronica siamo in grado di recuperarla velocemente così come ogni singolo file Web o quant'altro".

Rilevante, ha anche evidenziato il manager, la possibilità tramite il software NetApp Data ONTAP in cluster e la funzione NDO (Non Disruptive Operations), di effettuare aggiornamenti e ampliamenti a "caldo" e che la configurazione del sistema in RAID 6 con Double Parity garantisce prestazioni elevate e incrementa la sicurezza, in quanto previene la perdita dei dati anche nell'eventualità del guasto di due unità. ❋

F-SECURE ED EUROPOL CONTRO IL CYBER CRIME

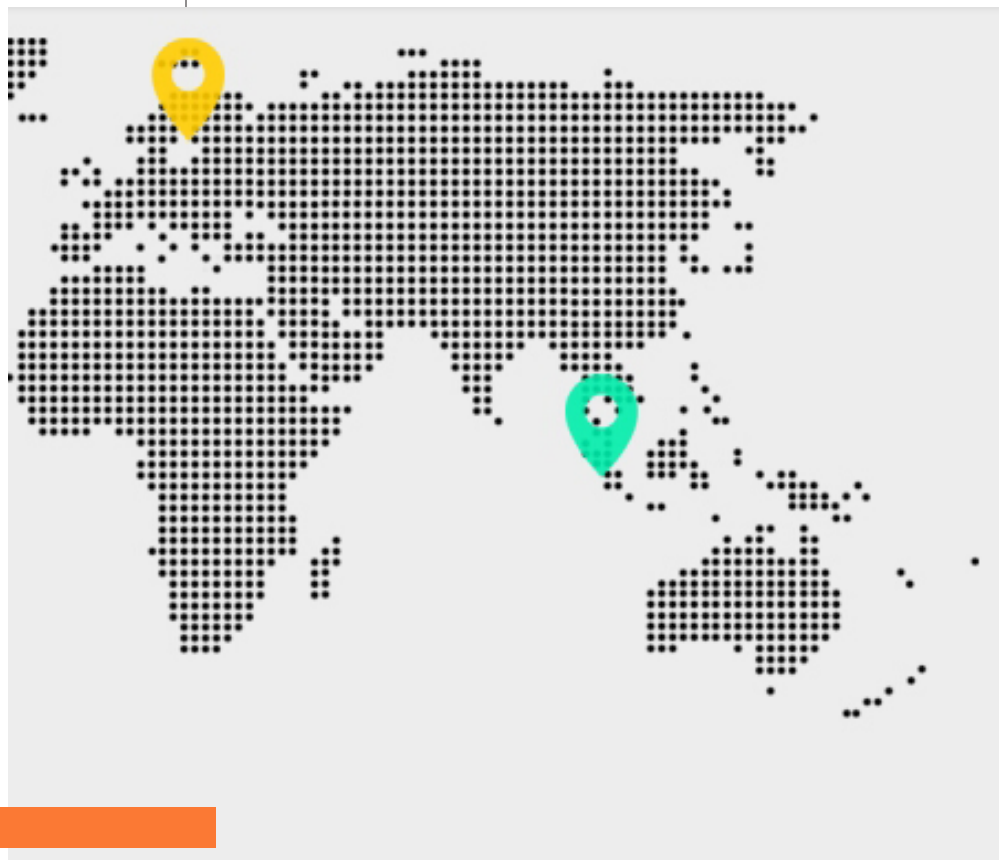
F-Secure ed Europol hanno siglato un memorandum che le vedrà operare congiuntamente per rispondere in modo sempre più efficace alle minacce

F-Secure ha sottoscritto un Memorandum of Understanding (MoU) con il Centro Europeo per il Cybercrimine di Europol (EC3) che consentirà una cooperazione avanzata nella lotta contro il crescente problema del crimine informatico. Il MoU è stato siglato presso l'headquarter di Europol all'Aia.

L'MoU è la conferma che affrontare le sfide odierne alla sicurezza digitale, rese ancora più critiche dalla adozione del Cloud, richiede un approccio collettivo in cui le forze dell'ordine e l'industria privata devono lavorare insieme in modo più stretto. Va osservato che in un panorama della sicurezza complesso, partnership come questa stanno diventando sempre più importanti, specialmente a causa della rapidità con cui la tecnologia continua a evolvere. In particolare, evidenzia F-Secure, l'MoU consentirà uno scambio tra le due parti di esperienze, statistiche e informazioni strategiche sulle minacce informatiche.

"La firma di questo memorandum d'intesa tra Europol e F-Secure migliorerà le nostre capacità e aumenterà la nostra efficacia nell'assistere le forze dell'ordine in Europa nel prevenire, perseguire e far cessare la criminalità informatica. Una cooperazione attiva di questo tipo tra le forze dell'ordine e l'industria è la via più efficace attraverso la quale possiamo sperare di rendere sicuro il cyber-spazio per i cittadini e le aziende europee. Sono certo che con l'alto livello di esperienza tecnica di F-Secure otterremo un significativo vantaggio per le nostre attività investigative in Europa. Sono grato per la loro collaborazione e ansioso di sviluppare un eccellente rapporto di lavoro", ha commentato la sigla dell'accordo Steven Wilson, Capo dell'European Cybercrime Centre (EC3) di Europol.

"La nostra missione è proteggere le persone e le aziende dalle minacce informatiche, e la cooperazione con le forze dell'ordine è una parte importante di questa missione. Siamo entusiasti di poter offrire la nostra intelligence delle minacce a Europol per aiutarli nei loro sforzi investigativi e di applicazione dell'ordine nel rendere il mondo online un posto più sicuro per tutti", ha aggiunto Kimmo Kasslin, Capo dei Laboratori di F-Secure. ❋



I Lab di F-Secure

INEBULA ALLA DISRUPTIVE WEEK MILAN 2016

La società del Gruppo Itway ha partecipato alla seconda edizione della settimana dedicata all'innovazione digitale

iNebula, società del Gruppo Itway, è stata presente in veste di sponsor e speaker alla Disruptive Week Milan 2016, la serie di eventi dedicata alle tecnologie emergenti e alla rivoluzione digitale.

Due i momenti dell'evento che l'anno vista coinvolta: nel primo Stefano Della Valle, VP Executive Sales and Marketing di iNebula, è intervento sul tema "Piattaforme multiservizio per IoT e M2M", mentre nel secondo iNebula ha partecipato all'IOTEXPO, evento di rilievo per le aziende operanti nel settore dell'IoT dove sono stati illustrati i progetti attualmente in corso dedicati allo smart work e alle smart city, due temi su cui il Gruppo Itway e i-Nebula sono molto attivi.

La partecipazione agli eventi è stata anche l'occasione per parlare in modo approfondito dei vantaggi offerti dalla piattaforma Connect di iNebula, la tecnologia alla base dell'infrastruttura integrata studiata per gli ambienti M2M e IoT capace di supportare oggetti smart, raccogliere i dati, archiviarli e distribuirli in modo intelligente per consentire un processo decisionale rapido ed efficiente.

Stefano Della Valle

Presso iNebula un gateway IoT

iNebula, ha evidenziato Della Valle, è peraltro in prima fila nell'adesione a iniziative volte a favorire lo sviluppo tecnologico e l'innovazione in chiave IoT. L'azienda ha infatti installato nella propria sede di Milano un gateway con possibilità di gestione dei dati attraverso la piattaforma iNebula Connect portando in Italia l'iniziativa internazionale "The Things Network", nata ad Amsterdam nel 2015.

Si tratta del primo passo, ha spiegato la società, verso la creazione di un'infrastruttura aperta, partecipata da aziende private, ma anche da cittadini, che consentirà di mettere in rete oggetti, applicazioni e dati, in modo da offrire servizi a valore aggiunto alle aziende e ai cittadini secondo la logica dell'Internet of Things (IoT), passi necessari per la realizzazione concreta di vere e proprie smart city.

In ottica "smart work", l'azienda ha anche illustrato il nuovo iNebula Contact Center, un servizio che permette di dare vita a sessioni audio/video con qualsiasi interlocutore senza doversi trovare fisicamente in ufficio.

Spazio è stato anche dedicato ad un recente upgrade di iNebula Safe Backup Sync, un servizio di backup dei dati che consente di disporre di una repository nel cloud nella quale salvare in tempo reale i documenti in lavorazione sul proprio dispositivo, e questo ovunque ci si trovi. ✱

INTERACTIVE INTELLIGENCE ANNUNCIA PURECLOUD ENGAGE

Contact Center più orientati al business e contatto con il cliente più friendly e produttivo con PureCloud Engage per Salesforce

Interactive Intelligence ha reso disponibile PureCloud Engage per Salesforce su Salesforce AppExchange. L'obiettivo dell'azienda è di dare alle imprese la possibilità di connettersi con clienti, partner e impiegati in un modo completamente nuovo.

Interactive Intelligence è un fornitore di servizi cloud per il customer engagement, le comunicazioni e la collaborazione, servizi progettati con l'obiettivo di aiutare le aziende di tutto il mondo a migliorare i servizi e la produttività e a ridurre i costi.

PureCloud Engage è un servizio distribuito attraverso la piattaforma PureCloud di Interactive Intelligence, una applicazione cloud dell'azienda che si presenta come un insieme di micro servizi indipendenti e con bilanciamento di carico basato sugli Amazon Web Services.

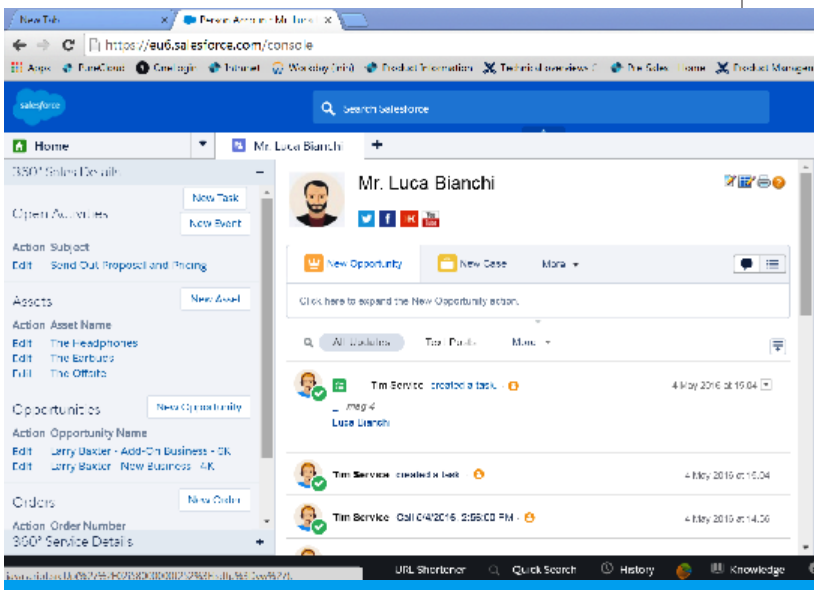
La piattaforma PureCloud costituisce, ha evidenziato la società, un set molto esteso di servizi progettati per garantire elevati risultati di business per le organizzazioni di ogni tipo e dimensione. Tra le funzionalità comprese nella soluzione:

- Schermate pop-up guidate da regole: dati dell'utente, come l'ID chiamante, il numero chiamato (DNIS), case number e indirizzo email, guidano finestre pop-up dei contatti associati a Salesforce, per generare o personalizzare un servizio più veloce ed efficiente.
- Controlli di gestione dell'interazione embedded: la capacità di gestire, monitorare e accodare le chiamate, le email, web chat e callback dall'interno dell'interfaccia Salesforce consentono un incremento della produttività.
- Presence Management : fornisce una serie di impostazioni di presence e stato in tempo reale al fine di migliorare la collaborazione.
- Reporting unificato: l'interaction reporting integrato con Salesforce permette una migliore comprensione della performance e migliora la coerenza e l'accuratezza dei dati.

"Non possiamo che elogiare il valore che PureCloud Engage ci ha portato, dal miglioramento di servizio alla crescita dell'efficienza. Sarà sicuramente un vantaggio in futuro e potremo potenzialmente espandere le caratteristiche che offriamo", ha affermato Steve Palencia, direttore di Universal Protection Service.

"Le aziende stanno cercando di trasformare il modo in cui si connettono con clienti, partner e dipendenti e prosperare nell'era del cliente", ha affermato Todd Surdey, SVP, ISV vendite di Salesforce. *"Sfruttando la potenza di Salesforce App Cloud, PureCloud Engage™ dà ai consumatori tecnologie cloud social, mobile e connesse provate, per accelerare il successo del business"*.

Come evidenziato, basato su Salesforce App Cloud, Interactive Intelligence PureCloud Engage per Salesforce è attualmente disponibile su AppExchange. ✱



Pop Screen di PureCloud

QNAP E XOPERO ASSIEME PER PROTEGGERE I DATI

La nuova soluzione Xopero QNAP Appliance semplifica il backup su NAS in rete e nel cloud

QNAP, Quality Network Appliance Provider e Xopero, produttore di applicazioni di backup in Europa, hanno annunciano di aver dato il via ad una partnership tecnologica in Italia per il prodotto Xopero QNAP Appliance. L'attività di distribuzione è stata, inoltre, affidata a S-mart, azienda fiorentina specializzata in soluzioni cloud e di sicurezza.

Xopero QNAP Appliance, prodotto di punta del Xopero, è una soluzione di backup per i NAS di QNAP, che ha l'obiettivo di trasformare il dispositivo NAS in un sistema di backup professionale, pur mantenendone immutate le funzionalità che lo equipaggiano.

Di base, Xopero QNAP Appliance è una soluzione di backup gestibile centralmente che permette di trasformare il NAS QNAP in un dispositivo di backup atto a proteggere l'infrastruttura IT dell'azienda.

Una volta installato il prodotto Xopero sul QNAP, diventa possibile eseguire il backup di file e cartelle da tutti i Pc e i server presenti nella rete, oppure creare immagini di backup dell'in-

tero sistema operativo attraverso le funzioni VHD (client) e System State (server), eseguire i backup dei Database (SQL, MySQL, PostgreSQL, Firebird), dei server Exchange (2007, 2010, 2013) e degli ambienti virtuali a livello di HOST (sia Hyper-V installandolo sull'host sia VMware in modalità agentless).

A questo Xopero QNAP Appliance aggiunge altre funzioni quali: backup incrementali e differenziali, preservazione dei dati, versioning dei file, crittografia AES-256, opzioni di compressione e di pianificazione dei backup. In pratica, può operare come una soluzione di disaster recovery sia per gli ambienti fisici sia virtuali che garantisce la continuità del business riducendo i tempi di inattività .

Tramite Xopero, ha evidenziato l'azienda, è anche possibile eseguire il backup degli endpoint, dei server e di interi ambienti virtuali sul NAS QNAP e in caso di crash avviare direttamente le loro immagini di backup, all'interno di macchine virtuali, create tramite la Virtualization Station di QNAP.

Per facilitarne l'adozione e capirne meglio i vantaggi, Xopero e QNAP hanno in corso di realizzazione un ciclo di seminari congiunti per conoscere le funzionalità di Xopero QNAP Appliance, il programma per i partner ed i benefici finanziari. ❋

Appliance QNAP per il backup

QLIK ANNUNCIA QLIK SENSE CLOUD BUSINESS

Visual Analytics disponibile via Cloud

Il nuovo servizio SaaS di Qlik mette a disposizione delle PMI e dei gruppi di lavoro la Visual Analytics su cloud per creare, gestire e condividere app

Qlik, società che sviluppa applicazioni per la Visual Analytics ha presentato Qlik Sense Cloud Business, un suo nuovo servizio che espande la precedente offerta Qlik Sense Cloud. Il nuovo prodotto è volto a consentire a piccole e medie imprese o a gruppi di lavoro di creare, gestire e collaborare con la Visual Analytics tramite cloud. Nello spirito del Cloud l'accesso è su abbonamento e non richiede particolari investimenti up-front.

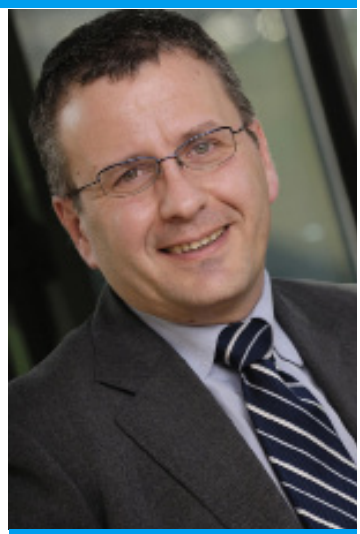
Le attuali offerte di Qlik Sense Cloud Basic e Plus, ha spiegato l'azienda, forniscono agli utenti privati i benefici di Qlik Sense, uniti alla possibilità di condividere analisi e informazioni. Qlik Sense Cloud Business integra il tutto con funzionalità di sicurezza e gestione e si focalizza, come evidenziato, sui servizi utili a gruppi di professionisti all'interno delle organizzazioni dando loro la possibilità di applicare e gestire app di analisi. Ad esempio, ha illustrato l'azienda, Qlik Sense Cloud Business include:

- Un'area di lavoro di gruppo, che consente agli utenti di collaborare, creare, revisionare e accedere a contenuti e app, migliorando la collaborazione senza penalizzarne la flessibilità.
- Uno spazio che raccoglie i dati di gruppo, che permette a tutti gli utenti di fornire informazioni riutilizzabili e coerenti, velocizzando il processo di elaborazione di nuove app ed eliminando l'ipotesi di mantenere alcune app una volta che le necessità dell'azienda si sono evolute nel tempo.
- Reti di gruppo condivise, che offrono molteplici network condivisi che gli utenti potrebbero essere invitati a seguire, con la possibilità di controllare quali utenti hanno accesso a quali app.

Non ultimo, il modello basato su Cloud permette alle aziende di aggiungere nuovi utenti e nuove app in base alle esigenze e con la flessibilità necessaria per affrontare le nascenti esigenze. ❋

DOPO QUELLA DEL CLOUD INIZIA L'ERA DELLE AUTO CONNESSE MA C'È IL PROBLEMA DEI DATI

Nell'era del Cloud la convergenza tra automotive e ICT genera enormi volumi di dati personali. Si apre il problema della loro elaborazione, conservazione e riservatezza. Il parere di NetApp



Roberto Patano

Le "auto connesse" sono una realtà e potrebbero rappresentare la fase finale dell'automobile come la conosciamo oggi. Il futuro in cui non ci sarà bisogno di qualcuno dietro il volante è oramai dietro l'angolo. Ciò che lo rende possibile sono sistemi IT che si basano sui dati per gestire l'interazione di un veicolo con le persone al suo interno e con l'ambiente esterno, dalla logistica alle reti urbane.

Per capire cosa attendersi e i problemi che si dovranno affrontare per quanto concerne i dati che verranno generati e conservati abbiamo chiesto l'auto di Roberto Patano, senior manager sytems engineering di NetApp Italia.

Il dato di partenza è che entro 5 anni si prevede che ci saranno 220 milioni di veicoli collegati sulle strade, il che, a parte un fatturato di oltre 152 miliardi di dollari per il solo software e le relative attrezzature, porterà a dover gestire e decidere come proteggere una mole enorme di dati.

Macchine intelligenti e connesse

I giganti del Net come Apple e Google, che detengono enormi masse di dati, puntano a macchine che siano collegate e che possano funzionare senza conducente. L'intero settore è però ad essere in fermento. Ford ha annunciato una partnership con Apple e Google, i cui prodotti Android Auto e Auto Play sono caratterizzati da un sistema automotive multimediale che consente agli automobilisti dotati di un iPhone o un telefono Android di accedere alla loro musica, di effettuare chiamate e di effettuare la navigazione GPS semplicemente con una voce Siri (funzionalità di iPhone) o con un comando Google Voice.

Da parte sua GM ha creato una divisione per sviluppare servizi di mobilità e ha investito 500 milioni di dollari in Lyft per sviluppare veicoli autonomi.

Il produttore di sensori di precisione (laser, ultrasuoni, telecamere a infrarossi o HD), Valeo, ha dimostrato il proprio know-how sviluppando un sistema di guida autonoma che utilizza i propri componenti.

Se le case automobilistiche sono scese in campo, osserva Patano, lo sono però anche le compagnie telefoniche. Ad esempio, Orange sta commercializzando un hotspot Wi-Fi sviluppato in partnership con Huawei che si inserisce nella presa accendisigari. Esso riceve e distribuisce i segnali 4G in macchina e si collega con attrezzatura da cruscotto come il GPS.

Si punta sulla personalizzazione

La parola chiave è però 'Personalizzazione', intendendo con questo veicoli che potranno essere adattati alle esigenze degli occupanti grazie ad algoritmi di apprendimento automatico e alla profilazione del proprietario o del passeggero.

Ma confluenza tra automotive, informatica, cloud, applicazioni, telecomunicazioni e reti ha, come già evidenziato, l'effetto di generare una moltitudine di dati, e dati che sono in buona parte personali.

Di chi è la proprietà, dove e chi li conserva e che utilizzo se ne può fare, osserva Patano, ha molte implicazioni, non solo per l'utente del veicolo. Per esempio, la raccolta dei dati da quella che sarebbe una capillare distribuzione di dispositivi IoT di elevata qualità e intelligenza, potrebbe contribuire a semplificare la gestione e ridurre i costi sociali. Attraverso la raccolta di dati provenienti da tutti i veicoli sarebbe possibile reindirizzare i veicoli verso percorsi alternativi, evitare ingorghi e di conseguenza ridurre i consumi energetici e l'impatto sul territorio.

Un futuro prossimo di macchine iperconnesse (fonte Fastweb)

Numerosi i vantaggi anche per la logistica con la possibilità di informare i player coinvolti nella supply chain n modo da ottimizzare il rifornimento delle scorte lungo le rotte più trafficate.

Di chi sono i dati?

Tutto ciò però porta a fare considerazioni sui dati. La questione dei dati generati dalle macchine connesse in rete è complessa e non del tutto regolamentata. I dati vengono prodotti tramite applicazioni per la navigazione, multimedia o di telefonia che sono gestibili dallo schermo di bordo della vettura. Forniscono informazioni circa le abitudini del guidatore (dove è stato, quanto si è fermato, cosa ha trasmesso, a che siti si è collegato, eccetera), che possono essere trasmesse al costruttore di automobili e da questi a terzi. Sembrerebbe logico, da un punto di vista giuridico, che i dati appartengano al pilota che li genera. Esistono già leggi sulla protezione dei dati ma il confine rimane incerto in relazione a chi i dati appartengono de facto.

In proposito la Federazione Internazionale dell'Automobile ha già lanciato una campagna chiamata "La mia auto i miei dati" relativa alla proprietà dei dati inviati da parte dei conducenti, campagna volta a sensibilizzare gli automobilisti sui dati che emettono mentre permette una maggiore libertà nel loro uso.

Come e dove archiviare i dati

L'archiviazione dei dati e la loro sicurezza, evidenzia Patano, è quindi un aspetto chiave della rivoluzione in atto, ma non è l'unico. Ad esso si aggiunge quello della gestione dei dati nel tempo. OEM del settore ed i loro partner potranno commercializzare sistemi in grado di raccogliere grandi quantità di dati. I giganti Web e le compagnie telefoniche stanno già mettendo piede in questo mercato di cui si prevede una rapida espansione, e non solo per motivi tecnologici. Si tratta infatti di aziende in grado di offrire nuovi servizi agli automobilisti in base a ciò che sanno su di loro e le loro abitudini al di fuori del veicolo.

"La connettività sugli automezzi non funziona a meno che la raccolta, l'accesso e l'analisi dei dati siano adeguatamente ponderate, supportati da tecnologie adeguate per gestire l'archiviazione dei dati, abbastanza scalabile per supportare lo sviluppo di nuove funzionalità. Le automobili sono state una questione sociale fondamentale nei paesi sviluppati negli anni 1960 e 1970. Ora, le automobili sono divenute una questione nei Paesi in via di sviluppo, anche in relazione all'urbanizzazione e all'inquinamento. Il 20° secolo ha visto l'avvento delle autovetture. Eppure ci sono ancora molti dibattiti a venire su tecnologie automobilistiche, affari e modelli industriali - e non solo: anche circa etiche, questioni filosofiche e comportamentali", mette in guardia Roberto Patano. ❋

di Giuseppe Saccardi

Più sicurezza per Cloud e Mobilità

La diffusione dei servizi Cloud e di Mobility stanno cambiando il modo con cui si interagisce sia nell'ambito professionale che sociale. Se l'aspetto positivo è indubbio si tende a dimenticare quello negativo: l'impatto sulla privacy e la sicurezza dei dati riservati, personali o aziendali che siano.

A quelli usuali si sommano ora i problemi derivanti dalla progressiva digitalizzazione dei servizi finanziari.

Con quella che certe volte viene proposta come facilitazione per il cliente (ma che non scaccia il dubbio che in primis sia volta a ridurre i costi per l'ente finanziario), molte banche e altri enti stanno spingendo l'uso di dispositivi portatili e fissi per l'accesso a quello che viene definito uno sportello virtuale, per prelevare o effettuare pagamenti e via dicendo.

Trattandosi di propri quattrini o di quelli dell'azienda è evidente che ai rischi già insiti nell'uso di dispositivi elettronici se ne aggiunge uno nuovo, soprattutto se il dispositivo viene smarrito.

Cosa fare? Visto che comunque poter pagare, effettuare transazioni in mobilità o via cloud, eccetera, è in effetti comodo, impossibile affermare il contrario anche per il più accanito tecnofobo. è opportuno porre attenzione al secondo fattore dell'equazione: la sicurezza. Perlomeno per quanto possibile nel caso un dispositivo venga smarrito.

Una cosa è certa, mettono in guardia gli esperti, la semplice password non basta proprio più. Ci vogliono strumenti più raffinati ed evoluti quando si trasferiscono dati, ad esempio la cifratura con robuste chiavi. E per accedere al dispositivo è meglio affidarsi non alle usuali password ma a dispositivi più sicuri quali i sistemi di riconoscimento biometrico, dalle impronte al palmo della mano. Così, tanto per prudenza. *

Numero 56 del 30/05/2016

Registrazione al tribunale n°574 del 5/11/2010

Editore: Reportec Srl

Direttore responsabile: Giuseppe Saccardi

In redazione: Gaetano Di Blasio, Riccardo Florio, Paola Saccardi

Immagini: dreamstime.com