DICEMBRE 2011
ANNO 1 - N.1

IP Security MAGAZINE

ETHOS MEDIA GROUP

Nasce IP Security Magazine

IP FOR DUMMIES

ISO/OSI, TCP/IP protocollo IP e soci: mini introduzione alle reti interconnesse

APPLICATION CASE

Soluzioni wireless ridondate per l'Unione dei Comuni del Medio Verbano

CHIEDI ALL'ESPERTO

Non è tutto ORO quello che è CLOUD

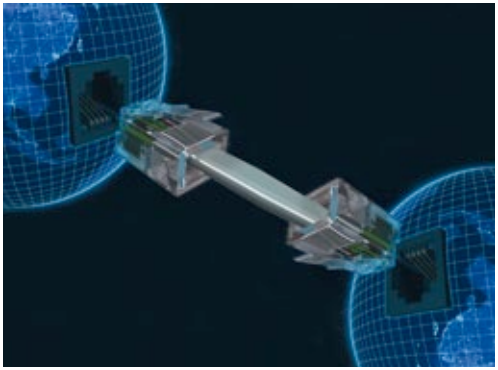
ETHOSMEDIAGROUP

COLTIVIAMO E FACCIAMO CRESCERE IDEE!

www.ethosmedia.it

Perché *IP Security Magazine*

L'ESPRESSIONE "IP SECURITY" assume significati diversi in base alla sua contestualizzazione.
In ambito informatico, si riferisce agli standard per la trasmissione sicura di informazioni pacchettizzate, mentre in ambito impiantistico di sicurezza o di sistemi per la comunicazione elettronica, rappresenta le tecnologie di protezione e prevenzione supportate dalla rete IP (videosorveglianza, antifurto e rapina, rilevazione gas e incendio, building/home automation, controllo accessi, ecc). Nel momento in cui, però, il protocollo IP viene utilizzato per trasmettere dati legati ai segnali di allarme o alle riprese video, le problematiche di sicurezza che si generano sono del tutto simili a quelle di tipica competenza dell'IT manager, entrando nel novero della sicurezza logica. La rivoluzione IP che sta digitalizzando i segnali d'allarme e veicolando su rete IP molte informazioni di sicurezza in senso tradizionale, porterà quindi indubbi vantaggi e opportunità di business, ma anche nuovi rischi e problematiche.



Sul fronte delle dinamiche del mercato, il processo di convergenza tra sicurezza fisica tradizionale e sicurezza logica va governato con equilibrio ed intelligenza. Il rischio è, da un lato, che il comparto della security tradizionale venga cannibalizzato dai colossi informatici, e dall'altro che le realtà ICT, attratte dalle marginalità della security fisica, perdano delle occasioni per mancanza di knowhow verticale. E' quindi essenziale che entrambi i comparti irrobustiscano le proprie competenze arricchendosi vicendevolmente, per creare sinergie profittevoli e durature.
Il tutto dovrà essere accompagnato da un approccio olistico alla sicurezza, detto di Security Convergence, che armonizzi competenze e responsabilità con una progressiva integrazione di processi, strumenti e risorse.
Da qui, l'idea di dar vita a IP Security Magazine, uno strumento di informazione altamente qualificato per traghettare il comparto sicurezza verso le opportunità della tecnologia IP e per indirizzare le realtà che si occupano di networking e IT. Uno strumento informativo che tiene il passo con le innovazioni di scena ad IP Security Forum, l'unica rassegna all-in-one di soluzioni, tecnologie e applicazioni per l'IP security al Nord e al Sud Italia. ■■

SOMMARIO

CONTENUTI VIDEO

CONTENUTI AUDIO

PHOTO GALLERY

IP Security Forum: la Puglia non tradisce le aspettative

LA PUGLIA polo tecnologico d'eccellenza per l'ICT non ha tradito le aspettative, affollando le sale congressuali di IP Security Forum e coinvolgendo un pubblico di operatori consapevoli del processo di convergenza tra sicurezza tradizionale e IP ed attenti alle evoluzioni tecnologiche e alle opportunità di business che si prospettano per il nascente comparto dell'IP Security.
Significative anche le presenze delle autorità locali e delle tante rappresentanze associative del comparto sicurezza e ICT, a testimoniare l'attenzione del territorio pugliese e dell'industria locale verso le iniziative di alta formazione

GUARDA IL TRAILER

professionale volte a promuovere la convergenza tecnologica, culturale ed operativa. Su questo tema erano essenzialmente incentrati tutti i lavori congressuali: dalle nuove prospettive tecnologiche alle possibili aree di rischio, dall'evoluzione della regola dell'arte alle scelte strategiche e di tendenza.

Il tutto rafforzato dai forti messaggi motivazionali di Mariella Pappalepore, alla guida del settore Terziario Innovativo e Comunicazione Confindustria Bari e BAT, di Giuseppe Gargaro (Presidente ASSISTAL), di Giovanni Sebastiano (Presidente del Distretto Produttivo dell'Informatica della Puglia) e di Giuseppe Mastronardi (Politecnico di Bari, Presidente di eBIS).

Molto apprezzate, infine, le relazioni dell'Avv. Valentina Frediani su privacy e installazione di videosorveglianza, come pure sulla tutela normativa del Cloud computing. Relazioni che facevano il paio con la lezione formativa sulle responsabilità Civili e Penali nell'installazione di impianti di sicurezza curata da Domenico Converso (Studio Legale Frediani).

Particolarmente riuscita, poi, la Tavola Rotonda dedicata al tema "Crisi della rappresentatività: quali conseguenze per la filiera della sicurezza?", che ha visto le associazioni del comparto sicurezza dialogare per la prima volta in un fronte unico con le rappresentanze di associazioni contigue o convergenti: dalla sicurezza informatica alla teleimpiantistica, dal mondo dei servizi e delle consulenze IT alle investigazioni private. Ma è stata la tecnologia la vera protagonista della giornata ed ha visto alternarsi relazioni e soluzioni presentate da Arteco Ivs, Beta Cavi, Bpg Radiocomunicazioni, Commend Italia, Digital System, Elp - Wolf Safety, Eurogroup, Indigovision, March Networks, Milestone Italia, Sir.tel, Trans Audio Video e Videotecnologie.

Lo scorso 27 ottobre si è quindi concluso con piena soddisfazione di organizzatori, pubblico ed espositori, riconfermando IP Security Forum come l'evento trainante per governare il cambiamento. ■■

Altri aggiornamenti su ***www.eventi.ethosmedia.it***

ASCOLTA

Intervista con
Domenico Favuzzi, Vice Presidente Vicario Confindustria Bari e B.A.T.

ASCOLTA

Intervista con
Giuseppe Gargaro, Presidente ASSISTAL

ISO/OSI, TCP/IP protocollo IP e soci:

mini introduzione alle reti interconnesse

OGNI GIORNO una quantità infi nita di dati attraversa i nostri computer, i nostri telefoni, le nostre automobili. Tutto è online e tutto ciò che utilizziamo, ogni singolo congegno connesso in rete, è parte di quell'universo che chiamiamo Internet. Per utilizzare un televisore, non dobbiamo certo conoscere il suo principio di funzionamento. Allo stesso modo, per usare un computer non dobbiamo essere dei programmatori. La tecnologia ci permette infatti di utilizzare le cose senza sapere nulla del loro funzionamento. Eppure ci sarà qualcuno che, seduto davanti al computer, si starà chiedendo come sia possibile che, nell'infinita complessità di Internet, ogni dato trasmesso raggiunga correttamente il suo destinatario. Ebbene, questi articoli sono dedicati proprio a chi ha la necessità, la curiosità o l'interesse professionale di sapere cosa succede quando apriamo Explorer e cominciamo a navigare. Partendo dai fondamentali (anche i più banali e scontati) arriverete col tempo a costruire un vero "manuale TCP/IP per autostoppisti"...dove finisce un allarmista e dove inizia un informatico.

Stefano Sacchini
Branch and product manager
Dime Sicurezza

COMINCIAMO con un concetto fondamentale: qualsiasi dispositivo (PC, server, tv, cellulare..) che abbia un'interfaccia di comunicazione è connesso in rete, la quale è parte di una rete, che a sua volta è parte di una rete...e così via. Quello che noi comunemente chiamiamo internet, non è un network globale in cui orbitano milioni di macchine, bensì è un insieme di reti tutte interconnesse tra di loro e potenzialmente completamente diverse tra loro. Ma allora com'è possibile che computer diversi che si trovino in reti diverse possano comunicare tra loro? La risposta è che tutti utilizzano le stesse regole di comunicazione, cioè gli stessi protocolli.

UN PO' DI STORIA

L'unificazione dei protocolli di comunicazione risale agli inizi degli anni '60, agli albori della guerra fredda. Gli Stati Uniti crearono l'Advance Research Project Agency (ARPA), un'agenzia con l'incarico di sviluppare una rete di comunicazione a prova di attacco nucleare. La necessità era di creare un sistema di comunicazione ridondante in cui, quand'anche fosse stata distrutta una base militare o una città che rappresentava un nodo della rete di comunicazione, i dati e le informazioni avrebbero dovuto trovare un percorso alternativo per giungere a destinazione. Nel 1968 la BBN fu incaricata dall'ARPA di sviluppare tale tecnologia. Ciò che fu concepito era un sistema cosiddetto a commutazione di pacchetto (pocket switching). In tale sistema i dati vengono incapsulati in pacchetti e inoltrati in rete. Sarà quest'ultima a stabilire il percorso che essi dovranno compiere fino al destinatario. La rete fu denominata ARPANET. Inizialmente era di dominio militare e interconnetteva cinque nodi. Nel 1972 i nodi erano già diventati trentadue e i professori universitari utilizzavano dei supercomputer, grandi quanto un armadio a quattro ante, per scambiarsi delle Email con connessioni di qualche Kb/s. Nel 1973 fu definito il TCP/IP, lo stack di protocolli su cui ancora oggi si basa l'interconnessione di rete globale: Internet.

TCP/IP, L'ILLUSTRE SCONOSCIUTO

Contrariamente a quanto si possa pensare,TCP/IP non è un protocollo di rete, ma un insieme di protocolli, ognuno dei quali opera indipendentemente e su livelli diversi. Ogni architettura di comunicazione ha almeno due interlocutori, mittente e destinatario, che sono denominati host, e una struttura di tipo gerarchico, dove i dati passano da un livello a un altro attraverso delle interfacce denominate Gateway. Immaginiamo che due direttori di due grandi aziende si trovino all'ultimo piano dei loro grattacieli. Il direttore A manda una lettera al direttore B. La lettera rappresenta il dato che vogliamo trasmettere e la procedura per spedire la lettera rappresenta il nostro protocollo di comunicazione. La lettera viene scritta dal direttore che la consegna alla segretaria (il suo gateway), che imbusta la lettera e inserisce la scritta "riservato". Poi la lettera viene passata all'ufficio corrispondenza, un altro gateway che vi appone sopra il mittente e il destinatario. Passa poi alla contabilità che la vidima e la consegna al postino. Come notate, la

Application	FTP, TELNET, RSH, RCP, RLOGIN, etc.
Presentation	
Session	
Transport	TCP
Network	IP
Data Link	Network
Physical Link	

nostra lettera è scesa di livello in livello fino a toccare quello più basso, il postino, per poi compiere lo stesso tragitto nel palazzo accanto, ma questa volta seguendo un percorso inverso. L'informazione digitale si muove su livelli che formano una struttura denominata ISO/OSI. I livelli sono sette: Fisico, Dati, Rete, Trasporto, Sessione, Presentazione, Applicazione (vedi tabella). TCP/IP occupa tre livelli della nostra torre: IP (internet protocol) si trova al livello più basso, quello della rete, il suo compito è di trovare la strada per arrivare a destinazione. TCP (trasmission control protocol) si trova a un livello superiore, quello del trasporto, ed ha un compito più "nobile": assicurare che l'informazione arrivi sana e salva. Infine troviamo i protocolli applicativi, quelli che si occupano di gestire una pagina web, un'Email o il download di un file.

IL PROTOCOLLO IP

Passiamo ora a parlare del livello più basso della nostra torre, in cui troviamo il protocollo IP. Affinché internet funzioni, ogni singolo PC connesso richiede un nome unico, in modo da non generare equivoci. Per fare in modo che ciò avvenga, il nome deve avere una struttura a gruppi e sottogruppi. Pensiamo agli stati, alle regioni, alle province e ai comuni. Posso identificare ogni singolo posto per via di un nome, e, quand'anche trovassi due vie con lo stesso nome, saprei che esse appartengono a due città differenti. La struttura di un indirizzo IP ricalca la stessa filosofia: è composto da quattro gruppi di otto bit; ogni gruppo può contenere 254 sottogruppi, e nel suo insieme identifica sia l'host, ovvero un computer connesso, che la sua rete di appartenenza. In base alla struttura che un indirizzo assume, esso viene associato a delle classi, che generalmente vanno da A a C. Ne deriva che in Internet ci sono 254 x 254 x 254 x254 indirizzi. In realtà non è così perché in ognuno di questi è possibile creare un numero indefinito di sottoreti. Questo significa che l'indirizzo non identifica un host, ma una connessione alla rete e noi non possiamo sapere (anzi, IP non sa e non è tenuto a saperlo) cosa si nasconde dietro quell'indirizzo.

AD ESEMPIO

Immaginiamo la struttura di un indirizzo IP: xxx.xxx.xxx.xx1. Se io sono xx1 e devo inviare dati ad un host, compilo la mia richiesta con il nome del destinatario e la lancio in rete. A quel punto IP controllerà se l'host destinatario si trova nel mio stesso segmento di rete. Se sì, il dato verrà inviato direttamente. Se invece il destinatario si trova in un diverso segmento, IP consegnerà la richiesta al suo gateway, il fatidico Router, affidando a lui il compito di trovare la rete di appartenenza. Ne derivano due considerazioni: la prima è che il protocollo IP non conosce il tragitto completo per giungere a destinazione (routing table) e deve solo sapere se il destinatario si trova nella sua sottorete. E indovinate chi dà questa informazione? La famosa quanto misconosciuta Subnet Mask. La seconda considerazione è che IP non ci dà alcuna garanzia che i dati arrivino a destinazione. Infatti spetterà al suo gateway cercare il destinatario, e non è detto che questo lo trovi. In tal caso, il router trasmetterà la richiesta a un altro gateway e così via. Ognuno conosce solo una parte del tragitto e nessuno dà garanzia della ricezione del destinatario. Si parla di Connectionless Pocket Delivery Service perché non è sempre possibile stabilire una connessione diretta
tra host mittente e host destinatario. È come mettere un messaggio in una bottiglia e gettarlo in mare sperando che le onde facciano il resto. Per sapere come viene garantita l'affidabilità delle comunicazioni dovremo aspettare di parlare del TCP, un protocollo che si trova ad un livello superiore e che gestisce l'integrità dei dati. Nella prossima puntata vedremo come IP agisce sui nostri dati per adempiere alla sua funzione. ■■

SiCUREZZA

7-9 NOVEMBRE 2012
Fiera Milano (Rho)

Biennale internazionale dei settori
antintrusione, rilevazione antincendio,
difese passive, home & building automation,
intelligence e antiterrorismo, prodotti e servizi
per forze di Polizia e Vigilanza Privata

www.sicurezza.it

FIERA MILANO

Fiera Milano SpA - Strada Statale del Sempione, 28 - 20017 Rho, Milano
Tel. +39 02 4997.6236 - Fax +39 02 4997.6252 - areatecnica1@fieramilano.it

Promossa da

ANIE SICUREZZA
SICUREZZA E AUTOMAZIONE EDIFICI

SICUREZZA ASSOSICUREZZA

In contemporanea con

LIFT

Soluzioni wireless ridondate

per l'Unione dei Comuni del Medio Verbano

STATO DI FATTO E SFI DA TECNOLOGICA

La Polizia Municipale presso l'Unione dei Comuni del Medio Verbano ha attivato con successo un sistema di videosorveglianza wireless delle aree comunali critiche realizzato con apparecchiature di ultimissima generazione. L'obiettivo era garantire al Corpo dei Vigili una copertura più uniforme del territorio grazie all'installazione di 50 telecamere collegate alla centrale operativa via radio, con l'ausilio di una rete wireless dedicata, che offre un elevato livello di sicurezza e ridondanza propria. L'esigenza di creare un'infrastruttura wireless è nata dalla necessità di realizzare un sistema a distribuzione capillare su un territorio ampio di più comuni, che non richiedesse interventi invasivi all'interno del singolo comprensorio comunale e che nel tempo potesse garantire larga espandibilità dell'impianto e l'eventuale condivisione di ulteriori servizi.

LA TECNOLOGIA MESSA IN CAMPO

SIR.tel. srl, società che opera da anni nel campo delle applicazioni wireless e video IP importando e distribuendo i migliori brand di settore e assistendo il System Integrator nella progettazione di sistemi complessi, si è adoperata nella pianificazione e progettazione di un sistema di centralizzazione video IP tramite collegamenti wireless atto a garantire, oltre che un ottimale collegamento dati, un elevato grado di stabilità della struttura network del sistema ed una facile espansione futura dello stesso. La piattaforma software di gestione video Genetec dedicata alla visualizzazione live, registrazione e gestione delle unità video, unitamente agli encoder MangoDSP, hanno conferito al sistema un'elevata qualità video ed un elevato frame rate delle immagini. Inoltre SIR. tel. ha realizzato ad hoc la piattaforma software NTG-Pro di monitoraggio e manutenzione telematica delle apparecchiature in campo completamente gestibile all'interno della stessa interfaccia utente di Omnicast, garantendo così una migliore e rapida gestione operativa del sistema. Le apparecchiature Infinet Wireless utilizzate per la rete radio hanno permesso di realizzare una rete wireless con tecnologia 2x2 MIMO con ridondanza hardware (doppia apparecchiatura radio) e gestione automatica dello scambio e della gestione del traffico senza router esterni di gestione, sia per le connessioni punto-punto di dorsale, sia per le connessioni multi-punto di raccolta, creando un'unica "Base Station Multipla" a copertura di un'intera area multicomunale. Questa soluzione garantisce un'espandibilità immediata fino a 450Mbps netti di traffico video (senza aggiungere hardware), o superiore al Gigabit aumentando il numero di apparati radio. Le soluzioni innovative sono molteplici: piattaforma software di gestione video Omnicast, a garanzia di infi nita espandibilità, ed integrazione verso terze parti; encoder Pegasus con intelligenza DSP a bordo che permette opzionalmente di installare on-board un plugin di video analisi del contesto senza richiedere hardware aggiuntivo; piattaforma software NTG-Pro di monitoraggio e telegestione per garantire riscontro immediato delle problematiche provenienti dal campo; tecnologia wireless 2x2 MIMO per multi-punto/punto-punto e ridondanza hardware Layer3 per un'assoluta scalabilità del sistema, ridondanza automatica sulle radio. E' la tecnologia 2x2 MIMO proprietaria di Infi net la peculiarità che ha permesso di creare un'infrastruttura di rete wireless che

VIDEO

Intervista con
Francesco Campanini, Sales Engineer di SIR.tel.

assicura nel tempo tre aspetti importanti: assoluta scalabilità; elevata effi cienza nelle connessioni punto-Multipunto; elevato throughtput netto. La scalabilità è garantita dalla possibilità di upgradare le unità esistenti mediante licenza software che ne regolamenta le prestazioni. Tale possibilità risulterà fondamentale laddove siano previsti ampliamenti o integrazioni con nuovi siti di espansione; ad esempio ad un link o una base station che oggi garantisce un throughput netto di 80Mbps, ma che in futuro, in seguito all'inserimento di nuove telecamere, dovrà garantire ulteriori 40 Mbps di banda disponibile (120Mbps di throughput netto in totale). Semplicemente eseguendo un upgrade di licenza (caricando un semplice file) si evita la sostituzione degli apparati ottenendo un aumento delle prestazioni a costi estremamente contenuti. Altro aspetto importante è l'effi cienza dei link wireless punto-multipunto introdotta da Infi net, con il suo metodo proprietario di "Dynamic Marker Access". Impiegando tale gestione, una Base Station autorizza la trasmissione dei dati delle CPE inviando un "token" ("marcatore"), in cui viene specifi cato il massimo intervallo di tempo che ha a disposizione per trasmettere e ricevere dati. Questa gestione evita la sincronizzazione GPS degli apparati, semplifi candone il funzionamento e l'uso. Si noti che le informazioni contenute nel token sono di tipo dinamico (cioè variano nel tempo a seconda delle esigenze delle CPE). Il Dynamic Marker Access permette di usufruire dei seguenti vantaggi principali: riallocazione dinamica Uplink/Downlink; velocità delle ritrasmissioni in caso di pacchetti non ricevuti; performance migliori (rispetto al TDMA) in condizioni di interferenza; basso sovraccarico del protocollo di gestione. Ulteriore benefi cio della tecnologia 2x2 MIMO propietaria di Infinet è l'elevato aumento dell'efficienza spettrale dei link wireless, che permette di ottenere un throughtput radio di 300Mbps (senza aggregazione) contro i 54Mbps dei classici sistemi OFDM, gestito poi nel network tramite porta Ethernet Gigabit. E' inoltre possibile usufruire delle funzionalità di Virtual LAN per separare a livello logico le reti presenti all'interno dello stesso mezzo fisico (video/VoIP/etc) e la combinazione con dispositivi di networking fi no a Layer 4 supporta inoltre la discriminazione del traffi co di provenienza e di destinazione, permettendodirettamente sulle dorsali wireless la gestione della priorità sulla base di policy di traffico. ■■

Per approfondimenti: www.sirtel.it

IP Security Forum

Semplicemente, grazie

Ethos Media Group ringrazia tutte le aziende, le associazioni e le persone che hanno contribuito al successo di IP Security Forum 2011

MEDIA PARTNER

www.ethosmedia.it - www.eventi.ethosmedia.it

Non è tutto ORO quello che è CLOUD

Pietro Cecilia
Esperto di networking e security,
Amministratore unico
Tsecnet (www.tsecnet.com)

I server reali gestiti dai cloud provider sono generalmente "progettati" per essere scalabili e altamente affidabili,così come le strutture che fisicamente li ospitano in appositi "data center", i quali possono essere in Italia o in qualsiasi altro paese del mondo e ciò potrebbe avere un impatto negativo nei confronti della fornitura di servizi di videosorveglianza. Ma quali sono tali servizi?
Il mondo della videosorveglianza è cambiato molto negli ultimi 15 anni. Dai vecchi sistemi analogici con i mitici registratori VHS si è passati ai videoregistratori digitali DVR, alle ultime soluzioni completamente digitali basate su sistemi IT. Il cloud computing sembrerebbe quindi essere la panacea per i servizi di videosorveglianza, o almeno per quelli che adottano sistemi completamente IT,

Intervista con
Valentina Frediani, esperto di diritto informatico

ma in realtà non è così o almeno non per tutti.
Attualmente il target è costituito dal cliente residenziale o dalla piccola/media impresa, che hanno strutture/aree da controllare con numero un limitato di telecamere e/o geograficamente distanti. I servizi disponibili sono:

1. Videosorveglianza (il software fornito come servizio)
2. Storage (quantità dei dati e tempo di archiviazione)
3. Video analisi (software/applicazione)

Un tipico esempio vede le telecamere (tipicamente IP) installate presso il cliente, collegate tramite ADSL alla rete internet e da qui alla "nuvola". Ovviamente il cliente può collegare più siti remoti alla stessa "nuvola" e usufruire dei servizi di archiviazione dei "suoi" dati, della visualizzazione da remoto delle immagini delle telecamere, nonché può ricevere - tramite PC, smartphone, ecc - gli allarmi generati dalle applicazioni di analisi video.
Esiste un'interessante applicazione antitaccheggio per i supermercati. In questo caso il provider fornisce una parte importante di analisi video specializzata nella funzione "antitaccheggio". Il servizio prevede l'installazione di telecamere presso il supermercato/negozio, le quali, collegate in rete ad un speciale "video server", fanno una prima analisi delle immagini, mentre la parte più "importante" dell'analisi video e "specializzata nell'antitaccheggio" è inviata al Cloud provider. Quest'ultimo fornisce in "tempo reale" al gestore del supermercato l'indicazione di eventuali situazioni anomale. L'applicazione è ancora più interessante se il servizio viene fornito dallo stesso cloud provider ad un numero elevato di supermercati geograficamente distanti tra loro.

PROBLEMA 1: NETWORKING

E' vero che con il cloud provider il cliente paga solo ciò che usa, che ha minori costi di energia elettrica, che ha meno fonti di calore in aree non adatte a gestirle (case, magazzini, negozi, etc) e minori costi di manutenzione, ma in realtà non è tutto positivo e ci sono tanti punti interrogativi e rischi nel cloud computing della videosorveglianza. Il primo, ma non per importanza, è quello tecnico e di prestazioni legato direttamente al networking e all'internet service provider utilizzato per l'accesso alla rete. Infatti il numero delle telecamere che possono essere collegate dipende dalla linea ADSL e, anche sfruttando il protocollo di compressione H264, il nu-

mero di telecamere che possono essere collegate alla rete è sicuramente non elevato e dipende comunque dalle prestazioni e dalla qualità dell'ADSL. In particolare quest'ultimo parametro è determinate nella fornitura del servizio del cloud provider, giacché tutto nasce dal segnale sorgente (del cliente), che deve essere privo di errori e stabile perché qualsiasi "errore" del segnale in partenza, che non sia generato da eventi "esterni", potrebbe essere scambiato per allarme, generando la psicosi dei falsi allarmi - che rappresenta uno degli elementi più fastidiosi per i clienti. Si potrebbe addirittura avere un cloud provider tecnologicamente all'avanguardia, ma avere un servizio globale scadente, se la qualità del segnale sorgente è bassa.

PROBLEMA 2: PRIVACY

Il secondo punto interrogativo riguarda l'aspetto regolatorio e le norme che i gestori dei sistemi di videosorveglianza sono tenuti ad osservare, in particolare quelli legati alla sicurezza dei dati e alla privacy. Usufruire di un servizio di cloud storage per la memorizzazione dei dati, in particolare per quelli personali o sensibili, può esporre il cliente a potenziali problemi di violazioni della privacy. Infatti i dati personali del cliente, o delle immagini registrate dal sistema del cliente, vengono di fatto affidate ad un soggetto terzo, con tutte le implicazioni del caso. E questo è tanto più critico se il soggetto terzo risiede all'estero, dove la legislazione che regolamenta la gestione dei dati personali e sensibili non è così evoluta come quella italiana, o quantomeno è diversa, quindi il provider potrebbe gestire tali informazioni secondo la legislazione del paese in cui sono localizzati fisicamente i data center. Questa doppia modalità di "trattamento" dei dati sensibili potrebbe creare seri problemi in fatto di privacy.

CONSIGLI PER GLI ACQUISTI

Ai clienti che vogliono utilizzare il cloud computing suggeriamo quindi di avvalersi di specialisti che possano effettuare le attività tipiche di progettazione e fornitura di un sistema che sia in linea con le aspettative di costo del cliente e con tutte le normative vigenti in fatto di privacy e sicurezza dei dati. Una particolare attenzione va rivolta al contratto, agli SLA (Service Level Agreement), alla qualità tecnica e dei servizi, nonché alla stabilità economica del cloud provider. Il cloud computing, secondo i guru delle previsioni di queste tecnologie (vedi IDC e Gartner group), avrà un futuro molto roseo con tassi di crescita importanti (a due cifre). Gli analisti sostengono anche che le nuove tecnologie, compreso il cloud storage, faciliteranno l'acquisto dello spazio e della CPU virtuale, andando a indirizzare soprattutto i problemi di sicurezza.
In conclusione, si può dire che il cloud computing è un servizio prevalentemente per le aziende che vogliono usufruire di servizi IT, ma soltanto in piccola parte dedicato alle aziende che vogliono servizi di videosorveglianza. Alla luce però di quanto successo nel passato, non è difficile ipotizzare per i servizi di videosorveglianza forniti tramite cloud computing una crescita per il futuro, ma se e solo se i cloud provider sapranno anticipare i tempi e fornire nuovi servizi/tecnologie più mirati alle esigenze tipiche della videosorveglianza. ■■

ANNO 1 – Numero 1 – dicembre 2011
Direttore responsabile
Andrea Sandrolini
Coordinamento editoriale
Ilaria Garaffoni
redazione@ethosmedia.it

Direzione Commerciale
Roberto Motta
motta@ethosmedia.it

Ufficio Traffico
Carolina Pattuelli
pattuelli@ethosmedia.it
tel. +39 051 0475136

Ufficio estero
international@ethosmedia.it

Pubblicità
Ethos Media Group srl
ethos@ethosmedia.it

Sede Legale
Via A. Manzoni 35 – 20900 Monza (IT)
Direzione, redazione, amministrazione
Ethos Media Group srl
Via Paolo Fabbri, 1/4 – 40138 Bologna (IT)
tel. +39 051 0475136
Fax +39 039 3305841
www.ethosmedia.it

Registrazione
Tribunale di Bologna al n° 8218
del 28/12/2011 - Dicembre 2011

Iscrizione al Roc
Ethos Media Group s.r.l.
è iscritta al ROC
(Registro Operatori di Comunicazione)
al n. 19315 del 2 marzo 2010

Periodicità - Mensile

Grafica / impaginazione
Lisa Cavallini

Ethos Media Group sr.l è associata ad ANES

a&S ITALY

Tecnologie e soluzioni per la sicurezza professionale

www.asitaly.com

A&S Italy, la forza del gruppo

A&S Italy è la rivista di riferimento in Italia sulle tecnologie e le soluzioni per la sicurezza professionale. **A&S Italy** è un prodotto editoriale assolutamente nuovo e originale, con un approccio né globale né locale, ma glocal.

Al mercato italiano della security serviva una sferzata propositiva, un'idea dirompente che permetta al settore di ingranare la quinta e manifestare tutto il suo potenziale non solo in Italia, non solo in in Europa, ma su tutti i mercati più interessanti. In questo processo, un editore che sta dalla parte degli operatori – un partner – deve preparare il terreno al proprio mercato, deve tirargli la volata per fargli tagliare traguardi sempre nuovi.

Da questa intuizione nasce **A&S Italy**, il brand globale della security con l'anima italiana.

La forza distributiva, la capacità di penetrazione e l'autorevolezza di un brand leader a livello globale si sposano in **A&S Italy** a quella miscela di passione, capacità, esperienza e knowhow che possiedono solo le persone – le anime – che vivono questo mercato da più di 20 anni.

A&S Italy, il brand globale della security con l'anima italiana.

ETHOSMEDIAGROUP

www.ethosmedia.it

Ethos Media Group srl – Via Manzoni, 35 – 20052 Monza (Italy) – Fax +39 039 3305841 – ethos@ethosmedia.it