DICEMBRE 2013 - ANNO 3 N. 9

ETHOSMEDIAGROUP
GLOBAL MULTIMEDIA CHANNEL

IP Security MAGAZINE

TECNOLOGIE, SOLUZIONI E APPLICAZIONI PER L'IP SECURITY

Cloud o non cloud? Questo è il dilemma

La piazza in movimento di *IP Security Forum* salpa nel capoluogo emiliano

Datacenter sicuri grazie agli UASG

UNI: una nuova norma contro gli eventi destabilizzanti

www.ipsecuritymagazine.it

SOMMARIO

ETHOSMEDIAGROUP
GLOBAL MULTIMEDIA CHANNEL

IP Security MAGAZINE

TECNOLOGIE, SOLUZIONI E APPLICAZIONI PER L'IP SECURITY

DICEMBRE 2013 - ANNO 3 - N. 9

guarda ascolta scarica

La convergenza prende corpo...editoriale

L'avevamo promesso quando abbiamo dato vita a questa testata e oggi, grazie anche agli importanti contributi in materia pervenutici dal *festival ICT*, possiamo cominciare a metterlo in pratica. Parliamo della famosa *convergenza culturale* tra sicurezza fisica e sicurezza logica, ossia di quel cambio di paradigma che impone ormai una doppia formazione a chiunque si occupi a vario titolo di *security* - sia essa intesa in senso *fisico* (soluzioni e dispositivi che minimizzano l'intrusione fisica ad un luogo asset), sia essa intesa in senso *logico* (per prevenire sottrazione o attacchi all'integrità dei dati). In entrambe le accezioni, è necessario procedere a cerchi concentrici.
Nella sicurezza informatica si deve partire dalla realizzazione fisica di reti ridondate che impediscano le connessioni non autorizzate, per poi passare attraverso un'adeguata ridondanza passiva, ed infine giungere alla security a livello di apparati attivi e software. Analogamente, la security fisica deve essere implementata partendo dalla protezione perimetrale outdoor e indoor, per poi inoltrarsi al controllo degli accessi e infine alla sensoristica e allarmistica interna all'area da proteggere. Analogie tra materie di confine che diventano sempre più palpabili da quando la sicurezza fisica, con la videosorveglianza in testa, ha cominciato a viaggiare su IP, portandosi in dote tutti i vantaggi – ma anche tutti i rischi - di questa illimitata autostrada.
L'IP è quindi l'anello di congiunzione tecnologico tra tematiche di per sé già affini per obiettivi, modalità operative e rilevanza quali elementi di reale abilitazione del business aziendale.
IP Security Magazine si è da subito prefissata l'obiettivo culturale di traghettare il mondo della sicurezza fisica tradizionale verso le opportunità, ma anche le problematiche, della sicurezza logica. In questo numero molti contributi di area IT danno testimonianza ed evidenza di questo obiettivo.
A voi giudicarne il valore.

Il successo della tua attività dipende dal tuo costante impegno negli affari. Per la sicurezza è meglio affidarsi a FGS che da oltre 25 anni opera nel settore, progettando, installando e assistendo Sistemi di Sicurezza Integrati "chiavi in mano" ad alta tecnologia, realizzati su misura per le tue esigenze.

www.fgs-impianti.it

FGS

Sistemi Integrati per la Sicurezza

VIDEOSORVEGLIANZA | ANTIFURTO | ANTINCENDIO | CONTROLLO ACCESSI

UNI: una nuova norma per rispondere agli eventi destabilizzanti

Intervista con Adarosa Ruffini(*)

Un modello di interazione tra soggetti pubblici e privati per reagire efficacemente agli eventi "destabilizzanti", in qualsiasi scenario sociale essi si verifichino. Questa la ratio dello standard messo a punto dalla Commissione UNI "Sicurezza della società e del cittadino" e confluito nella norma 11500:2013, che fornisce una guida per elaborare accordi di partenariato tra organizzazioni pubbliche e/o private. Con due elementi di unicità: la posizione di leadership italiana nella normazione convenzionale pattizia in un campo cruciale per la società moderna e il fatto che sia una donna a relazionare: la Prof.ssa Adarosa Ruffini.

Siete partiti qualche anno fa dall'istituzione di una Commissione per la Sicurezza della Società e del Cittadino in seno ad UNI e siete arrivati - a tempo record, direi - alla norma 11500.
Di cosa tratta la norma, quali problematiche risolve e a quali interlocutori si riferisce?

La costituzione della Commissione Tecnica U63 "Sicurezza della Società e del Cittadino" ha rappresentato la performante risposta di UNI (Ente Nazionale di Unificazione) ad un processo di globalizzazione che ha sempre più amplificato l' insicurezza percepita dal singolo e dalla collettività al verificarsi di catastrofi, atti terroristici, calamità naturali, crisi finanziarie ed incidenti industriali.
Per fronteggiare gli scenari di crisi generati da tali eventi destabilizzanti era necessario predisporre "*fossati normativi*" di prevenzione, pianificazione e gestione.
Citando una frase del suo Presidente Ing. Ivano Roveda, che ne circoscriveva il *framework* e superava la dicotomia fra *Safety & Security* suggerendo di definire la sicurezza *intrinseca* ed *estrinseca* a seconda che si contrapponesse ad un rischio interno od esterno allo scenario considerato, "*stabilire le linee strategiche e strutturali della Commissione rappresentava una sfida concettualmente ed operativamente stimolante per le sue valenze e ricadute sul mercato, sulla collettività e sui singoli, fossero essi operatori o meno*".

(*) Adarosa Ruffini è Docente della Facoltà di Ingegneria dell'Università di Pisa e Membro della Commissione UNI "Sicurezza della società e del cittadino" e relatrice della nuova norma UNI 11500:2013 che fornisce una guida per elaborare accordi di partenariato tra organizzazioni pubbliche e/o private.

L'esigenza che le norme, tanto mandatorie o cogenti quanto convenzionali e pattizie, fossero predisposte non solo in riferimento agli impatti e alla loro invasività ma che dovessero garantire la sicurezza dei cittadini quali utenti finali di un processo complesso di ripartizione del rischio, con attribuzione di varie tipologie di responsabilità tra gli operatori, ha suggerito quindi di predisporre forme di cooperazione che creino oggi scenari di partecipazione diffusa e siano pronte all'adozione di misure conservative e riparatorie che conducano al ripristino di condizioni giudicate accettabili da tutte le parti coinvolte. Lo standard UNI/11.500 stabilisce le linee guida per elaborare accordi di partenariato tra diverse organizzazioni coinvolte, pubbliche e private, che devono fronteggiare eventi destabilizzanti prima, durante e dopo il loro verificarsi e costituisce il primo accreditamento di una nuova norma riferita espressamente ad una dimensione collettiva della società qualificata dai principi del coordinamento e della cooperazione reciproci.

Nella norma sono standardizzati solo modelli funzionali-relazionali o è previsto anche l'impiego di tecnologie di sicurezza?

Il modello che sottende lo standard denominato "*Modello di relazione strutturata di Partenariato*" affronta in modo scientifico il problema delle relazioni tra soggetti, od entità, di diversa natura giuridica allo scopo di pervenire ad obbiettivi condivisi e nell'interesse di ciascuna delle parti coinvolte. Costituisce quindi uno strumento innovativo, stabile ma flessibile ad un tempo, di rapido adattamento alle esigenze di tutte le parti interconnesse e si orienta verso specifiche finalità di sviluppo contemperando cooperazione e competizione. Per le implicazioni dirette che ne derivano agli operatori economici interessati, pur essendo il modello uno schema definito di relazioni strutturate, favorisce la standardizzazione e l'uniformità anche delle tecnologie utilizzate, soprattutto sotto il loro profilo funzionale.

Nella sua relazione, ha accennato più volte al ruolo del soft low e alla sua integrazione con il diritto cogente, tra l'altro utilizzando l'espressione "normazione convenzionale pattizia" e non la più comune "normazione tecnica volontaria".
Perché? Cosa significa "diritto dolce"?

Partiamo da una considerazione: le nuove esigenze del mercato globalizzato e gli attuali momenti di grave congiuntura, soprattutto economica, hanno suggerito non solo un'attenta revisione delle tradizionali figure imprenditoriali, ma hanno anche orientato le scelte normative e contrattuali verso una nuova dimensione collettiva per lo sviluppo e la crescita complessivi.

Tali valutazioni hanno orientato l'ossatura di una nuova forma di diritto, quello dei tecnici, nel quale la funzione della normazione integrata (tanto mandatoria e cogente quanto convenzionale e pattizia) e del contratto hanno creato una sorta di *soft low* molto flessibile, idoneo a veicolare l'indistinto e mutevole conformarsi dei legami economici, e non, fra le entità implicate.

Riferite ad una consuetudine normativa già da tempo applicata e ad un chiaro disegno di politica legislativa che le preceglieva per garantire l'adeguamento allo "stato dell'arte" in continua evoluzione perché direttamente collegato alla ricerca e allo sviluppo tecnologico, le cosiddette *norme tecniche* prodotte dagli Enti di Normazione hanno contribuito inizialmente ad uniformare le tipologie della produzione e degli scambi in aree geografiche di carattere multinazionale.

Produzione e scambi che non sarebbero stati sufficientemente tutelati, qualora ad essi si fossero applicate unicamente le norme cogenti dei singoli Stati.

Attualmente, la negoziazione e la concertazione - che hanno fatto della normazione convenzionale e pattizia un potente strumento di *governance* che ha contribuito alla creazione di un impianto normativo comune ed integrato in cui le differenti parti hanno potuto instaurare una reale cooperazione e collaborazione - hanno reso possibile, attraverso l'attuazione dei principi di coerenza equità, integrità, correttezza e trasparenza, l'eccellente e virtuosa attuazione delle condotte strutturate che intercorrono tra i vari soggetti interessati.
La circostanza che tali regole siano state e continuino ad essere effettivamente osservate le ha qualificate quali norme riconducibili al "*principio di effettività*" e, come tali, *giuridiche* a tutti gli effetti e ne ha esteso l'applicazione ben oltre l'iniziale contesto tecnico.
A mio parere, lo scenario che il mondo italiano della normazione volontaria si trova attualmente a dover fronteggiare, e gestire, può essere infatti sinteticamente riassunto in tre distinte configurazioni:

a) la prima, di più ampio respiro legislativo, nella necessità di offrire un adeguato presidio normativo alla rappresentanza delle istanze normative sui tavoli europei ed internazionali, nonché nella finalità di raccogliere richieste e suggerire nuovi paradigmi di regolazione ad ogni soggetto esponenziale di interessi meritevoli di tutela;

b) la seconda, nella necessità di dover garantire all'impresa italiana, all'interno di un chiaro disegno di strategia industriale del Sistema paese, risposte adeguate di crescita e sviluppo a livello internazionale ed europeo per quanto riferito alla competitività, alla parità di trattamento, alla concorrenza e trasparenza, nonché di dover offrire un concreto sostegno alle piccole e medie imprese italiane, posto che l'Europa stessa ha posto l'accento anche sul collegamento necessario tra la microazienda ed il suo alto livello occupazionale;

c) la terza, di assicurare un complesso di riferimenti normativi che, riferiti al soddisfacimento degli interessi della collettività degli utenti e della complessiva offerta dei servizi, estenda su base volontaria anche l'attività certificativa, ben presente ed incisiva nel rapporto *business to business,* anche al rapporto *business to consumer*, e ciò al fine di favorire la sorveglianza attiva del consumatore alla corrispondenza alle performance richieste ed attese dei beni, dei servizi e delle prestazioni.

Questa norma, che peraltro è allo studio anche a livello internazionale, attribuisce una forte leadership italiana nella normazione convenzionale pattizia, in un campo per giunta cruciale e determinante per qualsiasi società.
Per una volta è l'Italia a fare da ente normatore pilota? E questo varrà anche in seno alla competente commissione ISO?
Lo standard ISO/ 22397 (di cui sono relatori Ivano Roveda, Capo della Delegazione Italiana e la sottoscritta), in via di redazione finale nel TC 223 Societal Security, accrediterà a livello internazionale le stesse linee guida dello standard UNI/ 11500, uniformando le regole di definizione delle relazioni intercorrenti tra le varie entità che intervengano sinergicamente prima, durante e dopo il verificarsi di ogni tipologia di evento destabilizzante.

La sicurezza, lo ha ribadito più volte nella sua relazione, non è che il punto di partenza dei modelli definiti e standardizzati in questa norma.
A quali altri scenari si possono applicare i modelli definiti nella UNI 11500?

Il coordinamento e la gestione delle attività che coinvolgono entità diverse, ciascuna titolare di funzioni differenti e di proprie procedure, ha da sempre manifestato elevati gradi di criticità.
Ciò in quanto l' approccio che tradizionalmente è stato utilizzato per il coordinamento delle funzioni attribuite per competenza istituzionale e legale a ciascuno dei soggetti attuatori ha quasi sempre generato realtà operative fortemente gerarchicizzate, difficili da integrare all'interno di un unico contesto.
Il più evidente limite concettuale di questo approccio è stato quello di considerare il livello di coordinamento superiore del soggetto attuatore unicamente quale risultato della raccolta delle informazioni e delle decisioni già assunte al suo livello inferiore e di non prevedere il confronto di tali informazioni e decisioni tra tutti i soggetti interessati, quale che sia il livello in cui le stesse siano state assunte e vengano concordate.
Inoltre, un altro aspetto problematico ai fini dell'attuazione di una soddisfacente integrazione, è dato dalla modificazione, totale e/o parziale, delle tecnologie utilizzate dai diversi soggetti potenzialmente interessati, con la conseguenza dell'obbligo per le entità realmente coinvolte dell'accollo di rilevanti costi per l'acquisto di nuove dotazioni.
Il nostro Modello, a contrario, tiene conto da un lato della necessità di rendere interattivi e dinamici i processi di gestione, e dall'altro garantisce il coordinamento dei soggetti attuatori attraverso la regolamentazione delle loro relazioni.
Abbiamo già detto di come le relazioni di Partenariato si sostanzino nella previsione di un insieme strutturato di accordi che impegnano le parti coinvolte nella precisazione di criteri che consentano di stabilire l'obiettivo ottimale per tutti i contraenti dell'accordo, la determinazione di regole per l'instaurazione e lo sviluppo della relazione, l'individuazione degli strumenti per il controllo e la verifica del rispetto degli accordi definiti.
Strutturare queste relazioni con un modello predefinito, e normativamente accreditato, ha quindi conseguenze sul funzionamento e sullo sviluppo della società, in realtà su tutti gli eventi definiti destabilizzanti, in qualsiasi scenario (sociale, politico, economico etc...) gli stessi si verifichino.

VIVOTEK

Il Vostro Esperto in Videosorveglianza IP

VIVOTEK INC.

VIVOTEK INC. (TAIEX: 3454). Fondata a Taiwan nel 2000, l'azienda è cresciuta rapidamente fino a diventare un brand prestigioso nell'industria della security. Conosciuta per la propria linea di soluzioni IP di grande qualità, VIVOTEK offre prodotti a prova di futuro e decisamente affidabili, rendendo allo stesso tempo più facile la transizione dalla TVCC tradizionale alla sorveglianza completamente IP. La sua vasta gamma di prodotti include telecamere network, server video, NVR e software per la gestione centralizzata.

Oltre 150 distributori autorizzati in più di 80 paesi garantiscono la disponibilità dei prodotti a dealer del settore security e telecomunicazioni, nonché ai system integrator che li scelgono per numerose applicazioni e progetti: dal settore bancario a quello della videosorveglianza urbana, negli hotel, nei trasporti, nel retail e in tanti altri contesti.

VIVOTEK
www.vivotek.com

VIVOTEK INC.
6F, No.192, Lien-Cheng Rd., Chung-Ho, New Taipei City, 235, Taiwan, R.O.C. | **T**: +886-2-82455282 | **F**: +886-2-82455532 | **E**: sales@vivotek.com

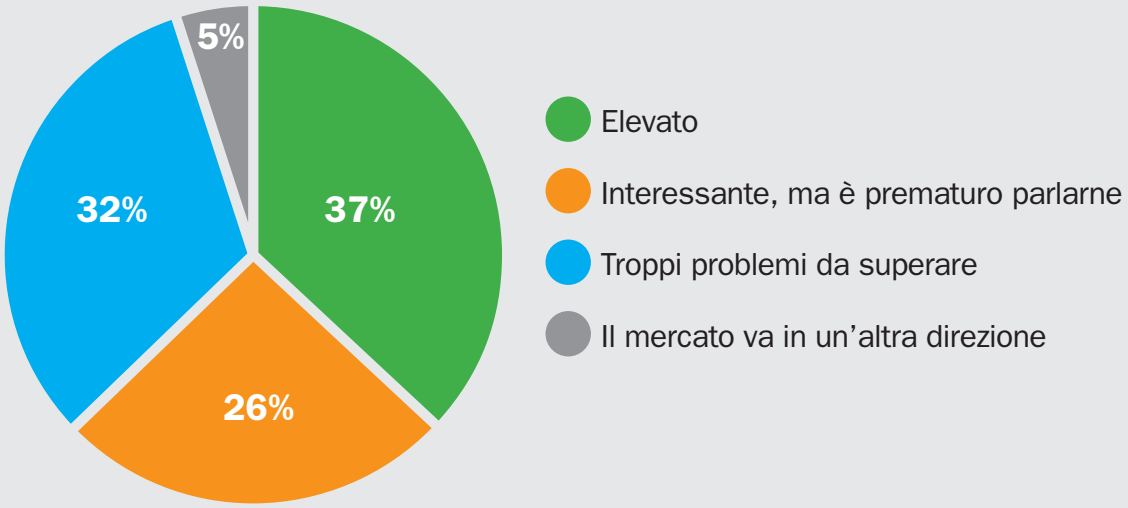
La Redazione

Cloud o non cloud? Questo è il dilemma...

Cloud o non cloud? Questo è il problema...
La "nuvola" informatica, che sta trovando interessanti applicazioni nel mondo della security, suscita reazioni contrastanti tra gli operatori. C'è chi la ritiene la tendenza più promettente dei prossimi anni e chi, al contrario, pensa sia prematuro anche solo parlarne. Le potenzialità ci sono – basti pensare agli incrementi di efficienza e al miglioramento della gestione operativa – ma i problemi da risolvere non mancano: alle questioni legate alla privacy e alla sicurezza delle informazioni, in Italia si sommano la carenza delle infrastrutture disponibili e l'inadeguatezza della normativa. Per saperne di più, abbiamo coinvolto i player del settore.

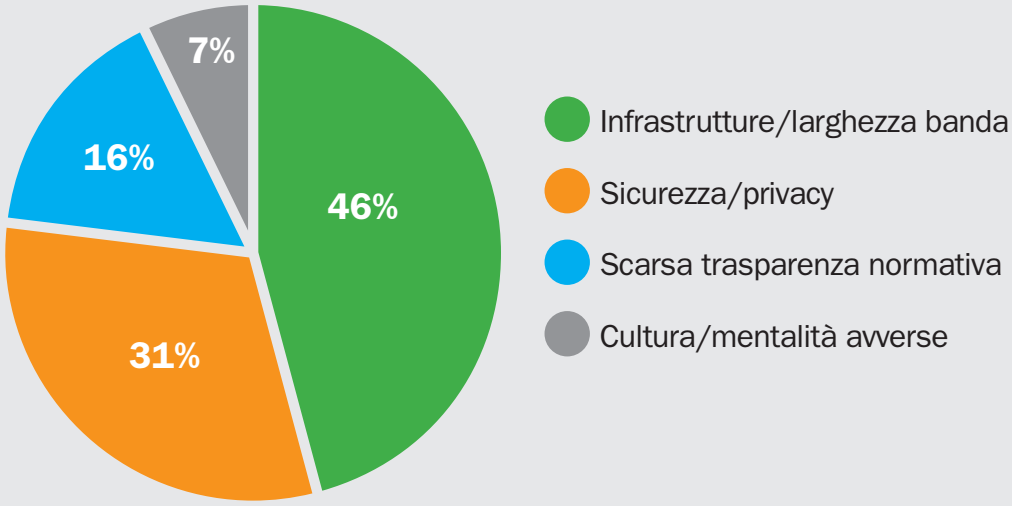
Negli ultimi anni la tecnologia cloud, che in Italia conosciamo anche come "nuvola informatica", sta richiamando un interesse sempre maggiore a livello internazionale. Una considerazione che vale anche per il settore sicurezza, nel quale le sue numerose applicazioni – dalla videosorveglianza (VSaaS), al controllo accessi (ACaaS), fino al Video Management System/ Software as a Service (SaaS) – stanno conquistando consensi via via più ampi.

IL POTENZIALE DELLA VSAAS E DELLA VCA CLOUD-BASED



A dare una valutazione positiva della tecnologia cloud è **IHS**/IMS Research. Secondo le stime del noto istituto di ricerca, nel 2011 la videosorveglianza as a service ha fatturato globalmente circa 500 milioni di dollari (+25% rispetto al 2010) e, se le tendenze in atto dovessero essere confermate, questo mercato potrebbe valere più di un miliardo entro il 2014. Questo, secondo l'analista **Sam Grinter**, "è il risultato della crescente domanda da parte degli utenti, delle piccole e medie imprese e degli enti governativi". Un'analisi confermata anche da **Access Markets International** (AMI) **Partners**, secondo la quale l'incidenza della nuvola sulla spesa globale in sicurezza delle piccole e medie imprese, che oggi rappresenta il 17%, potrebbe raggiungere il 24% entro il 2016. IHS prevede inoltre che nei prossimi anni l'applicazione alla videosorveglianza del cloud privato – che si distingue da quella pubblico per l'accesso ristretto dalla presenza di un firewall – si confermerà come un trend di grande importanza. Altre opportunità sembrano legate al VMS cloud-based (**Illy Gruber** di **NICE Systems** lo indica come uno dei trend più importanti soprattutto per le piccole imprese, alle quali permette un significativo abbattimento dei costi) e all'ACaaS (access control as a Service), che secondo IHS offre molte più opportunità – in termini di fatturato aggiuntivo e quota di mercato conquistabile – rispetto al controllo accessi tradizionale. Anche **Pierre Racz**, CEO di **Genetec**, ha indicato nelle soluzioni cloud la "tendenza più promettente" di questi tempi. Non a caso la multinazionale canadese ha lanciato una soluzione VSaaS che si avvale del supporto della piattaforma cloud-computing Windows Azure di Microsoft per "offrire alle PMI la massima affidabilità senza la complessità e i costi tradizionalmente associati all'installazione e alla gestione di sistemi di sorveglianza in loco". Obiettivo che riassume efficacemente uno dei punti di forza della nuvola: migliorare e semplificare la gestione operativa aumentando l'efficienza. Promozione a pieni voti, dunque? La risposta non è così scontata. Soprattutto se la dobbiamo contestualizzare nel nostro paese. Per chiarirci e chiarirvi meglio le idee, nel corso dell'ultimo anno abbiamo raccolto il parere dei player del mercato italiano. Ne è emerso un quadro assai composito, dove all'entusiasmo e all'ottimismo si affiancano dubbi e perplessità.

CLOUD: QUALI I PRINCIPALI PROBLEMI DA SUPERARE?



SECURITY CLOUD BASED: I FIDUCIOSI

Alcuni intervistati sembrano riporre fiducia nelle potenzialità del cloud computing. È il caso di **Alberto Vasta (Mobotix)**, secondo il quale la nuvola offre "centinaia di possibili e impalpabili applicazioni che saranno la nuova frontiera anche della videosorveglianza". **Denis Pizzol (Hikvision Italy)** è dello stesso parere, e ritiene che il cloud sia "un'importante opportunità legata al mondo delle tecnologie digitali e al networking in generale". La nuvola potrebbe inoltre garantire una "convergenza più veloce dall'analogico al digitale, perché semplifica ciò di cui molti installatori hanno timore ma al contempo bisogno: il know-how tecnologico su IP". A sostenerlo è **Francesco Paradiso (D-Link Mediterraneo)**, che sottolinea come attraverso questa tecnologia anche un installatore con una scarsa conoscenza di networking possa installare una soluzione su IP e renderla sicura: "Il cloud protegge infatti i sistemi di videosorveglianza attraverso l'HTTPS, il protocollo di sicurezza per la trasmissione dei contenuti sul web". **Andrea Natale (Tyco ADT Fire & Security)** vede invece grandi potenzialità di sviluppo soprattutto nel Software as a Service (SaaS), dove il cliente vede e usa solo un'interfaccia web. Un giudizio espresso, nelle parole dello stesso Natale, "in funzione dell'odierna difficoltà di accesso al credito, della volontà di investimento da parte dei clienti in impianti non legati alla propria attività, delle risorse necessarie per gestire impianti sempre più IT, della possibilità di avere un installato base sempre funzionante e aggiornato e della fruizione delle informazioni in mobilità".

SECURITY CLOUD BASED: I PERPLESSI

Nonostante gli evidenti vantaggi, la nuvola suscita anche diffidenza e scetticismo. "Parlare di security su base cloud fa un po' paura per tutte le implicazioni che la delocalizzazione della gestione/registrazione/analisi può avere", ci ha detto **Luigi Brambilla (Project Automation)**. "I sistemi di comunicazione, oltre che a offrire alte prestazioni, devono essere sicuri e avere funzioni di alta disponibilità garantita, non solo in termini di banda, ma anche di disponibilità del servizio". Da questo punto di vista l'Italia "non

sembra messa bene", precisa Brambilla, che è comunque più ottimista quando si parla di cloud legato alle applicazioni commerciali della videosorveglianza. Prudente anche **Alessandro Marcon (Pelco by Schneider Electrics)**, al quale – operando in un paese che sta ancora "muovendo i primi passi verso il cloud" – tutto sommato "non dispiacerebbe poter verificare prima l'esperienza in altri paesi". Meno possibilista è, invece, **Filippo Tommasin (AMACAnet.it)**: "In Italia già fa fatica a decollare la tecnologia IP sull'analogico… Pensare al cloud pare francamente prematuro".

VSAAS = VIDEOSORVEGLIARE TRA LE NUVOLE

L'introduzione della piattaforma cloud nella videosorveglianza risale ormai a più di dieci anni fa, ma è soltanto oggi che questa tendenza sta cominciando a prendere piede, promettendo di diventare una delle declinazioni più interessanti della nuvola nel settore security. I vantaggi operativi sono rappresentati dalla capacità di aggregare informazioni video provenienti da siti remoti in un'unica sorgente, alla quale si può accedere da qualunque luogo nel quale vi sia una connessione internet. Sul piano gestionale, invece, è possibile ottenere più efficienza, ridurre gli investimenti in hardware e facilitare l'adozione di standard e protocolli comuni. Senza dimenticare che la centralizzazione delle informazioni facilita l'estrazione di dati utili da impiegare nel marketing o ad altri scopi. IHS vede un grande potenziale nel mercato della VSaaS, e indica nella video content analysis cloud-based l'applicativo della svolta. Anche su questi temi, però, abbiamo riscontrato pareri discordi fra gli operatori intervistati.

VSAAS? GRANDE POTENZIALE

Tra coloro che ci hanno dato una valutazione complessivamente positiva c'è **Redo Bezzo (Honeywell Security Group)**, secondo il quale "in Europa questo mercato è in rapida crescita e le soluzioni VSaaS sono spesso richieste e rese ampiamente disponibili – in particolare nel Nord Europa e nei paesi scandinavi". Tra le diverse soluzioni hosted, la VSaaS è quella ritenuta "più vantaggiosa in termini di fatturato e di numero di telecamere IP e dispositivi adottati nel 2013". Per questa ragione, assicura Bezzo, i Servizi Video Hosted saranno "uno dei fattori decisivi per generare RMR (Recurring Monthly Revenue) e fornire una reale alternativa per acquisire profitti aggiuntivi". E l'Italia? Bezzo spiega che la carenza di banda larga fa sì che il mercato di riferimento sia "il più circoscritto in Europa", ma aggiunge anche che "la sua crescita è valutata essere a doppia cifra, analogamente a quella degli altri paesi europei". Quanto alla VCA cloud-based, si tratta di una funzionalità aggiuntiva che "contribuirà a far crescere le quote di mercato". L'opinione è condivisa da **Claus Rønning (Milestone Systems)**, che considera la VCA "un aspetto che andrà a completare e rafforzare l'offerta VSaaS". Anche Rønning ricorda che occorre superare alcuni problemi (larghezza di banda, limiti inerenti al processore a bordo camera), e intravede sbocchi interessanti per il business della video analisi in rete soprattutto "quando si vogliono estrarre dati demografici (ad esempio nel retail) e fornire un'analisi al marketing e non alla sicurezza fisica". Molto fiducioso è, infine, **Matteo Scomegna (Axis Communications)**, per il quale la VSaaS rappresenta "un trend in fortissima crescita, anche se di applicazioni reali se ne vedono ancora poche". Le potenzialità sono molto interessanti, perché – continua Scomegna – "la videosorveglianza come servizio permette e permetterà sempre più di approcciare il mercato analogico o, addirittura, quei mercati in cui la videosorveglianza non è ancora presente". Un ottimo esempio è offerto dagli algoritmi intelligenti, che "vantano già una forte presenza nel mercato del retail del conteggio persone".

VSAAS? MANCO A PARLARNE

Meno entusiasta sulla videosorveglianza e l'analisi video cloud-based è **Nicola Noviello (Arecont Vision)**, che vede invece "molto più fermento sulla crescita in termini di risoluzione". La VSaaS, spiega Novello, "sarà sicuramente un trend per gli anni futuri, ma per il momento non sarà ancora utilizzata come tecnologia di massa per impianti di videosorveglianza". Di idee simili sono **Ely Maspero (March Networks)** e **Pierfelice Peirano (TW2)**, il quale osserva che si tratterebbe di una buona idea "se la rete italiana non fosse un colabrodo". Per un responsabile di **Verint** ci sono due considerevoli ostacoli da superare: le infrastrutture ("esistono realtà e comuni geograficamente critici dal punto del digital divide") e la sicurezza, in cui "il concetto di cloud apre drammaticamente le porte alla protezione delle immagini acquisite". Mentre per **Ermanno Lucci (Daitem)** le perplessità sono legate soprattutto alle peculiari caratteristiche del Belpaese. Secondo Lucci, la mentalità italiana dominante "è quella di autosorvegliarsi e sapere esattamente chi osserva e da dove: la registrazione depositata chissà dove nel mondo non è propria del nostro approccio alla sicurezza". Perché si possa verificare un effettivo passaggio ai servizi cloud, conclude Lucci, occorre pertanto "lavorare sulla testa delle persone". **Luigi Bernardi (Bosch Security Systems)** solleva ancora una volta il problema delle infrastrutture, senza il cui ammodernamento sarà ben difficile parlare di VSaaS. "Al momento – spiega Bernardi – le telecamere scambiano dati in ambiente locale su bande intorno ai 10 MB, mentre la rete molto raramente consente scambi con bande superiori al MB (se non inferiori a 500 KB)". Di conseguenza, "è difficile immaginare traffici dati con telecamere che dovrebbero operare sempre alla massima risoluzione affinché il riconoscimento degli eventi possa sfruttare le prestazioni del sensore". **Flavio Venz (distributore esclusivo Grundig)** ritiene infine che le richieste del mercato stiano andando in un'altra direzione, quella degli "hardware per archiviare localmente: la tendenza è quindi opposta alla domanda di cloud, e questo varrà almeno per i prossimi cinque anni".

INSIDIE NORMATIVE

Un aspetto molto delicato in materia di cloud, e capace di superare anche quello tecnologico, è quello normativo, come rileva **Aldo Punzo (Bettini)**. Dello stesso parere è l'avvocato **Valentina Frediani** (**Studio Legale Frediani**), che precisa come sul piano giuridico la situazione sia "tutt'altro che chiara, soprattutto a causa di una normativa disallineata rispetto alle esigenze che può avere un modello di cloud computing, artefice di criticità e problematiche insidiose". Alla luce di queste considerazioni, prosegue l'Avv. Frediani, produrre una normativa nazionale da applicare in caso di contenzioso è una questione "da affrontare con la massima priorità".

LA PRIVACY FRA LE NUVOLE

Gli ostacoli e le problematiche da risolvere purtroppo non finiscono qui. La stessa IHS, dopo avere tessuto le lodi della VSaaS, sottolinea che i prezzi sono in media ancora assai elevati (soprattutto per il notevole costo delle relative infrastrutture), e che le modalità di installazione dovrebbero essere semplificate. *Last but not least*, occorre senz'altro affrontare lo scottante tema della privacy e della sicurezza delle informazioni. La "nuvola privata" è stata pensata proprio per garantire maggiori standard di sicurezza grazie alla presenza di un firewall, ma IHS osserva che "nessun network è mai completamente sicuro". Molto perplesso sulla questione è **Luigi Cavalieri Manasse (Diesis)**, secondo il quale "si parla molto, ma si fa poco". Cavalieri Manasse ricorda che i problemi di privacy già oggi evidenziati nell'utilizzo dei sistemi cloud-based sono numerosi – sicurezza dei server, localizzazione degli stessi in altri stati, credenziali, crittografia, gestione delle nomine dei responsabili del trattamento, e così via – e teme che l'utilizzo dell'analisi video possa ulteriormente amplificarli. Non la pensa così il già citato **Francesco Paradiso** (D-Link). Se si abbina il protocollo di sicurezza HTTPS a un ulteriore processo di autenticazione per rivedere le registrazioni attraverso il network video recorder su cloud, spiega Paradiso, si può infatti ottenere un alto livello di affidabilità ponendosi al riparo da "qualsiasi violazione della privacy". Che lo si veda in una luce più o meno positiva, il tema è indubbiamente di grande importanza. Come osserva l'avvocato Frediani, "è fondamentale avere garanzie sui profili e sulle modalità di accesso, per scongiurare il rischio di abusi non autorizzati e potenzialmente dannosi".

Cellopoint
Secure Your Email

Non riesci a trovare le email importanti?

Prova Cellopoint Mail Archiving

Vantaggi

- Conformità con le normative vigenti
- Back up veloce e restore immediato
- Risparmio di tempo grazie a funzionalità full-Text Retrieval (FTR)
- Ricerca rapida sui testi dei messaggi, su nomi e contenuti degli allegati, log
- Facile integrazione con l'infrastruttura e-mail esistente
- Estensione su storage esterno

Come funziona

Cellopoint Mail Archiving è la soluzione per la conservazione, l'archiviazione e l'e-discovery della posta elettronica. Grazie alla tecnologia CelloOS, offre capacità efficienti di indicizzazione e di archiviazione della posta che abbassano i costi di storage e riducono la quantità di dati sul server di posta, eliminando molti dei costi di gestione. Attraverso regole e policy garantisce la conservazione sicura della posta e la conformità alle normative vigenti.

horus informatica
value added distributor

Horus Informatica Srl
www.horus.it
T: **(+39) 02 33510135** Email: **commerciale@horus.it**

Luca Profico(*)

guarda il video

Datacenter sicuri
grazie agli UASG, Unified Application Service Gateway

Gli ADC - soprattutto per le organizzazioni più grandi – sono punti centrali e critici di aggregazione per il traffico delle applicazioni, nonché strumenti indispensabili per fornire accelerazione, sofisticato bilanciamento del carico, alta disponibilità, sicurezza a livello applicativo, gestione intelligente del traffico e supporto alla interoperabilità con il nuovo stack Ipv6. Ma, sempre di più, gli ADC - posti tra i data center, che servono le applicazioni web, e la più ampia rete Internet – forniscono funzionalità a valore aggiunto per sicurezza e prestazioni, al fine di migliorare la disponibilità e la protezione delle informazioni: SSL Offload, SSL Intercept, pre-autenticazione, Web Application Firewall (WAF) e mitigazione degli attacchi DDoS. Inoltre, i più moderni ADC includono anche sistemi di *scripting* che consentono agli amministratori di creare regole di Deep Packet Inspection (DPI) e di manipolare il traffico per le più svariate esigenze.

(*) Regional Sales Engineer di A10 Networks

La sicurezza di un'applicazione è un problema complesso: è fondamentale tenerne in considerazione i vari aspetti già in fase di progettazione, seguire metodologie corrette di scrittura del codice, aggiornare costantemente gli sviluppatori sulle best practice di sicurezza, e tutto questo a volte non basta. Esistono infatti rischi relativi all'integrazione di componenti di terze parti, o relativi al dialogo della propria applicazione con sistemi e servizi che potrebbero ad esempio risiedere esternamente alla propria rete e quindi fuori dal proprio controllo.

DENIAL OF SERVICE

Inoltre esistono i problemi relativi alla disponibilità di servizio e quindi agli attacchi di tipo DoS (Denial of Service): basati su enormi volumi di pacchetti di varia natura o di connessioni applicative, inondano un'applicazione o ne consumano lentamente le risorse con varie tecniche. Conseguentemente, l'ADC ha bisogno di affrontare prima gli attacchi volumetrici in modo altamente scalabile, e poi di limitare la quantità di richieste applicative o di individuare quelle che, pur essendo tecnicamente legittime, puntano a minare la disponibilità del servizio.
Gli ADC del datacenter – dovendo inoltrare tutte le transazioni indirizzate ai server – devono svolgere un compito gravoso: entrare nel merito di ogni singola richiesta. E, poiché gli attacchi di tipo applicativo non sono individuabili quando il traffico è cifrato in SSL, è spesso richiesto a questi sistemi di eseguire operazioni di decifratura prima della analisi. Il traffico va poi inoltrato o va intrapresa un'azione di mitigazione. E per mitigare gli attacchi DDoS bisogna innanzitutto identificare gli attaccanti e distinguere il traffico legittimo dal dannoso.
Esistono diverse tecniche: dalla semplice analisi statistica del numero di richieste in un lasso temporale fino a complessi processi algoritmici o addirittura basati su reti neurali che apprendono il "normale" agire di un utente e lo confrontano con il traffico che analizzano.

Ma le tecniche più avanzate non sono del tutto consolidate ed esistono attacchi che possono "inquinare" la base di apprendimento di alcuni motori. Peraltro, gli attacchi DDoS - molto dinamici – rendono complessa anche l'identificazione algoritmica del comportamento malevolo.
In ogni caso, occorre un meccanismo o una procedura che abiliti, secondo necessità, sistemi di mitigazione che possono risiedere sulla rete attaccata oppure in reti di terze parti (service provider, telco), e che li istruisca su quale tipologia o sorgente di traffico debba essere bloccata.
Nelle grandi organizzazioni si tende a utilizzare una combinazione di metodologie d'identificazione, per avere più riscontri correlati prima di abilitare meccanismi di mitigazione, e gestire in maniera più efficiente falsi positivi (identificazione erronea di attacchi in traffico legittimo, che provoca comunque l'interruzione del servizio) e falsi negativi (la mancata identificazione di attacchi).
L'ADC, situato di fronte a server critici, è ideale per la funzione di supporto della protezione DDoS. L'ultima generazione di macchine ADC tipicamente incorpora hardware dedicati ASIC (o chip programmabili FPGA) al fine di poter analizzare i pacchetti in *wire speed* per la gestione di attacchi volumetrici non applicativi. La mitigazione di questi attacchi richiede poca intelligenza e molta velocità nel trattare i pacchetti: per questa ragione l'utilizzo di componenti hardware dedicati è ideale. Condizione diversa è quella di mitigare attacchi di tipo "low and slow", basati sull'inoltro di un certo numero di richieste che rimangono incomplete o vengono distribuite su pacchetti numerosi, molto piccoli e inviati molto lentamente: mantenendo aperte molte connessioni verso il server di destinazione, essi impattano l'utilizzo di risorse e rendono difficoltosa la gestione delle richieste legittime. La difesa da questi attacchi richiede un'intelligenza che possa comprendere la dinamica del traffico.
La Deep Packet Inspection offerta dai sistemi ADC può anche aiutare nella gestione di problematiche di sicurezza applicative quali SQL injection, Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF), ecc., così come implementare meccanismi di autenticazione ulteriori a quelli proprietari delle applicazioni, e scaricare le applicazioni dalla gestione della componente SSL.

UNIFIED APPLICATION SERVICE GATEWAY

Ed è l'integrazione di tutte queste funzionalità di sicurezza, di mitigazione DDoS, Deep Packet Inspection, Web Application Firewalling, SSL Offload, con le funzionalità di bilanciamento locale e geografico ed i meccanismi di application delivery tipici di un prodotto ADC, a generare un nuovo dispositivo di rete, lo UASG (Unified Application Service Gateway).
Oggi più che mai, lo UASG è lo strumento imprescindibile di sicurezza nelle architetture dei datacenter moderni.

LA STRADA DA PERCORRERE PER MIGLIORARE LE PRESTAZIONI DEL TUO BUSINESS

Panasonic

Business intelligence video systems da Panasonic

Provate ad immaginare che contributo infinito potreste avere nel vostro business quotidiano con delle immagini **Real-Time** in alta definizione.

Business Intelligence Video Systems (BIVS) consente la comprensione immediata dei dati sui flussi **dei clienti, sui tempi di attesa, sulle aree a** rischio e l'analisi del **tipo di clientela**. Tutto questo vi permette di ottimizzare ogni centimetro della vostra attività al dettaglio cosa che prima era impensabile mentre provvede un'eccellente videosorveglianza - **Panasonic contribuisce a migliorare il vostro business**.

Per sapere di più visita: business.panasonic.it

BUSINESS INTELLIGENCE VIDEO SYSTEMS

Telecamere IP per la sicurezza dei trasporti pubblici di Szeged

STATO DI FATTO ED ESIGENZE DEL COMMITTENTE

Szeged, città ungherese ricca di storia con una popolazione di circa 163.000 persone, è tra le più grandi nella regione sud orientale dell'Ungheria. Szeged ha vissuto numerosi eventi negativi nel corso del 19esimo e 20esimo secolo, per via di disastri naturali o guerre. A seguito di questi eventi, Szeged ha dovuto recentemente ricostruire edifici, strade e riorganizzare il sistema di trasporti, modernizzando l'agglomerato urbano e rendendolo dinamico sia dal punto di vista culturale che economico. Senza dubbio, proprio questi trasporti pubblici hanno giocato un ruolo fondamentale per la rinascita della città, contribuendo però al tempo stesso a una crescita esponenziale del volume del traffico dovuto anche agli spostamenti dei pendolari. Tram, filobus ed autobus sono i tre elementi chiave su cui ruota la rete di trasporti a Szeged. La loro sicurezza, intesa come safety e come security, sono estremamente importanti poiché hanno un impatto diretto sulla vita dei cittadini e sulla ricchezza della città. Ultimamente, in considerazione del ruolo fondamentale giocato dal trasporto pubblico, l'amministrazione cittadina ha gradualmente aumentato il proprio impegno e investimento nel sistema stesso e nella modernizzazione delle infrastrutture, garantendo l'efficienza del funzionamento dei trasporti e migliorando ulteriormente la sicurezza.

In linea con questa modernizzazione, l'azienda statale Szeged Transport Co. Ltd. (SZKT), ha acquistato numerosi nuovi filobus. Grazie alla consulenza professionale di New Line Technologies, un integratore professionista di Sistemi di Trasporti Intelligenti (ITS), sono state implementate sui nuovi mezzi delle tecnologie più avanzate ed intelligenti e dei sistemi di sorveglianza ad alta qualità.

LA TECNOLOGIA MESSA IN CAMPO

In questo progetto sono state utilizzate 110 telecamere IP MD7560D di VIVOTEK, le cui qualità e tecnologia apportano un indubbio valore aggiunto alla scelta di New Line Technologies. Con il totale supporto del distributore locale VIVOTEK (IP Cam Technologies), New Line Technologies ha introdotto con successo le telecamere network MD7560D di VIVOTEK sui nuovi filobus di proprietà di SZKT per monitorare le cabine dei bus sia internamente sia all'esterno.

Il modello **MD7560D** è una telecamera mobile network da 2 megapixel antivandalo sviluppata da VIVOTEK e specificatamente progettata per i mezzi di trasporto quali bus, treni e altri veicoli. In ottemperanza con lo standard EN50155 per i dispositivi elettrici installati su binari, la telecamera può sopportare sollecitazioni, vibrazioni, fluttuazioni e condizioni tipiche dei treni rapidi, mantenendo una qualità video stabile e affidabile durante i movimenti del veicolo. Con una risoluzione 1600x1200, la MD7560D produce immagini estremamente chiare e dettagliate che possono rendere più agevole l'identificazione di persone e oggetti. Le riprese video delle attività dei passeggeri all'interno del veicolo o gli eventuali incidenti all'esterno possono essere catturate con chiarezza e registrate su un dispositivo mobile network installato all'interno di ogni filobus per essere successivamente utilizzate come prova documentale ed evidenza probatoria.

Sharon Lee, Direttore della Europe Business Division di VIVOTEK, ha commentato: “Per VIVOTEK è stato un onore avere questa grande opportunità: abbiamo assistito al miglioramento dell’infrastruttura security dei nuovi tram di Szeged Transport Co. Ltd.. Grazie a New Line Technologies, 110 telecamere network del modello VIVOTEK MD7560D sono state integrate in una fase preliminare. In seguito, il modello MD7560D si è dimostrato la scelta ideale per rafforzare la security nei trasporti usati dai cittadini di Szeged e per creare un ambiente più sicuro. In una fase successiva, ulteriori modelli MD7560D verranno aggiunti sia nelle cabine degli autobus meno recenti e sprovviste di telecamere, sia nelle cabine dei nuovi autobus.”

in breve

Location:
Tram, filobus ed autobus della città di Szeged, Ungheria

Tipologia di impianto:
telecamere IP sui filobus per monitorare le cabine internamente ed esternamente con apparecchiature di rete progettate per i mezzi di trasporto (conformi allo standard EN50155 per i dispositivi elettrici installati su binari: mantengono la qualità del video inalterata anche in caso di sollecitazioni, vibrazioni, fluttuazioni tipiche dei treni rapidi).

System Integrator:
New Line Technologies;
Distributore locale: IP Cam Technologies

Brand dei componenti:
VIVOTEK (telecamere IP mobile **MD7560D** 2 megapixel antivandalo)
www.vivotek.com

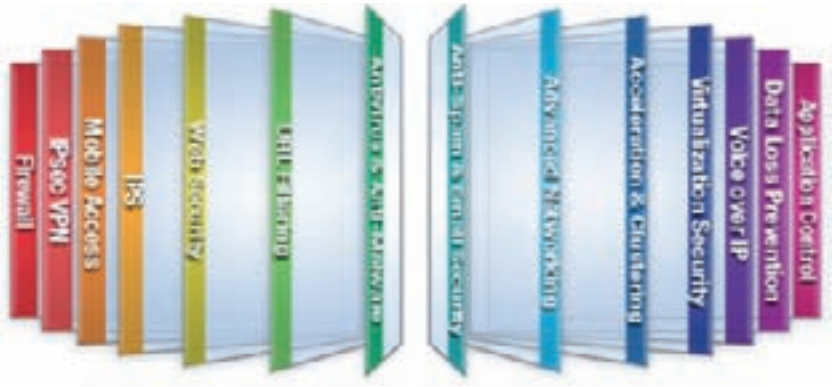
guarda il video

Affidabilità, flessibilità, semplicità d'uso:
un'infrastruttura di sicurezza omogenea per Unieuro

STATO DI FATTO ED ESIGENZE DEL COMMITTENTE

Azienda leader nella distribuzione al dettaglio di elettronica ed elettrodomestici, Unieuro è parte del Gruppo Dixons Retail. In Italia, UniEuro conta 96 negozi diretti e circa 70 punti vendita in franchising, distribuiti su tutto il territorio nazionale, per una superficie totale delle aree di vendita che raggiunge i 200.000 mq. Dall'avvio delle sue attività sul territorio italiano, Unieuro si è affidata alle soluzioni di sicurezza di Check Point, dapprima con i suoi tradizionali firewall, poi estendendo successivamente la sua infrastruttura per rispondere alle necessità che venivano man mano individuate. Nel corso del tempo, i firewall di UniEuro si sono via via arricchiti di software blade specifiche, che hanno gradualmente sostituito le soluzioni – tipicamente hardware – che ne svolgevano in precedenza le funzioni. Così facendo, Unieuro è passata da un'infrastruttura di sicurezza eterogenea a una piattaforma composta unicamente di soluzioni Check Point, almeno sul lato server. L'installazione è stata eseguita con successo da Unieuro con il supporto di Polimatica, partner che da tempo segue il cliente per le questioni infrastrutturali.

LA TECNOLOGIA MESSA IN CAMPO



I criteri seguiti da UniEuro per questo progetto di rinnovamento dell'infrastruttura sono stati sostanzialmente tre: il mantenimento della massima efficacia nella sicurezza, la governabilità dell'intera infrastruttura ed il raggiungimento di un positivo rapporto tra qualità e prezzo. Obiettivi che, con il passaggio alle software blade di Check Point, possono dirsi pienamente raggiunti.

"La nostra infrastruttura oggi è decisamente più moderna, oltre che più semplice ed intuitiva da utilizzare", ricorda Giancarlo Bianco, Head of ICT Technology, Unieuro. "L'automatizzazione di molti processi, che prima venivano condotti in modalità manuale, ha permesso di velocizzare sensibilmente molte operazioni, con vantaggi sostanziali nel time-to-market e nella capacità di rispondere in modo adeguato alle richieste che provengono dal business."

Ogni software blade soddisfa una necessità specifica, e presiede alla sicurezza aziendale in un ambito dedicato. Ed ogni software blade è a suo modo strategico, perché evita problemi e malfunzionamenti che potrebbero ripercuotersi sensibilmente sul business aziendale.

Una volta completata la propria infrastruttura di sicurezza, con l'efficace supporto di Polimatica, il team IT ha cercato di renderla ancora più funzionale al business. E proprio per rendere più evidente il legame tra il buon funzionamento dei sistemi di sicurezza e le attività dell'azienda, è stata aggiunta, come software blade più recente, la funzione SmartEvent. "Si tratta di uno strumento particolarmente utile per chi, come noi, vanta diverse funzioni di sicurezza ma ha un team dedicato relativamente ridotto", spiega ancora Giancarlo Bianco. "SmartEvent ci permette di mantenere una visione d'insieme dell'intera infrastruttura, offrendoci degli alert in real time ma anche la possibilità di avere dei report che illustrino gli eventi di sicurezza in modo chiaro, legandoli direttamente alle loro possibili ripercussioni sul business." La blade SmartEvent è stata una novità assoluta per Unieuro, che prima non disponeva di una soluzione unificata di gestione della sicurezza. Ed ha fatto immediatamente vedere i suoi benefici a livello di gestione.

VANTAGGI A BREVE E LUNGO TERMINE

Il passaggio alle software blade Check Point ha permesso a Unieuro di semplificare decisamente la propria infrastruttura, con vantaggi significativi nella gestione dei processi di sicurezza. In qualche caso, il tempo impiegato a gestire alcune attività ricorrenti si è più che dimezzato.

Parallelamente, sono stati ridotti i costi legati alle licenze dei sistemi, grazie al consolidamento dell'intera infrastruttura su soluzioni Check Point. E la scelta delle software blade, rispetto ai tradizionali sistemi basati su appliance, ha permesso di raggiungere una flessibilità nettamente superiore, oltre ad ottimizzare gli investimenti effettuati. Nella sostanza, UniEuro può aggiungere nuove blade ogni volta che si trova di fronte a una nuova necessità di sicurezza, senza dover sovradimensionare in partenza la propria infrastruttura.

Più in generale, obiettivo del team IT è quello di rendere la sicurezza un elemento fondante dell'azienda, e non più semplicemente un investimento obbligato, sensibilizzando il management verso le opportunità che un'infrastruttura adeguata può consentire di sfruttare. In questo senso, il costo di un mancato investimento in sicurezza non si misura solamente nel risparmio a livello di soluzioni, ma anche e soprattutto nelle opportunità di business che possono svanire a causa di un problema di sicurezza – ad esempio un blocco prolungato del sistema.
"Oggi più che mai, la sicurezza informatica va considerata un abilitatore del business aziendale, e la scelta di un'infrastruttura Check Point si è rivelata azzeccata sotto ogni aspetto, in particolare in quest'ottica", conclude Giancarlo Bianco.

in breve

Location dell'installazione:
sede aziendale Unieuro, Monticello d'Alba (CN)

Tipologie dell'installazione:
sistema di sicurezza informatica

Tratti salienti del sistema:
sicurezza distribuita e flessibile

Funzionalità principali:
gestione centralizzata, flessibilità, semplicità d'uso, riduzione dei costi

System integrator:
Polimatica **www.polimatica.it**

Brand dei componenti:
firewall standard, software blade Check Point
www.checkpoint.com

Videocontrollo
per il Ponte del Mare

STATO DI FATTO ED ESIGENZE DEL COMMITTENTE

Il Ponte del Mare è un ponte strallato ciclo-pedonale di recente costruzione nella città di Pescara. Con i suoi 466 metri di lunghezza tra le spalle ed i 172 metri di luce dell'impalcato sospeso, è tra i ponti ciclo-pedonali più grandi in Europa.
Il ponte collega la riviera sud con quella nord del fiume Pescara, permettendo di creare la necessaria continuità al Corridoio Verde Adriatico, la pista ciclabile che corre lungo tutta la costiera adriatica da Ravenna a Santa Maria di Leuca, in via di completamento.

LA TECNOLOGIA MESSA IN CAMPO

Il progetto si è evoluto con il cablaggio, l'installazione e il collaudo dei seguenti apparati:

- Telecamere in cabinet da esterno con tecnologia e sensore megapixel da 2Mp e ottica da 3.3-12mm (VKD-MP250) o 3Mp con ottica da 8-16mm (VKD-MP350), con ausilio di illuminazione IR ad alta efficienza e filtro ICR, mentre il sistema di trasmissione è stato affidato a protocollo di rete TCP\IP.

- Unità speed dome endless con zoom ottico 36x (VKD-M360) e sistema di trasmissione tramite protocollo di rete TCP\IP.

- Per evitare rallentamenti dovuti agli elevati flussi IP e alle elevate temperature, si è dovuto provvedere alla realizzazione di una rete ad anello ridondante con sistema a fibra ottica monomodale e switch industriali (SWC5D) con elevate prestazioni anche a temperature elevate e montaggio barra DIN a 24Vac.

Visto l'elevato flusso di dati, sono stati utilizzati 12 Hard disk da 2Tb in grado di garantire fino a 1 mese di registrazioni di backup.

- La parte di supervisione è stata invece realizzata con il sistema hardware e software CENTER128 di Videotrend, con l'ausilio di 4 monitor in cabinet metallico da 42" PR-M42D+, che è in grado di visualizzare fino a 128 canali (32 per ogni monitor) in real time.

- Il sistema, inoltre, è già predisposto per un futuro ampliamento con sistema di analisi video, serie VKD-AV, in grado di rilevare l'abbandono di oggetti, l'occupazione di spazi riservati, analisi direzionale, motion detector avanzato ed altre importanti funzioni.

- Per l'attraversamento del fiume è stato invece utilizzato un sistema di trasmissione radio con access point dual band 2.4/5.8 GHZ (PR-ACP3) in grado di garantire una banda di comunicazione fino a 108Mbps.

- La registrazione e l'analisi logica di funzionamento è stata affidata al sistema VKD-RAID128, in grado di supportare fino a 128 apparati IP con 16 slot per hard disk in modalità RAID 1 o 5, 2 reti 10/100/1.000 MBps e 3 alimentatori ridondanti, il tutto assemblato in un mobile rack metallico.

in breve

Location:
Ponte del mare, Porto canale di Pescara

Tipologia di impianto:
sistema di Videosorveglianza IP

Peculiarità dell'installazione:
elevati flussi IP e elevate temperature. Per evitare rallentamenti, si è realizzata una rete ad anello ridondante con sistema a fibra ottica monomodale e switch industriali (SWC5D) con elevate prestazioni anche a temperature elevate e montaggio barra DIN a 24Vac. Per l'attraversamento del fiume è stato utilizzato un sistema di trasmissione radio con access point dual band 2.4/5.8 GHZ (PR-ACP3) in grado di garantire una banda di comunicazione fino a 108Mbps.

Installatore:
Ditta Dino Pace srl

Distributore di zona:
2B Automazioni e Sicurezza srl

Brand:
Dahua Technology Co.Ltd, IR LAB Limited, Videotrend **www.videotrend.net**

IL MIGLIOR MODO DI GESTIRE LA TUA AZIENDA IT

Sia che sviluppiate, vendiate o implementiate soluzioni di tecnologia, Autotask offre tutto il necessario all'organizzazione, automatizzazione e ottimizzazione della vostra azienda IT fornendovi una piattaforma singola, integrata, basata su cloud ed accessibile da qualsiasi posizione. Finalmente potrete dedicare meno tempo alla gestione della vostra azienda e investirne di più nella crescita.

- Sales e Marketing (CRM)
- Service Desk
- Contratti
- Fatturazione
- Gestione progetti
- Pianificazione risorse
- Tempo e spese
- Gestione outsourcing
- Scorte
- Reportistica

Autotask®

RICHIEDETE OGGI STESSO LA DEMO A UN VOSTRO RAPPRESENTANTE

www.autotask.com/it | +44-203-006-3147

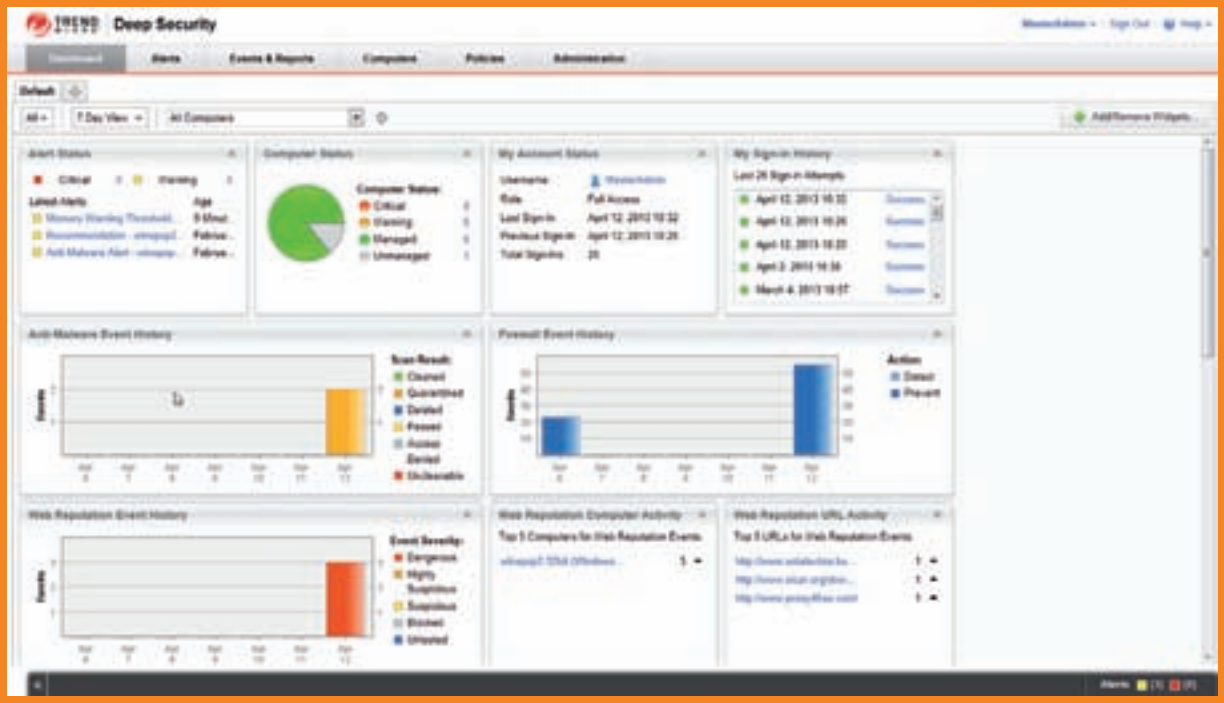
Sede del Consiglio della Regione Toscana

guarda il video

Ambienti virtuali sicuri
con una piattaforma per la sicurezza dei server completa

Nelle periodiche indagini svolte tra i responsabili tecnologici e i Ceo delle aziende, il primo elemento di preoccupazione per chi deve affrontare un progetto di virtualizzazione continua a essere la sicurezza. Con l'evoluzione dell'idea di perimetro aziendale e la possibilità per i diversi utenti di accedere in qualsiasi momento da qualsiasi luogo alle reti, l'identità fisica della macchina assume un significato diverso ed è necessario che la sicurezza segua questa stessa evoluzione.
Trend Micro è da 25 anni in prima linea per la totale sicurezza informatica degli utenti e delle aziende ed è in grado di rispondere in maniera efficace alle criticità legate alla sicurezza, che impattano oggi sui progetti di virtualizzazione.
Gli ambienti virtualizzati si distinguono per le loro caratteristiche di mobilità e flessibilità, per questo è necessario un approccio con soluzioni studiate appositamente per la loro particolare struttura. La soluzione di punta Trend Micro, progettata ad hoc per la sicurezza degli ambienti virtuali (sia a livello server che desktop) e che supporta le più recenti tecnologie dei produttori, è Trend Micro Deep Security.

Trend Micro Deep Security è una piattaforma per la sicurezza dei server completa, adattativa ed estremamente efficiente, che protegge le applicazioni e i dati aziendali da violazioni e interruzioni dell'attività senza costose patch d'emergenza. Deep Security si basa su moduli strettamente integrati che permettono di ampliare facilmente la piattaforma per garantire la sicurezza di server, delle applicazioni e dei dati sui server fisici,



virtuali e in-the-cloud, oltre che nei desktop virtuali, semplificando così le operazioni di sicurezza in azienda e garantendo un veloce ritorno degli investimenti nei progetti di virtualizzazione e cloud. Come? I moduli anti-Malware, IDS/IPS, Protezione Web Application, Virtual Patching e Log Inspection sono disponibili sia in configurazione agentless che agent based, permettendo così la protezione di qualsiasi ambiente.
L'ultimo in ordine di tempo ad aver compreso le caratteristiche uniche di Deep Security e ad aver adottato la soluzione è stato il Consiglio Regionale della Toscana.

UN CASO APPLICATIVO

Il **Consiglio Regionale della Toscana** ha il compito di valutare e approvare le scelte, i programmi e le iniziative legislative promosse dal governo locale sulle materie di competenza regionale. L'ente impiega 261 addetti a livello di struttura ai quali si sommano altri 246 collaboratori nelle aree dei gruppi consiliari. Nel corso degli ultimi tre anni i suoi sistemi IT sono passati da un'architettura fisica a una configurazione dei servizi di rete gestiti attraverso un'architettura completamente virtuale, che garantisce l'operatività per i servizi interni di back-office e quelli di front-office, esposti su Internet per l'accesso da parte dei cittadini. A questi si è aggiunta recentemente una porzione di ambienti applicativi in-the-cloud, impiegati principalmente per lo streaming video della diretta del Consiglio regionale e lo storage delle registrazioni delle sedute consiliari, rese poi disponibili via Web ai cittadini.
Con la progressiva digitalizzazione dei processi, quindi, il Consiglio Regionale della Toscana si è trovato a dover prestare particolare attenzione alla sicurezza e ai piani di continuità operativa, necessità diventata poi un obbligo di Legge con il Codice dell'amministrazione digitale, che impone di gestire i livelli di sicurezza e affidabilità dei servizi secondo una logica strutturata

In quest'ottica, Trend Micro Deep Security ha fornito all'ente una piattaforma di protezione server completa, in grado di proteggere i sistemi virtualizzati da violazioni di dati o interruzioni dell'attività, assicurando un elevatissimo grado di continuità operativa e la conformità agli standard interni di qualità e ai principi ITIL. La soluzione Trend Micro ha consentito di migliorare la gestibilità della sicurezza negli ambienti VMware, riducendo la necessità di continue operazioni di configurazione e aggiornamento e ha permesso di centralizzare la gestione dei processi di prevenzione dei rischi. In particolare, il sistema di patching virtuale consente la protezione delle vulnerabilità prima che possano essere sfruttate e facilita il rilascio di patch di emergenza, anche attraverso azioni pianificate, in modo da evitare costose interruzioni dell'attività di sistema.
Grazie al nuovo processo di semplificazione il Consiglio Regionale ha potuto abbattere i costi, risparmiando sulle spese generali di gestione e amministrazione dell'IT. A questi vantaggi si somma una copertura estesa rispetto a varie tipologie di rischio relative alle architetture software e piattaforme, incluse quelle in-the-cloud.

Trend Micro
Trend Micro su Twitter
Trend Micro su Facebook
Trend Micro su YouTube
Trend Micro su SlideShare

www.trendmicro.it

Non solo altissima definizione:
telecamere pensate per l'installatore

L'altissima definizione è senza dubbio il driver che domina le vendite di videosorveglianza e che sta governando la stessa transizione verso l'IP. Se però alle altissime prestazioni non si accompagnano anche una netta semplificazione di tempi e modi dell'installazione e quindi una riduzione dei costi di sistema, allora l'alta definizione rischia di diventare appannaggio di pochi eletti.
Forte di queste considerazioni e fedele alla propria mission di aggiornamento e miglioramento continuo di prodotti e prestazioni, Arecont Vision ha rinnovato la nota gamma di telecamere MegaView® e MegaBall® con funzioni e optional che, tramite il controllo a distanza di messa a fuoco e zoom, semplificano l'installazione, contribuendo a ridurre i costi complessivi di sistema.

MegaBall® 2

MegaView® 2

CONTROLLO A DISTANZA DI MESSA A FUOCO E ZOOM

Le nuove serie di telecamere all-in-one giorno/notte H.264 a tecnologia megapixel, MegaView® 2 e MegaBall® 2 ampliano la rinomata gamma di telecamere MegaView® e MegaBall®.

Entrambe le nuove serie sono dotate di obiettivi P-iris con controllo a distanza di zoom e messa a fuoco, che ne semplificano l'installazione, e della funzionalità opzionale "true Wide Dynamic Range (WDR)" a 1080p e 3 megapixel (MP).

UNA VISTA MEGA

Le telecamere MegaView® 2 sono disponibili con risoluzioni di 1,3 MP, 1080p, 3 MP, 5 MP e 10 MP. Come funzionalità opzionale, offrono un illuminatore LED integrato a infrarossi (IR). Le telecamere MegaView® 2 comprendono una scatola di derivazione e un supporto a parete a tre assi facile da regolare, che ne semplifica ulteriormente l'installazione. Gli alloggiamenti "bullet-style" sono dotati di certificazione ambientale IP66.

TELECAMERE SFERICHE

Le telecamere sferiche MegaBall® 2 sono disponibili nei modelli da 1,3 MP, 1080p, 3 MP e 5 MP, e comprendono una struttura integrata per la gestione dei cavi, che ne semplifica l'installazione. Le telecamere MegaBall® 2 possono essere installate anche utilizzando un versatile braccio di montaggio o un alloggiamento a cupola.

PENSATE PER L'INSTALLATORE

L'installazione di queste telecamere con controllo a distanza di messa a fuoco/zoom non necessita di regolazioni in loco del campo di visione o della messa a fuoco. L'obiettivo può essere controllato a distanza dal terminale. L'obiettivo P-iris offre la migliore posizione del diaframma per ottenere nitidezza delle immagini e profondità di campo ottimali. Le funzioni di scansione per la messa a fuoco a tutto campo o a breve distanza analizzano un'area di interesse o l'intera inquadratura per ottenere la messa a fuoco migliore per il campo di visione scelto.
"Il controllo a distanza di messa a fuoco e zoom rendono queste nuove telecamere straordinariamente semplici da installare, aiutando a ridurre i costi complessivi di sistema" - specifica Raul Calderon, Senior Vice President di Arecont Vision. "La decisione di aggiungere una scatola di derivazione ai sistemi di gestione dei cavi delle MegaView® 2 e delle MegaBall® 2 dimostra un'attenzione ai dettagli che nasce dal fatto che le nostre telecamere sono prodotte pensando agli installatori".

PIÙ DETTAGLI CON IL WDR

La tecnologia WDR di Arecont Vision produce una gamma dinamica fino a 100 dB a risoluzione piena senza diminuzioni nel frame rate. Combinando tempi di esposizione brevi e lunghi nello stesso campo visivo, il WDR massimizza la quantità di dettagli sia nelle aree luminose che in quelle scure. Le prestazioni WDR delle telecamere Arecont Vision offrono fino a 50 dB in più (300X) sulla gamma dinamica rispetto alle telecamere tradizionali.

PRESTAZIONI MEGA

Oltre all'obiettivo P-iris con controllo a distanza di messa a fuoco e zoom, le telecamere MegaView® 2 e MegaBal® 2 offrono molte funzioni che ne migliorano le prestazioni, tra cui doppio codec H.264 (MPEG-4 Part 10)/MJPEG, mascheramento area di privacy, funzione di rilevamento del movimento avanzata a 1024 zone, incredibili prestazioni in condizioni di scarsa illuminazione, funzione binning per aumentare la sensibilità (su modelli a 3 MP e 5 MP), cropping flessibile per regolare le dimensioni delle immagini e la possibilità di scegliere tra PoE (Power over Ethernet) o alimentazione esterna.

Arecont Vision
425 East Colorado Street,
7th Floor
Glendale, CA 91205 (USA)
Contatti per l'Italia:
nnoviello@arecontvision.com
Tel. +39 348 2456618

www.arecontvision.com

Soluzione per gestire la sicurezza

dove, come e quando vuoi

L'Italia è il primo paese europeo per diffusione di smartphone. Perché allora non controllare e gestire il sistema d'allarme con un'app per smartphone che consenta di inserire, disinserire e visualizzare lo stato dell'impianto a distanza, di consultare la memoria eventi, di escludere i rivelatori e di attivare dispositivi domotici? E se la nuvola fa ormai parte del nostro quotidiano, anche se spesso non ne siamo al corrente, perché non monitorare, controllare e configurare il sistema d'allarme via web browser con un'app basata sul **cloud**? Da queste considerazioni e dall'esperienza di un leader mondiale della sicurezza, nasce **LightSYS™ 2** di RISCO, l'unico sistema di sicurezza ibrido gestibile via Smartphone che offre una completa flessibilità di comunicazione e la massima libertà di scelta tra accessori e rivelatori cablati, bidirezionali radio o via Bus RISCO. L'App per smartphone permette all'utente di controllare in qualsiasi momento la propria casa o il proprio ufficio e di verificare in tempo reale l'attendibilità di un allarme in corso. La possibilità di usare qualsiasi combinazione di dispositivi come sirene e rivelatori radio bidirezionali, unite alla flessibilità di comunicazione via IP, GSM/GPRS o PSTN e ai vantaggi del collegamento via RISCO Bus, fanno di LightSYS™2 un sistema adatto a qualsiasi **installazione residenziale e piccolo commerciale** e consentono di risparmiare tempo e costi di installazione.

Inserimento/disinserimento del sistema di allarme a distanza

Verifica di un allarme in corso in tempo reale con la funzione di Video Verifica

Memoria eventi sempre disponibile

Smartphone App
Attraverso l'applicazione per smartphone iRISCO, gli utenti possono controllare e gestire il loro sistema LightSYS™ 2. L'App consente di inserire, disinserire e visualizzare lo stato dell'impianto a distanza, di consultare la memoria eventi, di escludere i rivelatori e di attivare dispositivi domotici. L'App è disponibile in versione iOS (per iPhone, iPad) e con sistema operativo Android.

Applicazioni Web
LightSYS™ 2 offre inoltre l'innovativa applicazione Web che permette di monitorare, controllare e configurare il sistema via web browser. Oltre a tutte le possibilità offerte dall'App per Smartphone, con l'App per web si può registrare il sistema, aggiungere utenti e altro. L'applicazione si basa su RISCO Cloud, l'esclusivo server di RISCO "sulla nuvola". Presto, sempre grazie al RISCO Cloud ed attraverso le App e il web browser, sarà anche possibile verificare visivamente gli allarmi adottando telecamere IP compatibili.

Flessibilità totale
La flessibilità di installazione è totale: l'installatore può scegliere di integrare dispositivi filari e radio in qualsiasi combinazione per un sistema **realmente ibrido**. La flessibilità si estende anche alla comunicazione che può essere vocale, via PSTN e GSM/GPRS oltre che IP, con moduli ad innesto. Ma soprattutto LightSYS™ 2 può beneficiare della gamma completa di accessori RISCO di ultima generazione collegabili via filo, via BUS e via radio, sia mono che bidirezionali.

Qualche esempio di combinazione:

1) **con rivelatori e sirene indirizzabili sul Bus RISCO** - per risparmiare su cablaggio e manodopera e sulle espansioni di zona, e per disporre di programmazione e diagnostica da remoto. Modelli: WatchOUT™ Extreme (rivelatore da esterno con 4 canali di rilevazione: 2 PIR e 2 a microonda); WatchIN™ (2 canali PIR e 2 a microonda ed antiaccecamento; ideale per ambienti industriali diffi cili); Industrial LuNAR™ (rivelatore industriale da soffitto con antimascheramento, ideale per magazzini); BWare™ & iWISE® Bus (versione indirizzabile su Bus dei rivelatori BWare™ e iWISE®); Microfono selettivo (ideale per caveau, casseforti, bancomat); ProSound™ (sirena con protezione unica antischiuma, antiperforazione e antiavvicinamento; tecnologia Surface Light Technology).

2) **rivelatori cablati** - modelli: Bware™ (rivelatori con microonda in banda K); iWISE® (rivelatori con resistenze di fine linea integrate); LuNAR™ (rivelatore da soffitto); DigiSense™ (rivelatori digitali con resistenze di fine linea integrate); ShockTec™ Plus (rivelatore sismico per protezione perimetrale); ViTRON™ Plus (rivelatore acustico rottura vetri); Rivelatore antiallagamento filare (si allarma in caso di allagamento sopra il livello del sensore).

3) **accessori radio mono e bidirezionali per antintrusione** (rivelatori da esterno, barriere radio, barriere agli infrarossi attivi, rivelatori PIR, rivelatori volumetrici, contatti radio bidirezionali per porte e finestre, rivelatori inerziali per protezione perimetrale, rivelatori acustici rottura vetri, sirene via radio per interno ed esterno), per sicurezza (rivelatori di fumo e calore, monossido di carbonio, gas e antiallagamento) e tastiere radio, telecomandi e dispositivi antipanico.

La tecnologia BUS di RISCO consente di ottenere due impagabili vantaggi: a) controllo e diagnostica da remoto dei parametri dei dispositivi; b) risparmio sui costi e i tempi di installazione e manutenzione.

Risco Group
Via Robecco 91
20092 Cinisello Balsamo (MI)
Tel. +39 02 66590054
Fax +39 02 66590055
info@riscogroup.it

www.riscogroup.it

Speed dome e NVR
ideali per l'IP HD

Serve ancora ripeterlo? IP e alta definizione sono ormai elementi imprescindibili di un'offerta di successo e che permettono al mercato della videosorveglianza IP di crescere anche in questo 2013 di passione. La sempre maggior concentrazione di interesse sull'alta definizione, eletta da molti buyer come motivazione più convincente per passare definitivamente ai sistemi di rete, è un punto chiave della crescita. Forte di queste considerazioni, JVC Professional lancia una nuova speed dome di rete PTZ della linea Super LoLux 1080p HD e un NVR ideale per la registrazione IP HD.

FATTE APPOSTA PER L'IP HD

Eccellenti immagini ad alta risoluzione 1080p, design moderno e accattivante, affidabilità elevata, ampia area di ripresa: queste sono solo alcune delle caratteristiche che rendono la nuova speed dome di rete PTZ modello VN- H557U, della linea Super LoLux 1080p HD di JVC Professional, la telecamera ideale per l'uso in applicazioni come centri commerciali, aeroporti e stazioni di servizio.

QUALITÀ DELL'IMMAGINE

La telecamera è dotata di zoom ottico 10x e pan/tilt 350°, mentre la sua tecnologia Super LoLux HD offre una risoluzione brillante ad alta definizione e una notevole sensibilità della luce per produrre immagini a colori con soli 0,45 lux. E' dotata di potente funzionamento dual stream (30ips/30ips JPEG/H.264 High Profile) e permette la registrazione su scheda SD di allarme ed esportazione diretta del file MPEG4. Dispone inoltre di riduzione dinamica del rumore 3D e supporta l'ultima protocollo ONVIF per le telecamere di rete (Profilo S).

OTTIME PRESTAZIONI

Economica, ha ottime prestazioni sotto i punti di vista. Fornita di supporto allarme audio integrato, la speed dome di rete PTZ VN- H557U si può installare anche in opzione multi-angolo.

Il tempo di latenza è di soli 50ms quando si utilizza un joystick USB per il controllo pan e tilt, inoltre è testata per avere un MBTF (mean time between failures) di ben 30.000 ore. Se il tempo atteso tra un guasto e l'altro è il più lungo del mercato, significa quindi che la telecamera è assolutamente affidabile e che ha una vita operativa decisamente più duratura della media. Infatti la speed dome VN- H557U garantisce molti anni di servizio senza richiedere alcuna manutenzione.

REGISTRATORE DI RETE IDEALE PER L'IP HD

Completa la gamma il registratore di rete VR-X1600U/3200U.
Semplici e robusti nel design, i videoregistratori di rete di JVC sono ideali per le registrazioni HD IP. Pronto all'uso appena estratto dalla confezione, l'NVR di JVC non richiede alcun software aggiuntivo o server di rete, avendo pre-installato il software Milestone Xprotect Enterprise.
VR-X1600U è un registratore a 16 canali che viene fornito con 16 licenze XProtect Milestone e 100ips di registrazione. Se si ha necessità di registrare un numero maggiore di telecamere, si può optare per il modello VR-X3200U a 32 canali. Entrambi i modelli possono essere implementati installando licenze aggiuntive: da 16 canali a 32 canali e da 32 canali a 64 canali.
Con la funzione Master/Slave il numero di NVR e telecamere che possono essere gestite e visualizzate in contemporanea è illimitato.

SERVE UN RIEPILOGO?

Riportiamo in sintesi le caratteristiche della nuova proposta di JVC Professional per la registrazione di rete senza necessità di software aggiuntivi.

- 16 canali /32 canali
- 1TB hard disk drive
- Tre HDD addizionali
- Pre-installato Milestone XProtect enterprise software
- Max registrazione 2800ips in H.264 High Profile VGA
- RAID 1, 5 and 10 (RAID 6 optional)
- Master slave

JVC Professional Europe
Filiale italiana
Via Giuseppe Sirtori
720129 Milano (MI)
Tel. +39 02 269431
Fax +39 02 26929361
info@jvcpro.it

www.jvcpro.it

SECURITY EXPO 2014

19-22.03.

INTERNATIONAL SPECIALISED EXHIBITION FOR SECURITY SYSTEMS AND EQUIPMENT

INTER EXPO CENTER • IEC

www.iec.bg

www.bcci.bg/fairs/security

Un'immagine dell'edizione veronese

La piazza in movimento di *IP Security Forum* salpa nel capoluogo emiliano

È Bologna - la rossa, dotta e grassa città emiliana - la prossima mèta di IP Security Forum.
La prima tappa del 2014 del roadshow riporta infatti la "piazza in movimento" e il felice format veronese nel bel mezzo del capoluogo emiliano, aggiungendo nuovi ingredienti alla già piccante ricetta dell'ultima edizione.

Il prossimo 6 Marzo la mostra-convegno dedicata alle soluzioni per l'IP Security diventerà infatti un**'agorà di discussione**, aperta all'analisi e alla condivisione di tutti i presenti.
Il pubblico verrà condotto letteralmente per mano in un percorso contenutistico che si snoda *attraverso e lungo gli stand*, dalla teoria alla pratica senza soluzione di continuità, per toccare con mano le potenzialità della tecnologia e per commentarne dal vivo pro e contro.

SERVE UN RIEPILOGO?

Cos'è IP Security Forum
IP Security Forum è l'unico *congresso con l'expo intorno* dedicato alle tecnologie per la sicurezza fisica in tutte le applicazioni che viaggiano su IP: **videosorveglianza** ma anche **intrusione, controllo accessi** e tutto ciò che ruota attorno al **cloud computing**.

Un roadshow sul territorio
Originariamente nato per svilupparsi in due soli momenti convegnistici (uno primaverile e uno autunnale), si è col tempo trasformato in un vero **roadshow itinerante** sul territorio, che ha toccato le più diverse tappe geografiche: da Napoli a Verona, da Bari a Vicenza, da Torino a Bologna passando per Milano e altro ancora.

Il format
Rivisto e ripensato edizione dopo edizione per allinearsi alle sempre diverse esigenze del mercato, il format di *IP Security Forum* vuole accrescere l'osmosi tra **area expo e sessioni congressuali**, per garantire la piena fusione tra le due facce - descrittiva ed espositiva - di una stessa medaglia: la tecnologia per la sicurezza fisica che viaggia su IP in tutte le sue applicazioni, performance e funzionalità.

Il congresso
Sempre più profilato e snello, si focalizza sui temi portanti della vera *rivoluzione copernicana* della security: la **comunicazione su IP** con i relativi pro e contro tecnologici, con le opportunità di business che reca e la nuova competizione che innesca. Ma il congresso affronta anche temi a più ampio spettro: dalle responsabilità civile e penali degli operatori di sicurezza alla mai definitivamente chiusa questione della privacy.

La community
IP Security Forum è un contenitore aperto al contributo di tutti i protagonisti dell'attuale processo evolutivo, che vede la security convergere sempre più massicciamente verso l'ICT e il networking.
Sii anche tu parte del cambiamento!

ANNULLIAMO LE DISTANZE

La piazza itinerante di IP Security Forum annullerà dunque le distanze - fisiche e soprattutto concettuali - tra parte congressuale e spazio espositivo, testimoniando che le "soluzioni di sicurezza" sono risposte tecnologiche a problemi estremamente concreti. Questo richiederà da un lato uno sforzo da parte delle aziende che esporranno, chiamate a mettere in mostra gli applicativi e il potenziale di problem solving racchiusi nelle tecnologie di sicurezza presentate, più che le "scatole" o i pezzi di ferro.

Paul Hennings e Josh Woodhouse all'edizione vicentina

Dall'altro lato si richiederà al pubblico uno sforzo di partecipazione e di coinvolgimento con la proposizione di casi concreti da sottoporre alle aziende e agli esperti in un ampio question time che spazierà dalle tecnologie alla privacy, dalle novità legislative ai trend di mercato.

LA COMMUNITY ALL'APPELLO

Questo sforzo, condiviso e inframmezzato da momenti ludici e conviviali, porrà le basi per la costruzione di una vera community delle tecnologie per l'IP Security: una rete di portatori di interessi simili e interconnessi che crescerà di dimensione e di valore al crescere dei suoi utenti.
Sarai dei nostri? L'appuntamento è a Bologna con nuove idee e sorprese: stay tuned!

www.ipsecurityforum.it

IP Security FORUM

6 MARZO 2014

• BOLOGNA •

Major Sponsor

AXIS COMMUNICATIONS

HIKVISION

VIDEOTREND

in collaborazione con

a&S ITALY
Tecnologie e soluzioni per la sicurezza professionale
www.asitaly.com

IP Security MAGAZINE
www.ipsecuritymagazine.com

secsolution
security online magazine
www.secsolution.com

registrati su www.ipsecurityforum.it

IP Security MAGAZINE
TECNOLOGIE, SOLUZIONI E APPLICAZIONI PER L'IP SECURITY
www.ipsecuritymagazine.it

ANNO 3 – Numero 9 – Dicembre 2013

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 L. Teruzzi, 15 - 20861 Brugherio (MB)

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 - bimestrale

Privacy (banche dati)
Le finalità del trattamento dei dati dei destinatari del Periodico consiste nell'assicurare informazioni tecniche e specializzate a soggetti che per la loro attività sono interessati ai temi trattati. Tali dati sono trattati nel rispetto del D.Lgs. 196/2003. Responsabile del trattamento dei dati raccolti in banche dati ad uso redazionale è il direttore responsabile a cui gli interessati potranno rivolgersi per esercitare i diritti previsti dall'art. 7 del D. Lgs. 196/2003

Grafica / impaginazione
zeronovecomunicazione.it

Ethos Media Group sr.l è associata ad ANES

WEBSITE

secsolution
security online magazine

security magazine online

www.secsolution.com è il portale d'informazione di riferimento b2b per i professionisti della security in Italia.
In soli quattro anni di operatività, **www.secsolution.com** si è consolidata come piattaforma autorevole di aggiornamento in materia di sicurezza fisica ed elettronica. Studiato per essere massimamente usabile, **www.secsolution.com** è un portale dalla navigazione intuitiva e che contiene un motore di ricerca interno selezionabile per tecnologia, brand e parole chiave. L'ampia gamma di sezioni tematiche, abbinata ad un vasto parco multimediale con audio, video, interviste e trailer di eventi, copre tutte le tematiche di interesse per gli operatori: da quelle strettamente tecnologiche a quelle normative, da quelle economico-fiscali alla formazione professionale, fino alle curiosità. L'update quotidiano seguibile anche su Twitter, e la frequentatissima newsletter, inviata a cadenza settimanale ad un target altamente profilato, chiudono il cerchio dell'aggiornamento settoriale.

secsolution.com

il security magazine online
Per un aggiornamento
giornalistico quotidiano,
interattivo e ricco
di spunti e contenuti.

ETHOSMEDIAGROUP
GLOBAL MULTIMEDIA CHANNEL

Ethos Media Group s.r.l.
Via L. Teruzzi, 15
20861 Brugherio (MB) Italy
Fax +39 039 3305841
ethos@ethosmedia.it
www.ethosmedia.it