GIUGNO 2014 - ANNO 4 N. 12

ETHOS MEDIA GROUP
GLOBAL MULTIMEDIA CHANNEL

IP Security MAGAZINE

TECNOLOGIE, SOLUZIONI E APPLICAZIONI PER L'IP SECURITY

Video IP: cosa considerare prima di cablare

Anche Bari ha detto sì a IP Security Forum

Niente più regole per installare Reti e Sistemi Elettronici e Digitali

Cloud ed imprese: Linee Guida della Commissione Europea

www.ipsecuritymagazine.it

SOMMARIO

GIUGNO 2014 – ANNO 4 – N. 12

ETHOSMEDIAGROUP
GLOBAL MULTIMEDIA CHANNEL

IP Security MAGAZINE

TECNOLOGIE, SOLUZIONI E APPLICAZIONI PER L'IP SECURITY

3 **EDITORIALE**

Nel cuore della convergenza
con la *business intelligence*

4 **EVENTI**

Anche Bari ha detto sì
a IP Security Forum

7 **LE INDAGINI**

Molti professionisti IT
vorrebbero rivedere i sistemi
di sicurezza aziendale
La Redazione

10 **Crouching Yeti:**
una campagna di spionaggio ancora
in corso con oltre 2.800 obiettivi
importanti in tutto il mondoe
La Redazione

14 **CHIEDI AL LEGALE**

Cloud ed imprese:
Linee Guida della
Commissione Europea
Roberta Rapicavoli

17 **CHIEDI ALL'ESPERTO**

Niente più regole
per installare Reti e Sistemi
Elettronici e Digitali
Eros Prosperi

19 **Video IP:**
cosa considerare prima di cablare
La Redazione

26 **FOCUS PRODUCT**

La prima speed dome
2MP Full HD 32 x zoom ottico PTZ

28 **Analisi video e security**
per retail e non solo

24 **APPLICATION CASE**

Videosorveglianza IP end-to-end
per l'aeroporto East Midlands

32 **Videosorvegliare gli accessi**
di una multinazionale dell'IT

35 **Sicurezza e domotica via IP**
per un'importante industria avicola

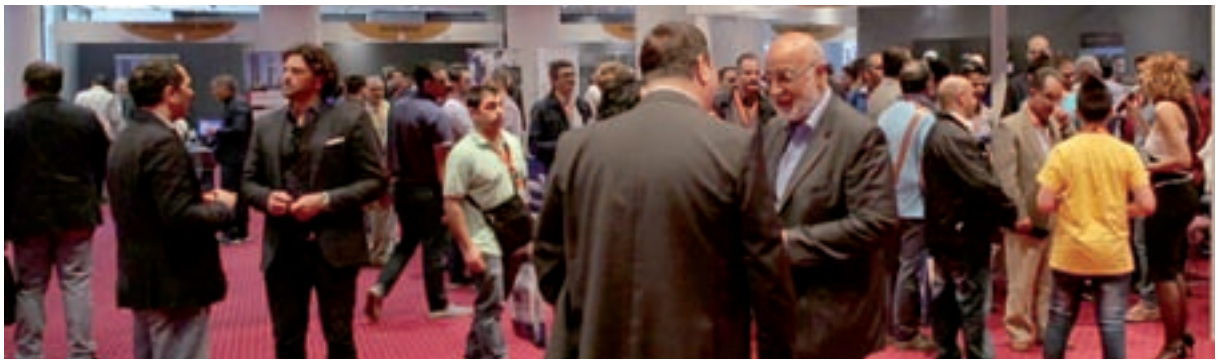
guarda ascolta scarica

Nel cuore della convergenza
con la *business intelligence*

Convergenza, in senso figurato, significa punto di sintesi di diverse informazioni. Riportata nel nostro settore, si può rappresentare con una sola interfaccia capace di collazionare, valutare e gestire tutti i sistemi che generano, rilevano e utilizzano dati...o anche solo con un uso più articolato dei dati già individuati. Di questo aspetto comincia ad accorgersi anche l'ingessato mondo della security fisica (l'unico settore ad alta vocazione tecnologica che ancora non è migrato totalmente verso l'IP), soprattutto nel più evoluto segmento della videosorveglianza, dove i metadati - dati che forniscono informazioni su altri dati - cominciano, seppur a rilento, ad essere considerati come strumenti non solo per dare più efficienza ai sistemi di sicurezza, ma anche per incrementare il business del cliente. Un esempio? Immaginiamo quante variabili potrebbero cambiare in un continuo flusso di soggetti/oggetti in un aeroporto gremito: utilizzando i metadati si può tracciare ogni oggetto e "comprenderlo" in modo finora inimmaginabile (capendo che cos'è, se è fermo o in movimento, quanto misura, per quanto tempo sta sulla scena, dove si trova in un certo frame e in un certo momento, etc). Questa comprensione profonda rivoluziona il modo di intendere il dato video, che non è più inteso solo come una sequenza di immagini utile per individuare ogni potenziale minaccia (nell'esempio di prima, eventuali atti terroristici), ma anche come elemento di business intelligence (sempre nell'esempio di prima, la rilevazione di un assembramento può essere intesa non solo come minaccia, ma anche come "punto caldo" di un aeroporto ove occorre aumentare il personale addetto alle informazioni, eliminandolo magari dalle "aree morte"). Per far sì che questa convergenza si completi, però, occorre avviare un cambio di paradigma nella mentalità di chi si occupa di security fisica, che già da tempo lavora a braccetto con chi si occupa del network IT ma che è tuttora spesso visto come un ingombrante intruso. Per far questo occorre che anche chi si occupa di security fisica conosca le minacce che incombono sulla rete. Ecco perché questo numero riporta, per cominciare, due indagini sulle vulnerabilità aziendali e sui principali metodi di attacco ai network.

Anche Bari ha detto sì
a IP Security Forum

La spumeggiante piazza di Bari non ha tradito le aspettative! Gli operatori della Puglia, polo tecnologico d'eccellenza per l'ICT, hanno infatti affollato gli stand e seguito fino all'ultimo speech la penultima tappa del 2014 di IP Security Forum, che ha chiuso i battenti il 4 giugno scorso con grande soddisfazione di espositori e visitatori.
Da rimarcare la presenza di molti prestigiosi vendor, che hanno portato nella piazza itinerante di IP Security Forum il loro knowhow e le loro ultime tecnologie, con due lanci in anteprima europea.
Da rimarcare, ancor prima, l'alta profilazione e lo straordinario livello di attenzione e partecipazione della platea, davvero instancabile nel seguire appieno la ricca offerta formativa della giornata.



articolarmente apprezzato da visitatori e sponsor, l'innovativo **format** di *IP Security Forum*, già collaudato al Nord ma al suo debutto nella piazza meridionale: un percorso in cui il pubblico veniva letteralmente "preso per mano" ed accompagnato attraverso e lungo gli stand, per acquisire una formazione tecnica capace di spaziare dalla teoria alla pratica senza soluzione di continuità.
Fondamentale poi per la riuscita dell'evento, lo sforzo delle aziende espositrici, che hanno saputo enfatizzare gli **applicativi** e le capacità di integrazione e di *problem solving* racchiuse nelle soluzioni di sicurezza, più che i singoli prodotti.
Fondamentale infine il **linguaggio** della parte più squisitamente formativa: un registro franco e diretto, "da tecnici a tecnici", che ha posto al centro del triplo momento formativo pomeridiano i possibili conflitti tra security tecnologica e privacy, la progettazione degli impianti IP video e le modalità per installare sicurezza nel modo più corretto e con la giusta modulistica.
Il risultato di queste sinergie è stata una giornata dedicata non solo alla videosorveglianza su IP, ma anche all'antintrusione, alla domotica e alla building automation, al networking e a tutti i segmenti della sicurezza fisica che già utilizzano o che stanno migrando verso l'IP e al cloud computing.

GRAZIE A VOI

Ci preme ringraziare le **istituzioni del territorio**, che hanno risposto con sincero entusiasmo, testimoniando l'attenzione dell'amministrazione e dell'industria locale verso le iniziative di formazione professionale volte a promuovere la convergenza tra operatori della security tradizionale e mondo IT/networking. Non meno importanti, i patrocini delle tantissime **associazioni legate al comparto sicurezza**, che hanno accompagnato e sostenuto l'intera campagna di comunicazione e diversi momenti formativi. Last but not least, un caloroso GRAZIE va agli **sponsor** e ai **partner** di *IP Security Forum* che, in una congiuntura certamente ancora complessa, hanno scelto di investire in formazione, scommettendo ancora una volta sulla crescita e sul futuro professionale del comparto sicurezza. GRAZIE quindi a quanti hanno reso possibile questo importante momento formativo: Axis Communications, Canon Italia, D-Link Mediterraneo, Electronic's Time, Elmat, Europlanet, For.tech, Hikvision Italy, Honeywell Security Group, Indigovision, Inim Electronics, Jvc Professional Europe, Marss, Panasonic Italia, Pelco by Schneider Electric, Risco Group, Samsung Techwin Europe, Satel Italia, Videotrend.

L'ultima tappa del roadshow 2014 si chiude alla Fiera di Milano-Rho, in seno alla mostra-convegno SICUREZZA, dal 12 al 14 novembre 2014: stay tuned on *IP Security Magazine!*

Defining the future landscape of security

Register at ifsec.co.uk/IFAD11

17-19 June 2014, ExCeL London

IFSEC International

COMMERCIAL & GOVERNMENT SECURITY

17-19 JUNE 2014 EXCEL LONDON UK

Bringing together the entire buying chain at the largest security industry event

Providing an opportunity for the security industry to discover the latest technology and insight at ExCeL London. With top class education sessions in the IFSEC Academy and the leading solutions from the key players, IFSEC International attracts a global audience keen to discover what's in store for the future of security. We're looking forward to seeing you in London!

#LondonCalling @IFSEC

Physical Security & Perimeter Protection | Smart Buildings | Video Surveillance | Access Control & Intruder Alarms | IT & Cyber Security | Integrated Security | Safe Cities

PART OF PROTECTION & MANAGEMENT 2014

Organised by UBM

La Redazione

Molti professionisti IT vorrebbero rivedere i sistemi di sicurezza aziendale

Websense ha presentato i nuovi risultati della ricerca "Roadblocks, Refresh, & Raising the Human Security IQ", condotta a livello mondiale dal Ponemon Institute. Tale ricerca dimostra che esistono alcuni problemi di comunicazione tra professionisti della sicurezza IT e vertici aziendali, che vi sono tuttora scarse conoscenze nell'ambito della sicurezza IT sia tra i dirigenti che tra i dipendenti ed evidenzia in generale il desiderio di rivedere gli attuali sistemi di sicurezza. La ricerca, che ha coinvolto circa 5.000 professionisti IT a livello mondiale, ha rivelato quindi un gap nelle conoscenze e nelle risorse disponibili all'interno delle aziende, determinando una maggiore vulnerabilità e il rischio superiore di subire attacchi data theft.

"Questa ricerca sulla sicurezza del Ponemon Institute evidenzia che la mancanza di comunicazione e formazione e l'esistenza di sistemi di sicurezza inadeguati permettono ai criminali informatici di attaccare le aziende di tutto il mondo" - ha dichiarato John McCormack, Websense CEO. "Non bisogna sorprendersi che molti responsabili della sicurezza siano delusi dal livello di protezione offerto dalle soluzioni installate, dal momento che spesso si tratta di soluzioni legacy, che non riescono a bloccare la catena di un attacco per prevenire il furto dei dati".
Il report "Roadblocks, Refresh, & Raising the Human Security IQ" ha coinvolto i professionisti IT con un'esperienza di circa 10 anni provenienti da 15 Paesi: Australia, Brasile, Canada, Cina, Francia, Germania, Hong Kong, India, Italia[1], Messico, Paesi Bassi, Singapore, Svezia, Regno Unito e Stati Uniti. I risultati ottenuti a livello mondiale evidenziano che le aziende sono d'accordo nel dover risolvere il divario di comunicazione tra i team di sicurezza e i dirigenti per proteggersi contro gli attacchi avanzati data steal. Per quanto riguarda il mercato italiano, i risultati evidenziano:

OSTACOLI NELLA COMUNICAZIONE TRA PROFESSIONISTI IT E DIRIGENTI

- il 30% dei team di cyber sicurezza non parla mai con i dirigenti in merito alla sicurezza informatica;
- tra quelli che invece lo fanno, circa un quarto (22%) affronta l'argomento solo una volta all'anno, mentre il 16% ogni sei mesi. Solo il 4% lo fa con una frequenza settimanale;
- solo il 44% crede che la propria azienda investa abbastanza in personale qualificato e tecnologie efficaci per portare avanti gli obiettivi aziendali di sicurezza informatica.

I PROFESSIONISTI DI SICUREZZA CHIEDONO UN REFRESH COMPLETO DEI SISTEMI DI SICUREZZA

- il 32% degli intervistati farebbe una revisione completa dei sistemi di sicurezza installati in azienda, se avesse a disposizione le risorse necessarie;
- quasi la metà (48%) è spesso delusa dal livello di protezione della soluzione di sicurezza che ha a disposizione;

[1] In Italia la ricerca ha coinvolto 250 professionisti IT e addetti alla sicurezza IT con una media di 13 anni di esperienza nel settore

- il 51% crede che il furto dei dati possa essere causato da un cambiamento del vendor di sicurezza;
- gli attacchi APT e di data exfiltration sono le principali preoccupazioni dei professionisti della sicurezza IT;
- solo un terzo, il 31%, dichiara che sta pianificando importanti investimenti e miglioramenti delle proprie difese informatiche nei prossimi 12 mesi.

AUMENTARE IL QI DELLA SICUREZZA UMANA

- solo il 44% crede che la propria azienda investa abbastanza in personale qualificato e tecnologie efficaci per raggiungere gli obiettivi di sicurezza informatica;
- il 41% delle aziende non forma i propri dipendenti in merito alla sicurezza informatica;
- l 31% è stato sottoposto a un processo di creazione di modelli nel loro ruolo attuale. Tra questi, quasi tutti (94%) lo hanno trovato importante in termini di gestione dei rischi informatici;
- secondo i professionisti di sicurezza, i tre principali eventi che potrebbero obbligare i dirigenti a destinare budget superiori volti a garantire la sicurezza informatica sono: furto della proprietà intellettuale (69%), perdita di fatturato a causa di un downtime del sistema (51%) e data breach che coinvolgono i dati dei clienti (49%).

“Le minacce avanzate e gli attacchi di data exfiltration sono le principali preoccupazioni per i professionisti della sicurezza IT” - ha dichiarato il Dr. Larry Ponemon, chairman and founder of the Ponemon Institute. “Queste preoccupazioni si manifestano perché credono che la propria tecnologia abbia bisogno di una revisione e che ci sia un divario crescente nella condivisione delle conoscenze e delle risorse tra i professionisti della sicurezza IT e lo staff dirigenziale. E’ incoraggiante però che la ricerca riveli per il futuro dei progetti di investimento nella tecnologia e nella formazione”.

www.websense.com/triton

La Redazione

Crouching Yeti:
una campagna di spionaggio ancora in corso con oltre 2.800 obiettivi importanti in tutto il mondo

Kaspersky Lab ha pubblicato un'analisi approfondita del malware e dell'infrastruttura server di comando e controllo (C&C) che fanno parte della campagna di cyber-spionaggio chiamata *Crouching Yeti* dal Global Research and Analysis Team di Kaspersky Lab (GreAT). L'inizio della campagna risale alla fine del 2010 ma risulta attiva ancora oggi e miete nuove vittime ogni giorno.
Vediamo di cosa si tratta.

Energetic Bear/Crouching Yeti è coinvolto in una serie di campagne composte da attacchi persistenti di tipo avanzato (APT). Secondo la ricerca di Kaspersky Lab, le vittime riguardano un più ampio numero di imprese di quante previste inizialmente. I settori nei quali sono state identificate il maggior numero di obiettivi raggiunti sono: industriale/meccanico; manifatturiero; farmaceutico; costruzioni; istruzione; Information Technology. Il numero totale di "vittime" accertate è di oltre 2.800 in tutto il mondo, tra le quali i ricercatori di Kaspersky Lab hanno identificato ben 101 organizzazioni. La lista degli obiettivi colpiti indica che l'interesse di Crouching Yeti è rivolto agli obiettivi strategici, ma non solo: dimostra anche interessi verso istituzioni non così ovvie per la loro importanza. Gli esperti di Kaspersky Lab credono che potrebbe trattarsi di "vittime collaterali", per cui potrebbe essere più opportuno considerare Crouching Yeti non solo come una campagna che mira ad una specifica area di interesse, ma come una campagna più ampia che rivolge il proprio interesse a diversi settori. Le organizzazioni vittime di questa campagna si trovano per lo più negli Stati Uniti, Spagna, Giappone, Germania, Francia, Italia, Turchia, Irlanda, Polonia e Cina. Data la natura delle vittime che sono state colpite, l'impatto che questa campagna potrebbe avere su queste organizzazioni è la divulgazione di dati sensibili come informazioni commerciali riservate e know-how.

TOOL NOCIVI CON DIVERSI MODULI AGGIUNTIVI

Crouching Yeti è sicuramente una campagna moto sofisticata. Ad esempio, i criminali che si nascondono dietro a questo attacco non hanno utilizzato nessun exploit zero-day, solo exploit facilmente recuperabili su Internet. Ma questo non ha impedito alla campagna di rimanere nascosta per diversi anni. I ricercatori di Kaspersky Lab hanno trovato prove dell'esistenza di cinque tipi di strumenti nocivi utilizzati dagli aggressori per impossessarsi di informazioni preziose dai sistemi compromessi: Havex Trojan; SysMain Trojan; Backdoor ClientX ; Backdoor Karagany e stealer collegati; Lateral movement e tool second stage. Lo strumento più utilizzato è l'Havex Trojan. In totale i ricercatori di Kaspersky Lab hanno scoperto 27 versioni diverse di questo programma dannoso e diversi moduli aggiuntivi, tra cui alcuni strumenti finalizzati alla raccolta di dati provenienti da sistemi di controllo industriale. Per il comando e controllo, Havex e gli altri strumenti

nocivi usati da Crouching Yeti si connettono a una vasta rete di siti web violati. Questi siti ospitano informazioni sulla vittima e smistano comandi ai sistemi infetti oltre che moduli di malware aggiuntivi. L'elenco dei moduli scaricabili include strumenti che servono per rubare password e contatti di Outlook, catturare screenshot e moduli per la ricerca e il furto di alcuni tipi di file: documenti di testo, fogli di calcolo, database, file PDF, unità virtuali, file protetti da password, chiavi di sicurezza pgp, e così via.

SPIONAGGIO INDUSTRIALE

Allo stato attuale Havex Trojan è noto per avere due moduli molto speciali finalizzati a raccogliere e trasmettere ai criminali i dati provenienti da specifici ambienti IT industriali. Il primo è il modulo scanner OPC. Questo modulo è progettato per raccogliere dati estremamente dettagliati sui server OPC in esecuzione nella rete locale. Tali server sono di solito utilizzati negli ambienti in cui sono in funzione diversi sistemi di automazione industriale. Il modulo scanner OPC è accompagnato da uno strumento di scansione della rete. Questo modulo è progettato per eseguire la scansione della rete locale, cercare tutti i computer collegati alle porte relative al software OPC/SCADA e provare a connettersi a tali host per individuare quale potenziale sistema OPC/SCADA sia in esecuzione e trasmettere tutti i dati raccolti ai server di comando e controllo.

ORIGINE MISTERIOSA

I ricercatori di Kaspersky Lab hanno osservato diverse caratteristiche che potrebbero lasciar intendere la nazione d'origine dei criminali che si nascondono dietro questa campagna malware. In particolare, hanno eseguito l'analisi della marcatura oraria di 154 file concludendo che la maggior parte dei campioni sono stati compilati tra le 6:00 e le 16:00 UTC, che potrebbe corrispondere in pratica a qualsiasi paese in Europa cosi come nell'Europa dell'Est. Gli esperti hanno inoltre analizzato la lingua utilizzata. Le stringhe presenti nel malware analizzato sono in inglese (scritto da non-nativi). A differenza di altri ricercatori che si sono occupati di questa particolare campagna gli specialisti di Kaspersky Lab non hanno potuto arrivare alla conclusione che questi criminali avessero origine russa. Quasi 200 codici binari dannosi e il relativo contenuto operativo non presenta alcun contenuto in cirillico (o traslitterazione), a differenza invece di quanto osservato nei risultati documentati da Kaspersky Lab durante la ricerca di Ottobre Rosso, Miniduke, Cosmicduke, Snake e TeamSpy. Inoltre, sono stati trovati degli indizi che farebbero pensare a una provenienza francese e svedese. Nicolas Brulez, Principal Security Researcher di Kaspersky Lab, ha dichiarato: "Energetic Bear è stato il primo nome dato a questa campagna da Crowd Strike in base alla loro terminologia. Bear fa riferimento al paese di origine in quanto Crowd Strike ritiene che la campagna sia di origine russa. Kaspersky Lab sta ancora indagando su tutte i collegamenti esistenti; tuttavia, al momento non sono presenti prove sufficienti per stabilirne l'origine. Anche la nostra analisi dimostra che l'attenzione globale dei criminali è molto più ampia e non mira solo ai produttori di energia. Sulla base di questi dati, abbiamo deciso di dare un nuovo nome al fenomeno: lo Yeti ricorda un po' un orso, ma ha un'origine misteriosa." Gli esperti di Kaspersky Lab stanno continuando la loro indagine collaborando con le forze dell'ordine e i partner industriali. Il testo integrale della ricerca è disponibile su Securelist.com. I prodotti Kaspersky Lab rilevano ed eliminano tutte le varianti del malware utilizzato in questa campagna.

www.kaspersky.eu/it

Il festival ICT 2014 ti aspetta.
Save The Date, The Big Date.

@Mediolanum Forum - Assago (MI)

Networking, Sicurezza Informatica, Cybercrime, Cloud Computing, soluzioni Datacenter, Unified Communication & Collaboration, Internet, Web, Innovazione, Hacking, Programmazione, Sviluppo, Startup e decine di altri temi ti aspettano!

#festivalICT2014

info@festivalict.com
www.festivalict.com

Roberta Rapicavoli(*)

Cloud ed imprese: Linee Guida della Commissione Europea

Il 26 Giugno sono state presentate dalla Commissione Europea le "*New guidelines to help EU businesses use the Cloud*", aventi lo scopo di fornire un aiuto e un supporto per le imprese che intendano avvalersi di servizi in cloud. E' noto infatti che, nonostante la consapevolezza dei profili di criticità legati ai servizi in cloud, spesso le imprese (e soprattutto le PMI) non hanno una forza contrattuale tale da poter negoziare le clausole proposte dai fornitori, il cui contenuto talvolta non è definito in modo chiaro e non comprende, o considera solo in modo superficiale, aspetti invece centrali per la gestione del servizio, quali ad esempio quelli legati alla sicurezza o alla disponibilità dei dati immessi nei sistemi in cloud. Ma non solo. Talvolta, nel considerare i servizi offerti dai diversi fornitori, si riscontrano differenze di varia natura nei contenuti dell'accordo proposto, che investono perfino la terminologia adoperata, generando in tal modo difficoltà notevoli per l'impresa interessata al servizio che intenda effettuare una comparazione delle soluzioni presenti sul mercato. Proprio per tale motivo, al fine di superare detti limiti, far accrescere la fiducia delle imprese e agevolare la loro scelta nella fase di valutazione dei servizi, sono state elaborate, peraltro anche con la partecipazione di alcune società che operano nel settore, le Linee Guida in esame, in cui viene espressamente indicato, come strumento da adottare per raggiungere gli obiettivi perseguiti, quello della standardizzazione dei Service Level Agreements (SLA), ossia di quella parte del contratto in cui vengono definiti gli aspetti tecnici e giuridici relativi al servizio offerto.

(*) Avvocato www.consulentelegaleinformatico.it

In particolare, un primo aspetto di rilievo affrontato nel documento presentato dalla Commissione, è legato alla necessità di predisporre i Service Level Agreements con un linguaggio chiaro, comune, accessibile a livello globale, che segua le evoluzioni tecnologiche delle soluzioni innovative proposte, rivolte, appunto, ad un "pubblico globale", cui deve essere garantita la possibilità di confrontare i diversi servizi offerti. Così, al punto 2 delle Linee Guida, intitolato "Cloud SLA Vocabulary" vengono fornite le definizioni di importanti concetti in materia di cloud, cui i fornitori dovranno attenersi e ai quali le imprese potranno far riferimento in sede di valutazione e scelta del servizio cloud di interesse.

L'utilizzo di terminologia comune nei Cloud Service Legal Agreements è solo uno degli aspetti considerati. Ed infatti, nelle Linee Guida, si evidenzia che, sempre al fine di garantire una facile comparazione dei diversi servizi offerti ed accrescere la fiducia delle imprese interessate ad aderirvi, si rende necessario considerare e descrivere all'interno dei Service Level Agreements alcuni elementi fondamentali, quali: la disponibilità e l'affidabilità dei servizi cloud, la qualità dell'assistenza fornita dal provider dei servizi, l'ottimizzazione della gestione dei dati conservati in cloud, i livelli di sicurezza.

I profili analizzati hanno certamente notevole rilievo perché le Linee Guida, nell'indicare gli elementi che dovranno essere ricompresi all'interno dei SLA, precisano altresì i criteri e le specifiche che dovranno essere considerati. A tal proposito, ad esempio, in ordine alla gestione dei dati, le Linee Guida contengono specifiche indicazioni in ordine alle operazioni di cancellazione (che dovranno interessare tutti i server in cui i dati siano stati conservati, dovendosi infatti garantire la totale eliminazione di ogni file riferito all'utilizzatore del servizio una volta cessata la finalità perseguita) ed ai profili del trasferimento dei dati all'estero (per cui si richiede al fornitore di indicare nel dettaglio il luogo di allocazione dei server utilizzati per offrire il servizio, così da consentire all'impresa di effettuare le opportune valutazioni).

I requisiti e gli aspetti esaminati sono solo alcuni di quelli che dovranno essere considerati in fase di redazione dei Cloud Service Level Agreements, in base ai criteri e alle specifiche espressamente indicati nelle stesse Linee Guida, alcuni dei quali dovranno comunque essere valutati avendo riguardo al servizio cloud concretamente offerto.

In attesa del prossimo passo, ossia quello di testare le indicazioni contenute nel documento presentato dalla Commissione con le aziende e, in particolare, con le piccole e medie imprese interessate ai servizi cloud, deve certamente ritenersi positiva l'iniziativa che ha condotto all'elaborazione delle Linee Guida esaminate. Linee Guida che, secondo quanto espressamente dichiarato dal Vice Presidente della Commissione, Viviane Reding, "*accresceranno la fiducia delle aziende e dei cittadini europei nei nuovi servizi di cloud*", potendosi pertanto rinvenire quello stesso spirito che guida altre iniziative europee, quale quella della riforma in materia di protezione dei dati personali attraverso l'adozione del Regolamento Europeo, ancora in fase di approvazione.

23–26 SEPTEMBER 2014

The World's Leading Trade Fair for Security & Fire Prevention

THE NUMBER ONE FOR 40 YEARS

Meet exhibitors and safety experts from over 100 nations at the global marketplace. Discover new safety trends, exciting innovations and top-class forums. Seize your opportunity for know-how, networking and business!

MESSE ESSEN
Place of Events

www.security-essen.de

40 YEARS
security essen 2014
THE NUMBER ONE

Eros Prosperi(*)

Niente più regole
per installare Reti e Sistemi Elettronici e Digitali

"Ogni realizzazione di Reti e Sistemi fonia, dati, video va certificata con adeguata documentazione, per facilitare le attività di manutenzione e per costituire il necessario supporto per future scelte strutturali e tecnologiche degli IT Manager". Questo è il pensiero di Assotel, di recente confluita in Assistal - Confindustria. Un pensiero controcorrente, dal momento che l'abrogazione dell'art. 2 del DLgs. 198/2010 e del D.M. 314/92, assieme alla non applicabilità del DM 37/2008 (art. 2 comma f) ai Sistemi di Comunicazione Elettronica e Digitali interconnessi a Rete Pubblica, va in tutt'altra direzione. Ma al contempo genera un vuoto normativo che potrebbe mettere a rischio la tutela dei committenti e la valorizzazione delle Imprese serie.

(*) Vicepresidente Vicario Assotel

PARTE IL MATCHING DAY PROGRAM DI ASSOTEL

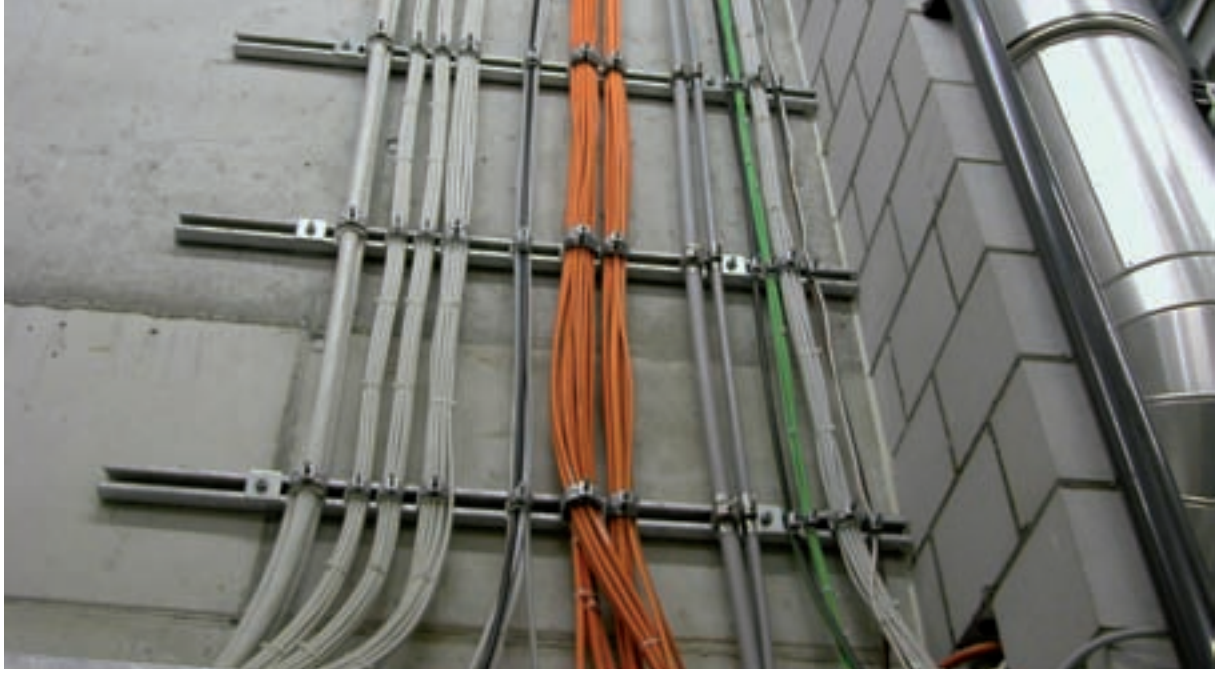
Per le imprese è oggi essenziale fare networking, soprattutto nei settori tecnologici, visto che il mercato richiede sempre più servizi integrati orientati al risultato. Le imprese associate ad **Assistal**, **Assotel** e **AIPS** possono a tal fine partecipare al **Matching Day Program**, il cui obiettivo è creare occasioni di incontro tra imprenditori, agevolando le relazioni tra le imprese e stimolando le sinergie. I Soci potranno attivare proficue collaborazioni, presentare le eccellenze della propria azienda e promuovere attività congiunte per sviluppare il business. Il modello operativo è quello dell'uno a molti: all'incontro, riservato a 10\12 persone, il rappresentante di un'azienda presenta infatti ai colleghi intervenuti la sua realtà e le competenze che può mettere a disposizione. Segue sempre un momento conviviale per approfondire singolarmente la conoscenza con gli intervenuti.
Il primo Matching Day è fissato per il 17 **Settembre 2014** presso la Sede Sociale di Via Restelli 3 (Milano). Seguiranno altre date ad ottobre e Novembre 2014. Per info e iscrizioni **www.assotel.it**

L'abrogazione delle specifiche disposizioni di legge che regolavano la fornitura, la realizzazione e il collaudo di reti e sistemi fonia, dati, video interconnessi o da interconnettere a Rete Pubblica di Comunicazione Elettronica e, quindi, a Internet rende difficile, ai Committenti pubblici e privati, l'individuazione delle Imprese che operano secondo la regola dell'arte, con organizzazione aziendale e competenze tecnico professionali adeguate, come richiesto anche dal Testo Unico Sicurezza, DLgs.81/08, art. 90 comma 9.

Per Assotel, l'Associazione Imprenditoriale di Categoria delle imprese che installano infrastrutture e apparati per fonia-dati-video sistemi, è, da sempre, indispensabile dare certezze esecutive ai Committenti, valorizzando e promuovendo la professionalità delle Imprese che installano reti e sistemi di telecomunicazioni e IP security.

Per questo - dice Eros Prosperi Vicepresidente Assotel – "*l'Associazione ha elaborato una Guida per l'Utente che indica alcune Prassi mirate a contrattualizzare correttamente l'iter progettuale, realizzativo e certificativo dei Sistemi interconnessi o da interconnettere alla Rete Pubblica di Comunicazione* Elettronica".

Di più: *"i Soci Assotel si sono auto-imposti di rilasciare ai Committenti un Attestato di Corrispondenza alla Regola dell'Arte, denominato AtCo".* Questo modulo, predisposto ed elaborato da una commissione mista di Imprenditori, Professionisti e Opinion Leader, attesta le modalità di realizzazione di Sistemi di Comunicazione Elettronica e Digitali, interconnessi a Rete Pubblica. Unitamente ad altri documenti (progetto, relazione tecnica, schema di numerazione delle connessioni cablate, schema a blocchi di posizionamento apparati, schema delle numerazioni e tipologie di accesso alla Rete Pubblica, nonché Certificazioni strumentali di quanto eseguito, l'**AtCo** (Attestato di Corrispondenza) è per i Soci Assotel l'elemento fondante di una cartella di documentazione che ogni accorto Committente dovrebbe richiedere alle Imprese fornitrici e conservare in azienda.



La Redazione

Video IP:
cosa considerare prima di cablare

È più facile che un cammello passi per la cruna di un ago che non trovare una rete senza passaggi complessi. Predisporre una rete adibita a trasportare le immagini di un sistema di videosorveglianza dal punto di ripresa a quello di visione o di memorizzazione è tutt'altro che un'operazione semplice. Anzi, proprio il sottovalutarla porta l'installatore a dover affrontare poi una serie di problematiche che spesso emergono solo in fase di cablaggio o, ancora peggio, quando l'impianto viene attivato. Questo perché, in molti casi, l'attenzione di chi progetta è focalizzata esclusivamente sul corretto posizionamento delle telecamere, dimenticando tutto quanto sia legato al percorso che i cavi devono compiere per assicurare il collegamento. Identificare dove far transitare questi cavi infatti non è semplice e può richiedere competenze o attrezzature molto particolari. Un problema che non riguarda solo gli edifici di pregio o quelli residenziali, ma investe anche le strutture industriali e produttive.

La presenza di motori elettrici o cavi di potenza può creare interferenze

Se parliamo di strutture residenziali, solitamente viene richiesto che i cavi rimangano nascosti alla vista, senza peraltro comportare interventi a livello di muratura. Questi ultimi, infatti, da un lato hanno costi elevati, dall'altro provocano evidenti disagi, soprattutto nel caso di edifici già occupati. Negli edifici storici, o di elevato valore artistico, poi, le sovraintendenze sono spesso intransigenti e non autorizzano nemmeno il posizionamento di canaline a vista. Un buon progettista, quindi, è chiamato in primo luogo a saper coniugare le esigenze legate alla sicurezza, con un'adeguata predisposizione delle telecamere, con la necessità di collegamento, sia per la trasmissione dei dati sia per l'alimentazione elettrica. In alcuni casi, l'impiego della tecnologia PoE (Power over Ethernet), che supporta il transito di energia e dati su un unico mezzo fisico, può contribuire a mitigare il problema, ma non lo elimina comunque completamente. "Dimenticarsi" di questi fattori può far lievitare significativamente i costi, con la conseguenza di dover poi presentare un consuntivo sostanzialmente diverso da quanto preventivato, scontrandosi quindi con il cliente finale. Questo anche alla luce del fatto che attrezzature speciali, come le elettroscale, non fanno quasi mai parte della comune dotazione di un'azienda di installazione, per cui devono essere noleggiate, con conseguente aumento delle spese.

PROTEZIONI PER TUTTI I GUSTI...

Riuscire a far transitare il cavo rappresenta solo la prima delle difficoltà di un'installazione. I cavi, infatti, non possono essere posati ovunque; occorre valutare la loro eventuale esposizione a fattori climatici e ambientali ostili. Aspetti che si possono superare scegliendo guaine di protezione adeguate. Il produttori propongono le soluzioni più svariate, in grado di resistere a eventi estremi, dall'attacco dei roditori a quello delle fiamme, passando attraverso la posa in acqua o la presenza di agenti chimici aggressivi. Tutte soluzioni che costituiscono comunque un costo aggiuntivo. Il tutto senza dimenti-

Una posa non corretta può compromettere la qualità delle immagini

care che, pur scegliendo la protezione più opportuna, si tratta comunque dell'aggiunta di un ulteriore fattore di instabilità. Queste soluzioni di solito offrono una barriera garantita solo per un certo arco temporale, relativamente limitato, costringendo quindi a successive spese di manutenzione, nonché a possibili disagi e malfunzionamenti, che potrebbero incidere negativamente sulla sicurezza. Il tutto senza contare che non si devono riempire le canaline per oltre il 50% dello spazio disponibile.

PERICOLO INVISIBILE

Il pericolo maggiore per una rete di trasmissione dei dati, arriva da un elemento invisibile: i campi elettromagnetici. Spesso si discute del possibile impatto negativo che le emissioni elettromagnetiche possono avere sulla salute. Per la comunicazione, invece, si sa già: i campi elettromagnetici, creati da cavi di potenza e motori elettrici, soprattutto in ambito industriale, o semplicemente dalla presenza di altre antenne, interferiscono pesantemente con i segnali in transito sui classici doppini in rame. Così, oltre a ridurre sensibilmente la qualità della trasmissione, possono indurre disturbi tali da impedire del tutto la comunicazione. La vulnerabilità delle reti ai rumori indotti dalla presenza di campi elettromagnetici cresce in base all'aumento della velocità e della frequenza di trasmissione. La direttiva EMC 89/336 CEE relativa alle emissioni elettromagnetiche, inserita nella Direttiva Macchine, obbliga il produttore a garantire la sicurezza degli impianti e/o delle apparecchiature industriali: la corretta e tempestiva trasmissione dei segnali costituisce dunque un fattore determinante in campo industriale, non solo per ottimizzare la produzione e ridurre al minimo eventuali onerosi fermi impianto, ma anche per la sicurezza, dal momento che un errore di comunicazione in ambito produttivo può rivelarsi pericoloso. I classici doppini in rame twistati, impiegati per la comunicazione anche in ambito manifatturiero, sono in grado di compensare parzialmente l'effetto delle interferenze provenienti dall'esterno. Presentano però il limite di essere efficaci

solo quando la fonte del disturbo è relativamente lontana o ha un'intensità poco elevata. In caso di ambienti estremi, invece, per difendersi dalle interferenze EMC occorre adottare delle schermature, essenziali nel caso di più doppini posti a breve distanza l'uno dall'altro. All'aumentare delle prestazioni, inoltre, si possono verificare fenomeni di diafonia fra le singole coppie di un medesimo cavo.

PRO E CONTRO DELLA SCHERMATURA

Le schermature possono riguardare i cavi che provocano il disturbo, oppure quelli che lo subiscono. Utilizzando cavi schermati del tipo Stp (Shielded Twisted Pair) si riesce a limitare l'interferenza reciproca fra singoli doppini, in quanto questi cavi sono realizzati con coppie schermate in modo individuale. Con la tipologia ScTP (Screened Twiested Pair), invece, ossia cavi da 100 Ohm ricoperti da uno schermo, si proteggono le comunicazioni dalle interferenze esterne, evitando che il campo indotto possa danneggiare altri cavi che siano posati a breve distanza. Gli schermi a nastro, infine, costituiti con un composto di alluminio/poliestere avvolto intorno ai conduttori o alle coppie twistate, hanno un costo relativo ma sopportano un numero ridotto di flessioni e torsioni ripetute, per cui non sono idonei a essere impiegati su sistemi in movimento. In questi ultimi casi è meglio optare per uno schermo "a spirale". Si tratta di una struttura costituita da un fascio o da capillari paralleli e inclinati rispetto all'asse del cavo, che viene avvolto sul cavo stesso o sui conduttori; è in grado di sopportare sollecitazioni meccaniche anche ripetute, con lo svantaggio che la copertura offerta nelle migliori condizioni possibili arriva solo al 97%.

Quando la protezione deve essere più elevata, nell'ordine del 98%, è più indicata la "calza", ossia uno schermo a treccia capace di bloccare tutte le frequenze. Ha infatti una struttura costituita da fasci di capillari paralleli, tessuti alternativamente in senso orario e antiorario, la cui inclinazione è determinata dal passo di avanzamento e dalla percentuale di copertura richiesta. La calza è in grado di resistere a lungo, anche se sottoposta a sollecitazioni ripetute, ma anche in questo caso la protezione non raggiunge il 100%. In presenza di comunicazioni particolarmente critiche occorre perciò utilizzare una schermatura "combinata", che si ottiene dalla sovrapposizione della treccia e del nastro di alluminio/poliestere. Si crea così una barriera in grado di assicurare una protezione assoluta, a fronte però di costi elevati. Ulteriore limite: in caso di torsioni e flessioni ripetute questa struttura si deteriora rapidamente, per cui è necessario provvedere a sostituzioni periodiche.

Fallo subito!

sec solution

Videosorveglianza IP end-to-end

per l'aeroporto East Midlands

STATO DI FATTO ED ESIGENZE DEL COMMITTENTE

L'aeroporto East Midlands è un importante snodo per gli spostamenti aerei dei passeggeri inglesi e ogni anno collega oltre 4 milioni di persone con oltre 90 destinazioni. Inoltre, è il più importante scalo aereo dell'Inghilterra per il trasporto di merci, ospita svariati operatori nel settore delle spedizioni aeree, quali DHL, TNT e UPS, ed è il principale snodo aereo utilizzato dalla Royal Mail.
Recentemente sono stati installati dei sistemi di videosorveglianza IP end-to-end di IndigoVision sono presso l'aeroporto East Midlands, che ora dispone di un sistema di analisi più dettagliato e di una maggiore capacità di archiviazione per le riprese di videosorveglianza.

LA TECNOLOGIA MESSA IN CAMPO

In collaborazione con il partner locale P&G Electrical, IndigoVision ha riutilizzato parte dell'infrastruttura e delle telecamere esistenti e ha aggiunto nuove telecamere ad alta definizione, 195 telecamere statiche e 18 telecamere PTZ. Si tratta di una combinazione di unità analogiche e IP collegate ai videoregistratori di rete (NVR) di IndigoVision. L'architettura distribuita e aperta del sistema video IP di IndigoVision rappresenta la piattaforma ideale per eseguire la migrazione degli impianti TVCC esistenti e assicurarne l'integrazione con altri sistemi di sicurezza.
L'avanzata tecnologia di compressione di IndigoVision limita le esigenze di archiviazione, rispettando, al tempo stesso, i requisiti per la conservazione delle riprese stabiliti dal governo. La procedura di esportazione delle riprese per un'eventuale analisi è stata altresì semplificata. Tutte le telecamere installate nell'aeroporto utilizzano ora la tecnologia Activity Controlled Framerate (ACF) di IndigoVision. L'ACF controlla il frame rate del flusso video della telecamera in base alla quantità di movimento presente nella scena. Tre workstation dotate di "Control Center" sono state installate per consentire il monitoraggio di più siti dalla zona di parcheggio, dalle postazioni di sicurezza e dai centri di controllo sulla pista.
Tra i principali vantaggi, si evidenziano: architettura distribuita e aperta, che consente l'integrazione con altri sistemi; monitoraggio da più siti; facilità di utilizzo e interfaccia intuitiva, esportazione semplificata delle riprese.

LA PAROLA ALLA COMMITTENZA

Il feedback degli utenti su Control Center è stato molto positivo, soprattutto in merito alle funzionalità di salvataggio, guard tour e riconoscimento degli allarmi, così come per quanto riguarda l'interfaccia intuitiva e facile da usare. John Doherty, Security General Manager dell'aeroporto East Midlands, ha dichiarato: "Con l'ausilio di nuove tecnologie, la soluzione IndigoVision ci ha permesso di rafforzare il monitoraggio della sicurezza e l'analisi delle riprese all'aeroporto. Siamo un'azienda di grandi dimensioni con più siti da monitorare e il sistema di videosorveglianza IP ci ha offerto una soluzione semplice da usare e capace di soddisfare tutte le nostre esigenze".

in breve

Location e committente:
Aeroporto East Midlands, UK

Tipologia di installazione:
videosorveglianza IP end-to-end

Vantaggi:
architettura distribuita e aperta, monitoraggio da più siti, facilità di utilizzo e interfaccia intuitiva, esportazione semplificata delle riprese.

Partner:
P&G Electrical

Brand:
Indigo Vision
www.indigovision.com/it

La prima speed dome
2MP Full HD 32 x zoom ottico PTZ

Samsung Techwin rafforza la sua nota famiglia di telecamere e dome camere open platform WiseNetIII con il lancio del modello SNP-6320, la prima speed dome al mondo 2MP Full HD e con zoom ottico 32 x PTZ. Oltre al potente zoom ottico 32 x, la speed dome SNP-6320, conforme allo standard ONVIF, prevede uno zoom digitale a 16 x che la rende una soluzione IP ideale per aeroporti, porti, parcheggi industriali e commerciali, e in tutti quegli ambienti ove siano richieste alte performance PTZ.

guarda il video

LIBERTÀ DI SCELTA

"La speed dome SNP-6320, assieme al modello vandal-resistant e idrorepellente SNP-6320H, che incorpora un sistema di riscaldamento alimentato a PoE+ che permette agli operatori di lavorare anche in condizioni climatiche estreme, rappresenta una *new entry* importante nella gamma open platform WiseNetIII di telecamere IP a 1.3, 2 e 3 megapixel e dome" - dichiara Tim Biddulph, Product Manager per la divisione Security Solution di Samsung Techwin Europe Ltd. "Con queste novità Samsung Techwin cambia il modo di lavorare nell'IP. Un punto chiave sono le possibilità open platform dei processori WiseNetIII DSP, che offrono agli utenti la massima libertà di scelta nella combinazione di videoanalisi e video management software (VMS) per soddisfare ogni volta al meglio le proprie necessità."

PER TUTTE LE CONDIZIONI AMBIENTALI

Il **Wide Dynamic Range** incorporato nel processore WiseNetIII DSP, portato ora a performance superiori ai 120dB, è in grado di produrre immagini molto accurate anche in scene che contestualmente contengono delle aree molto scure e delle aree molto chiare. Ma i modelli SNP-6320 e SNP-6320H offrono altre caratteristiche fondamentali: dal **Defog** (che rende nitide le immagini catturate in condizioni ambientali non ottimali a

causa di pioggia, fumo o nebbia) al **Digital Image Stabilization**, che annulla l'impatto negativo delle vibrazioni. Due caratteristiche particolarmente importanti per la protezione perimetrale di ambienti come porti e aeroporti. I due modelli sono anche dotati di audio bi-direzionale che permette di interfacciarsi con sistemi locali PA. Tutte queste caratteristiche sono state progettate per ridurre tempi e costi dell'installazione.

PER TUTTE LE CONDIZIONI DI LUCE

I modelli SNP-6320 e SNP-6320H catturano immagini a colori ad alta qualità anche quando il livello di illuminazione è di 0.03 Lux e garantiscono un frame rate elevatissimo di 60fps a 1080p. Queste dome possono inviare **molteplici flussi video a molteplici frame rate e risoluzioni**, in base al dispositivo che le riceve (registratore, software di visualizzazione o App per dispositivo mobile) - una caratteristica particolarmente importante quando sono coinvolti diversi interlocutori. L'utilizzo di banda contenuto grazie all'algoritmo di **compressione H.264** favorisce il controllo del tempo di latenza delle dome, rendendo il tracking manuale degli oggetti ancor più semplice e immediato. La memoria proprietaria SD/SDHC/SDXC permette agli utenti autorizzati di accedere da remoto e di scaricare i video registrati sulla **memory card**. I nuovi modelli sono infine equipaggiati con **Intelligent Video Analytics** (IVA), che assiste gli operatori nella rilevazione di vari elementi e comportamenti (rilevazione volto, esplosivi, direzione in entrata/uscita, oggetto scomparso/apparso, tampering – funzione che crea un allarme se la lente di una telecamera viene oscurata da spray o se è soggetta ad un movimento/angolo di visuale diversi da quelli consueti).

STRATEGIA A PIATTAFORMA APERTA

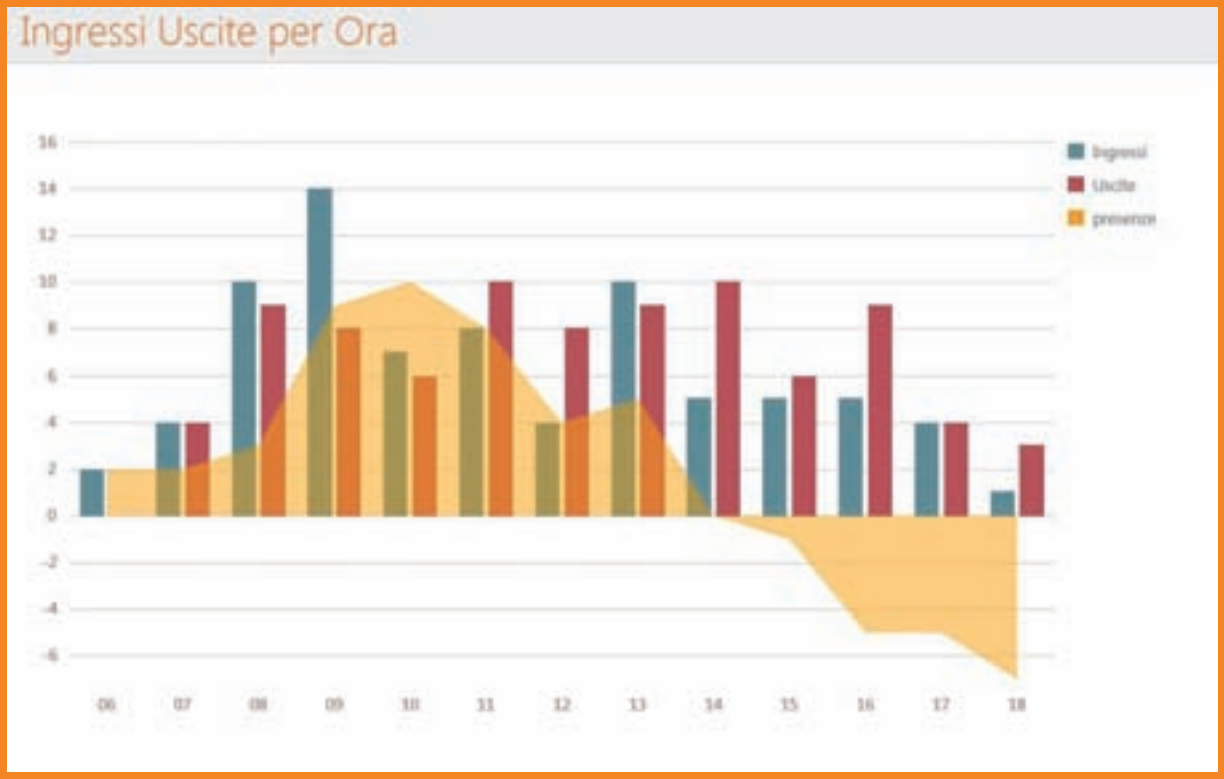
Questa strategia "open" affonda le radici nella necessità, avvertita al massimo nella presente situazione congiunturale da aziende ed istituzioni, di garantirsi benefici di lungo termine derivanti dall'investimento in videosorveglianza, quindi "a prova di futuro" in termini di espandibilità del sistema e di futura integrazione con nuove tecnologie. Ecco perché le potenzialità open platform del processore WiseNetIII DSP sono il vero "cuore" delle telecamere e dome di ultima generazione: una piattaforma veramente aperta permette infatti agli utenti di uploadare senza problemi delle **App** e di farle girare su qualunque telecamera o dome camera WiseNetIII. Per fare un esempio, le App possono attivare le funzioni di videoanalitica: un commerciante potrà quindi facilmente utilizzare un'App di videoanalisi della AgentVI, che offre una soluzione di business intelligence basata sul comportamento dei clienti nel negozio con le mappe delle "aree calde" su base oraria/giornaliera/settimanale, per implementare il suo merchandising e per identificare ad esempio dove collocare l'area promozioni o i prodotti a minore vendibilità. Analogamente, il personale di sicurezza di alcune aree sensibili potrebbe voler utilizzare l'App di videoanalisi di Foxstream, che è ideale per le applicazioni perimetrali. La libertà è totale.

SAMSUNG TECHWIN EUROPE
Viale Brianza, 181
20092 Cinisello Balsamo (MI)
Tel: +39 02 38608228
Fax: +39 02 38608901
stesecurity@Samsung.com

www.samsungsecurity.com

Analisi video e security
per retail e non solo

roteggere beni e persone, monitorare e analizzare aree sensibili, prevenire crimini o incidenti sono esigenze che riguardano molte realtà come scuole, negozi, aeroporti, chiese, stadi, ospedali, banche e centri commerciali. La possibilità di adottare una soluzione che garantisca la sicurezza e al contempo fornisca l'analisi dei flussi di persone e degli approcci comportamentali di fruizione di questi ambienti, è fondamentale per i responsabili di queste attività. Canon ha messo a punto una soluzione di Video-Analisi e Business-Intelligence chiamata **Canon Business Imaging Intelligence**.



ANALISI DEI FLUSSI

Questo sistema è stato specificatamente studiato per il settore retail, ma è ideale anche per tutti gli ambienti in cui si renda necessario monitorare l'affluenza di pubblico. **Canon Business Imaging Intelligence** abbina le caratteristiche di una videocamera di sicurezza a quelle di uno strumento destinato all'analisi video per la raccolta di dati statistici. Offre molteplici applicazioni utili per le diverse realtà commerciali ed è in grado di fornire diverse informazioni sia di carattere quantitativo che qualitativo, come ad esempio il conteggio in tempo reale del flusso di persone che entrano o escono da un'area specifica oppure l'analisi dei flussi di utenti rilevati in determinati intervalli di tempo. Questo sistema è poi in grado di stimare il numero di persone presenti all'interno di uno spazio commerciale a partire dalla somma di ingressi e uscite per tutti i varchi di accesso, nonché di calcolare in tempo reale il numero di persone presenti in una delimitata area (ad esempio un reparto, vetrina o scaffale) e il loro tempo di permanenza.

ZONE CALDE E ZONE FREDDE

Un altro dato interessante fornito da **Canon Business Imaging Intelligence** è la stima della percentuale di occupazione di aree virtuali da parte di soggetti di interesse, e per ciascuna area è in grado di segnalare il superamento di una certa soglia percentuale. Grazie a questi dati il sistema è in grado di effettuare una stima e una mappatura delle "zone calde" e "zone fredde", ovvero delle zone con maggiore o minore presenza di persone in un determinato intervallo di tempo all'interno di aree virtuali. Le strutture commerciali, e non solo, possono utilizzare questa informazione per analizzare in modo sistematico il livello di affollamento all'interno di un'area specifica, piuttosto che per

visualizzare su mappa grafica le aree con maggior presenza di persone in un intervallo temporale stabilito. In questo modo sarà possibile ottimizzare anche le risorse dedicate ai singoli reparti: personale, energia elettrica, climatizzazione, etc..
Un'importante caratteristica della soluzione Canon risiede nella flessibilità nella consultazione dei dati, infatti è in grado di fornire tutte le informazioni statistiche relative ai comportamenti delle persone all'interno di precise aree virtuali in modalità differenti grazie alle dashboard personalizzabili, offrendo di fatto preziose analisi statistiche ai fini delle strategie di marketing. I dati e le statistiche messi a disposizione da **Canon Business Imaging Intelligence** possono avere un forte impatto a livello di strategie di merchandising: capire quali sono i percorsi più *battuti*, analizzare come i clienti si avvicinano ai prodotti esposti, esaminare l'efficacia dei punti display, valutare visivamente l'impatto delle attività promozionali, sono tutte informazioni che possono aiutare ad apportare le corrette modifiche al layout di uno store e ottimizzare l'esperienza d'acquisto. La soluzione Canon è poi un importante strumento anche ai fini di sicurezza: se implementata in base a queste specifiche, è in grado di calcolare il percorso delle persone all'interno di aree virtuali, di conseguenza la rilevazione di un movimento anomalo o improvviso, di un singolo o di una folla, potrebbe significare un pericolo, e il sistema intelligente di Canon è in grado di garantire interventi tempestivi e risolutivi. **Canon Business Imaging Intelligence** lavora nel pieno rispetto delle normative in merito della tutela della privacy, elaborando i flussi video in tempo reale, producendo solo dati statistici e senza che nessuna immagine venga archiviata: un altro motivo per scegliere Canon come partner ideale per la consulenza e lo sviluppo delle soluzioni tecnologicamente più avanzate in grado di conoscere, incrementare e consolidare il business.

CANON ITALIA
Strada Padana Sup 2/B
20063 Cernusco Sul Naviglio – MI
Tel. +39 02 82482276
Fax +39 02 82484276
VCC.PROIG@canon.it

www.canon.it

SICUREZZA

Biennale Internazionale di Security & Fire Prevention

Fiera Milano (Rho) 12.14 NOVEMBRE 2014

Follow us on

RISPARMIA TEMPO E DENARO!

Registrati e acquista il biglietto al 50% su **www.sicurezza.it**

THE INTERNATIONAL NETWORK

EXPOSEC
San Paolo - Brasile 13.15 Maggio 2014

XX FISP
San Paolo - Brasile 08.10 Ottobre 2014

EXPO MILANO 2015

FIERA MILANO

Official Partner

Videosorvegliare gli accessi
di una multinazionale dell'IT

STATO DI FATTO ED ESIGENZE DEL COMMITTENTE

NTT DATA è un'azienda multinazionale – con headquarters localizzati in Giappone – che fornisce servizi professionali nel settore IT, spaziando dalla consulenza allo sviluppo dei sistemi fino all'outsourcing. Aiutando i Clienti a realizzare innovazione, NTT DATA sviluppa nuove soluzioni per bisogni futuri. Nata con il nome di NTT (Nippon Telegraph and Telephone), NTT DATA contribuisce a diffondere una mentalità basata sulla "qualità" prima di ogni altra caratteristica. Quotata in Borsa dal 1995, continua anche oggi il suo percorso rivolto alla costante innovazione per fornire soluzioni IT a clienti di oltre 35 Paesi. Per monitorare gli accessi, NTT DATA si è affidata alla tecnologia di videosorveglianza IP firmata D-Link, tramite il suo partner STT Servizi Telematici Telefonici.

LA TECNOLOGIA MESSA IN CAMPO

L'impianto è pensato per la protezione di edifici e dipendenti, ospiti e manutentori, attraverso il monitoraggio degli accessi anche fuori dall'orario di ufficio. Quello per NTT DATA Italia è un progetto in divenire, del quale ad oggi sono stati ultimati i primi due step: due sedi sono già state completate, la terza è quasi pronta; a fine progetto, le strutture protette da videosorveglianza D-Link saranno quelle di Milano, Roma, Torino, Napoli, Treviso, Pisa e Cosenza. A pieno regime, il progetto vedrà l'installazione di 80 Videocamere Dome D-Link DCS-6113, dotate di un sensore CMOS progressivo a 2 megapixel, compressione H.264, visibilità notturna e supporto PoE, ideali per installazioni a soffitto e in ampi spazi e perfette per il video monitoring ad alta definizione 24/7.

Le videocamere DCS-6113 Full HD Day & Night montano un filtro ICR e forniscono immagini nitide e con un eccezionale livello di dettaglio anche in condizioni di scarsa illuminazione o di oscurità totale, a colori durante le ore diurne e in scala di grigi di notte. Grazie alla compressione video H.264, MPEG-4 e MJPEG di alta qualità, queste videocamere supportano lo streaming simultaneo e consentono lunghe registrazioni pur mantenendo un incredibile livello di dettaglio: queste caratteristiche rendono la DCS-6113 un prodotto largamente utilizzato per le soluzioni di videosorveglianza. Per quanto riguarda le aree esterne la scelta è ricaduta sui modelli DCS-6314 e DCS-6513.

Entrambe sono Videocamere Dome FullHD Day & Night e dispongono di Wide Dynamic Range (WDR): questa caratteristica garantisce una qualità delle immagini migliorata anche in condizioni di illuminazione non omogenea o insufficiente, in modo da permettere di identificare soggetti retroilluminati o posizionati in aree sovrailluminate.

Rispetto alla DCS-6314, la più potente DCS-6513 è in grado di vedere fino a 20 metri in condizioni di totale oscurità (5 metri in più della DCS-6314), ha un sensore CMOS da 3 megapixel contro i due della DCS-6314 ed è dotata di lente P-IRIS motorizzata.

Le immagini riprese sono registrate dagli NVR D-Link e permettono la ricerca di eventi come accessi non autorizzati, furti o atti vandalici. Le registrazioni sono garantite, nei termini di legge, dai 15 Network Video Recorder (NVR) a due scomparti DNR-326, semplici da installare e configurare grazie all'interfaccia intuitiva dalla quale è possibile gestire l'intero sistema. Il sistema di pianificazione altamente configurabile degli NVR consente di impostare la registrazione continua o limitata a specifici intervalli temporali, per ciascuna videocamera in modo indipendente, di configurare compressione, risoluzione e frequenza dei fotogrammi di tutte le videocamere collegate, e di attivare la registrazione su evento.

Il dispositivo NVR può essere configurato in modo da sovrascrivere automaticamente i dati più vecchi al termine dello spazio su disco rigido, consentendo una registrazione continua e ininterrotta. Gli utenti possono specificare per quanti giorni conservare una registrazione (tenendo in considerazione la capacità del disco rigido e le normative vigenti).

L'installazione è stata realizzata da STT Servizi Telematici Telefonici S.r.l., società esperta nella progettazione, costruzione e gestione dell'infrastruttura ICT. Grazie a 25 anni di esperienza nell'integrazione dei sistemi dati e voce – e grazie anche alla partnership con i vendor più affermati del mercato come D-Link – STT è stata in grado di acquisire un portafoglio clienti in ambito Retail, Finance, Farmaceutico, Industria, Servizi, Grande Distribuzione, Logistica, Sanità e Pubblica Amministrazione. Con due sedi in Italia e un team di oltre 35 persone, STT può fornire un servizio di assistenza estremamente efficace su tutto il territorio nazionale.

in breve

Committente e location:
NTT DATA
(diverse sedi italiane. A progetto ultimato: Milano, Roma, Torino, Napoli, Treviso, Pisa, Cosenza)

Tipologia di installazione:
Videosorveglianza su IP per proteggere edifici e dipendenti, ospiti e manutentori attraverso il monitoraggio degli accessi anche fuori dall'orario di ufficio. A pieno regime, verranno installate 80 videocamere e 15 NVR per la registrazione.

System integrator:
STT Servizi Telefonici Telematici
www.stt-telefonia.it

Brand dei componenti:
D-Link Italia **www.dlink.com/it/it**

Sicurezza e domotica via IP

per un'importante industria avicola

STATO DI FATTO ED ESIGENZE DEL COMMITTENTE

L'industria Avicola F.lli Carbone si estende su una vasta area nel comune di Acerra e si compone di un complesso di capannoni nei quali sono presenti delle automazioni che vanno gestite e controllate, in ottemperanza anche alle nuove normative di settore che impongono ambienti idonei, rispondenti a requisiti ben precisi. Di vitale importanza per il benessere degli animali è il monitoraggio di alcuni parametri quali: temperatura, umidità degli ambienti, ed altri. Tali parametri vanno mantenuti sempre entro certi limiti e livelli: in caso di anomalie è richiesto un intervento immediato del personale dell'azienda affinché il tutto venga ripristinato entro i valori prestabiliti, con conseguenti fermi degli impianti fino ad intervento ultimato. Nell'ultimo periodo la struttura è stata inoltre oggetto di diversi furti ai danni di cose ed animali. La proprietà ha pertanto manifestato la necessità di una soluzione di sicurezza che evitasse i furti e che permettesse una gestione integrata e remota, nonché automatizzata, degli impianti tecnici presenti nei vari capannoni, al fine di ottimizzare tempi e modalità di intervento, nonché i conseguenti costi legati ai fermi della struttura.

LA TECNOLOGIA MESSA IN CAMPO

La ditta di installazioni Tecnoimpianti di Barbarino Antonio di Cervinara (AV), supportata dalla consulenza della Jaratech di Antonio Pascarella (Maddaloni), consulente e programmatore di sistemi integrati, ha prospettato ai proprietari dell'azienda avicola:

- una soluzione di gestione e controllo domotico degli impianti presenti nei singoli capannoni (fino a quel momento gestiti in maniera stand-alone) attraverso i Moduli IP Controller serie IPC di MARSS;
- una soluzione di videosorveglianza IP con telecamere Megapixel, che offrono un maggior livello di dettaglio e quindi permettono di identificare meglio gli oggetti e di videosorvegliare aree più ampie.

Il tutto dopo aver cablato la struttura e l'area in questione con una rete in fibra ottica plastica, che offre un'alta velocità di trasmissione dei dati e un'eccellente stabilità di trasmissione, perché resistente ai disturbi elettromagnetici (radio-frequenze, motori, ecc.), oltre ad una maggiore sicurezza.

I BENEFICI

Grazie ai Moduli IP Controller serie IPC l'azienda ha potuto ottenere:

- la centralizzazione di tutte le automazioni presenti nei singoli capannoni nel centro di controllo situato nel capannone principale;
- la centralizzazione di alcuni comandi destinati a scopi di sicurezza e gestiti dalla vigilanza notturna interna (es l'illuminazione);
- la remotizzazione di alcuni allarmi direttamente sui dispositivi mobili dei proprietari (smartphone, tablet, pc) in maniera tale da garantire loro il pieno controllo della struttura anche nei giorni festivi e nel corso delle attività fuori sede.

I Moduli IPC di Marss, basati sulla tecnologia TCP/IP di tipo stand-alone, sfruttano le potenzialità del Cloud e sono dotati di ingressi ed uscite che consentono di interfacciare qualsiasi impianto, sistema o dispositivo già esistente ed installato in una struttura. Attraverso l'App IP Controller, scaricabile gratuitamente da AppleStore e Googleplay, l'utente è abilitato al controllo e gestione remota e centralizzata, via smartphone e tablet, di tutti gli impianti interfacciati ai Moduli IP Controller, in modo semplice, sicuro ed efficace. Nello specifico dell'Avicola F.lli Carbone, questo ha portato all'ottimizzazione nella gestione risorse umane, che possono ora intervenire da remoto e tempestivamente in caso di allarmi tecnici e/o anomalie nella struttura.
L'App IP Controller oltre ad essere dotata di un'interfaccia grafica ad icone personalizzabili secondo l'esigenza dell'utente, supporta il servizio di Notifiche PUSH, che avverte in modo istantaneo in caso di cambiamento di stato degli impianti e dispositivi gestiti dai Moduli IP Controller, anche ad App chiusa.
La proprietà ha inoltre evidenziato un abbattimento dei costi di fermo impianto ed una piena gestione di tutta la struttura. Basta collegarsi all'App IP Controller per visionare in qualsiasi momento e ovunque lo stato degli impianti ed intervenire in caso di necessità.

in breve

Location dell'installazione
Avicola F.lli Carbone

Tipologia di installazione:
Domotica

Tratti salienti del sistema:
Controllo e gestione remota centralizzata degli allarmi tecnici e di sicurezza presenti nella struttura avicola, via Moduli IP Controller

Funzionalità principali:
il sistema abilita l'utente finale alle funzioni domotiche, via APP IP Controller, sfruttando gli impianti già esistenti

Installatore:
Tecnoimpianti di A. Barbarino - Cervinara (AV)

Distributore:
Jaratech di A. Pascarella - Maddaloni (CE)
www.jaratech.it

Brand:
Marss **www.marss.eu**

WEBSITE

secsolution
security online magazine

security magazine online

www.secsolution.com è il portale d'informazione b2b di riferimento per i professionisti della security in Italia.
In pochi 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 Facebook, 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 Venini, 37
20127 Milano
Fax +39 039 3305841
ethos@ethosmedia.it
www.ethosmedia.it

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

ANNO 4 – Numero 12 – GIUGNO 2014

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

PRINT PDF E-MAGAZINE WEBSITE

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

Il futuro è adesso!

a&s Italy interpreta sul mercato italiano la mission del network di riviste tecniche a firma **a&s**, leader a livello globale nell'editoria specializzata in security. In meno di tre anni, **a&s Italy** ha conquistato l'assoluta readership nell'editoria italiana di sicurezza, confermandosi il partner più autorevole per penetrare il mercato locale e per tirare la volata sui mercati esteri. **a&s Italy** è l'unica rivista che realizza indagini di mercato e inchieste di settore, che parla all'Italia aprendo una finestra sul mondo globale, che dialoga a tu per tu con utenti finali e decisori politici. **a&s Italy** rispetta i propri partner, certificando la tiratura e la distribuzione. Soprattutto **a&s Italy** viene letta, perché non è fatta di riempitivi tra un redazionale e l'altro, ma di contenuti tecnici innovativi che la consacrano come opinion leader.

Tiratura certificata secondo
il regolamento CSST:
codice CSST n. 2012-2328
del 27/02/2013

VOCI DAL MERCATO

Questa rubrica è lo spazio del chiarimento tecnico, dello smascheramento dei pregiudizi, della rivelazione del non detto e delle verità nascoste.

FOCUS PRODUCT

La voce tecnica dell'azienda. È lo spazio dove raccontare prodotti e sistemi che risolvono problematiche e meritano particolare approfondimento.

TECH CORNER

Lo spazio tecnico per eccellenza. La Redazione sviscera storia, evoluzione e tendenze di una specifica tecnologia interpellando i leader di mercato su argomenti di scenario.

APPLICATION CASE

Non c'è soluzione senza applicazione. Questo è lo spazio dove illustrare casi di di successo e applicativi di particolare valore aggiunto.

COMPONENT CASE

Dove l'accessorio è protagonista. Lo spazio tecnico per far uscire il componente dall'accezione di "accessorio" e restituirgli una dignità da protagonista.

INNOVATION CASE

Quando un'idea creativa genera progresso, allora si parla di innovazione. Il mercato racconta le applicazioni, le intuizioni, le idee che generano innovazione e aggiungono valore.

ETHOSMEDIAGROUP
GLOBAL MULTIMEDIA CHANNEL

Ethos Media Group s.r.l.
Via Venini, 37
20127 Milano
Fax +39 039 3305841
ethos@ethosmedia.it
www.ethosmedia.it