DICEMBRE 2014 - ANNO 4 N. 15

ETHOSMEDIAGROUP
GLOBAL MULTIMEDIA CHANNEL

IP Security MAGAZINE

TECNOLOGIE, SOLUZIONI E APPLICAZIONI PER L'IP SECURITY

La Sicurezza ai tempi dell'IoT

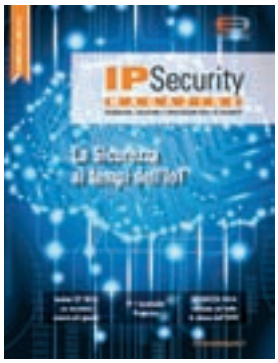
festival ICT 2014: un successo ancora più grande

IP = Inevitabile Progresso

SICUREZZA 2014: edizione col botto in attesa dell'EXPO'

www.ipsecuritymagazine.it

SOMMARIO



DICEMBRE 2014 - ANNO 4 - N. 15

ETHOSMEDIAGROUP
GLOBAL MULTIMEDIA CHANNEL

IP Security MAGAZINE

TECNOLOGIE, SOLUZIONI E APPLICAZIONI PER L'IP SECURITY

guarda ascolta scarica

La Sicurezza ai tempi dell'IoT

Il 2014 si chiude con una doppietta di eventi che hanno legato ancor più indissolubilmente i due mondi trattati dalla nostra testata: l'ICT e la security fisica. Due sono infatti stati gli appuntamenti che hanno visto protagoniste queste tecnologie: **festival ICT e SICUREZZA 2014**.
Interessante rilevare che entrambe le fiere hanno riscosso un forte successo di pubblico e che entrambe sono state sponsorizzate da vendor non solo provenienti dall'area di focalizzazione della fiera, ma da entrambi i settori. Ancor più interessante rilevare che il pubblico richiamato da tipologie di eventi tutto sommato diversi – non solo per merceologie trattate ma anche per target di riferimento – diventa sempre più vicino. Se infatti la videosorveglianza si integra nel controllo accessi ed assieme viaggiano su IP, l'interlocutore (che è anche buyer, per chi propone tecnologie) non può essere più soltanto il security manager, ma deve per forza essere anche l'IT manager. O un'unica figura che assommi competenze in entrambe le materie. Non è quindi un caso che la prossima edizione di SICUREZZA, prevista per il 2015, abbia deciso di ampliare la proposta espositiva alla cyber security. In un mondo sempre più connesso, l'ICT riveste infatti un ruolo chiave non solo per garantire la business continuity ma anche per contrastare attacchi sempre più frequenti e sofisticati. Del resto in un mondo dove le "cose" dialogano tra loro e tutto – infrastrutture, industria, singoli individui – è collegato a una rete, il tema sicurezza deve saper cambiare pelle e diventare elemento di protezione omnibus. E soprattutto di monitoraggio e miglioramento delle performance.

Tua la sicurezza,
nostro lo storage.
La forza della scelta.

Marc Cisneros

Custode,
Avvocato,
Guardiano.
362.512 ore registrate,
15.643 riprese valide,
7.453 sequenze archiviate,
2.423 imprese messe in sicurezza,
1.512 clienti protetti,
1 soluzione per la videosorveglianza.

Disponibile fino alla capacità di **6 Tb!**

WD Purple™
Lo storage per la videosorveglianza.

WD Blue™ WD Green™ WD Black™ WD Red™

Scopri di più sulle soluzioni di Marc su:
wd.com/choice

WD®
absolutely™

2178-800046-F00 Feb 2014

La Redazione

guarda il video

festival ICT 2014:
un successo ancora più grande

La seconda edizione del festival ICT, di scena lo scorso 6 Novembre al Mediolanum Forum di Assago, ha ottenuto un successo ancora più importante rispetto alla già entusiasmante prima edizione. Con 1081 visitatori certificati e un incremento ben del 35% rispetto all'edizione 2013, il festival ICT si riconferma il nuovo appuntamento del settore ICT in Italia.

La manifestazione, nata nel 2013, fin da subito si è fatta notare dal comparto per la sua energia, originalità e capacità di rivoluzionare il modo di fare eventi nell'ICT. "Il successo del festival ICT è dovuto al fatto che non è nato come una brutta o bella copia di altre manifestazioni. E' stato concepito totalmente da zero, grazie alla dettagliata conoscenza del settore, degli altri eventi verticali e delle reali esigenze del mercato" - ha dichiarato Federico Lagni, ideatore dell'evento.
Il festival ICT 2014 ha offerto al pubblico la possibilità di ascoltare 70 interventi, tra cui 6 apprezzati laboratori. I contenuti della manifestazione erano tutti orientati ad un pubblico business e professionale, con temi attuali, altamente rilevanti e fruibili in sale parallele e macrotematiche.

E' piaciuta molto anche l'Arena, un'area in cui si sono riuniti community, users group ed associazioni, tutti legati a uno o più temi ICT. Un vero "aggregatore di aggregatori", che si è rivelato essere un'area ad alto tasso di relazione, di condivisione di informazioni e quindi di innovazione.

SPONSOR DI PESO

La seconda edizione ha consacrato il festival nel suo status di "nuovo palcoscenico dell'ICT", visto l'alto numero di Sponsor e la loro rilevanza. Si parte dall'orgoglio italiano (rappresentato da WSS Italia, Wildix, V-Valley, VoipVoice, VoiceMyMail, TWT, Total Pri-

vacy System, Tesla Consulting, Synesthesia, Run Time Solutions, Reiss Romoli, Ready Informatica, Informatica Veneta, IFIConsulting, IdeaPM, Hosting Solutions, Gruppo PLS, Federprivacy, e-via, Enter, EDSlan, Digitel, Data Wipe Bank, Clouditalia, Alba S.T., AFGE – Alta Formazione Giuridico-Economica, Advantec ed Achab), fino al respiro mondiale con la presenza di tantissimi colossi ICT: Smart Technologies, Schneider Electric, Rittal, Juniper Networks, Check Point, Xorcom, WatchGuard, Teldat, Sophos, Ricoh, Polycom, Plantronics, Panduit, Novell, NetIQ, NEC, Microsoft, Kaspersky, Jabra, innovaphone, Huawei, Hikvision, MAXfocus, F-Secure, Exclusive Networks, Emerson Network Power, Cyberark, Brocade, Aruba Networks, Arrow ECS, Allnet, Alcatel-Lucent, Aerohive Networks ed A10 Networks.

Lo staff di festival ICT, oltre alle tante attività post-evento, è già al lavoro con l'edizione 2015: a breve saranno comunicata data e location - stay tuned!

www.festivalict.com

La Redazione

guarda il video

SICUREZZA 2014: edizione col botto in attesa dell'EXPO'

Corridoi pieni a tutte le ore per un'edizione 2014 di grande successo: +26% di visitatori rispetto all'edizione 2012; +33% di superficie espositiva; + 25% di espositori diretti, per un totale di 512 aziende su 29.000 metri quadrati e oltre 20.000 visitatori. In sensibile aumento anche i visitatori stranieri (+43%), provenienti da 78 diversi paesi. A questi si aggiungono i 107 top hosted buyer provenienti da 27 paesi, protagonisti di oltre 850 incontri one-to-one organizzati con gli espositori. E soprattutto, energia ed entusiasmo da vendere, che consegnano SICUREZZA ad un più importante ruolo sulla scena europea, da consolidarsi a partire dal 2015 con la nuova cadenza negli anni dispari. Il debutto ad ottobre 2015, con un'*edizione intermedia* in concomitanza con l'esposizione universale.

Ma per intanto godiamoci i fasti dell'edizione 2014, che ha visto Fiera Milano lavorare a stretto contatto con le aziende, le associazioni e gli editori di settore. Naturalmente Ethos Media Group e le sue testate (IP Security Magazine inclusa) erano in prima linea con tre eventi ad alto tasso di innovazione e uno stand "con una marcia in più". In senso letterale, visto che c'era una Ferrari.

IP SECURITY FORUM

Partiamo dall'evento *IP Security Forum*, di cui la testata *IP Security Magazine* è di fatto una "costola editoriale". *IP Security Forum* rappresenta ormai un appuntamento fisso con fiera SICUREZZA, dove la versione *international* del format - che si alterna alle varie puntate *light* itineranti sul territorio italiano – trova la cornice più adeguata per fornire formazione tecnica e analisi di mercato di altissimo livello, con una vision e un'impronta marcatamente internazionali. Gli articoli di Paul Hennings, Presidente di *IP User Group*, e Aaron Dale, Market Analyst Security & Fire Group di *IHS*, ci daranno un assaggio del livello scientifico della giornata.

ITALIAN SECURITY LEADERS, TOP 25

E anche quest'anno SICUREZZA è stato il palcoscenico per un'anteprima dell'annuale ed attesa indagine finanziaria realizzata da Ethos Media Group in collaborazione con KF Economics (Gruppo K Finance): *Italian Security Leaders, Top 25*. Rimandando a trattazioni più specifiche per gli approfondimenti contenutistici, questa è la sede per rimarcare lo spirito della nostra indagine, che intende inquadrare lo stato di salute e le tendenze che governano un comparto che, anche nel 2013, ha vantato performance di tutto rispetto. L'unicità dell'indagine, ripresa e pubblicata in più lingue e su più testate internazionali, la rende un fondamentale momento di riflessione sulla tenuta del comparto security in Italia e anche sulla tenuta di ciascuna azienda, fornendo uno strumento per "guardarsi dentro" con spirito critico e spinta al miglioramento.

CCTV REAL DEMO LIVE

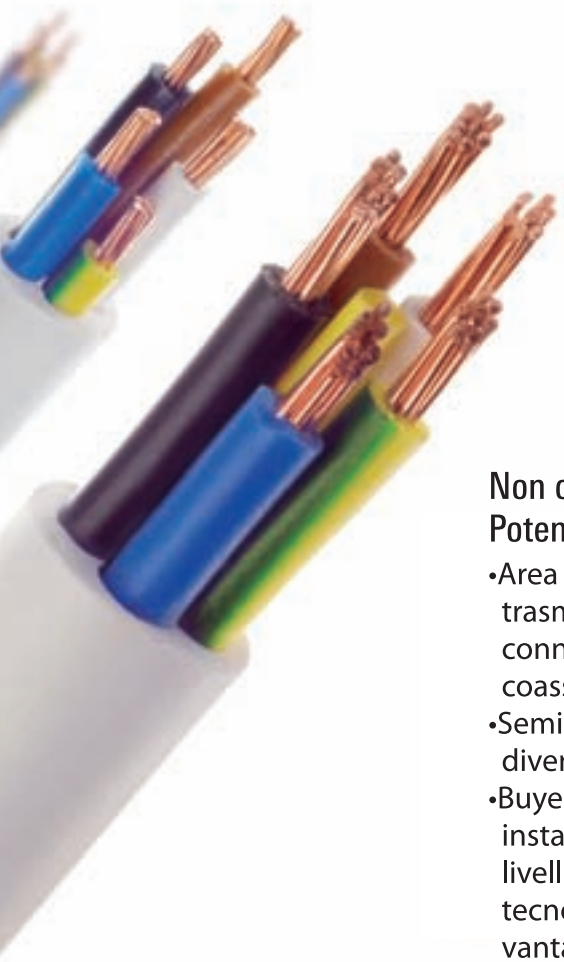
Una lunga denominazione per raccontare un'esperienza straordinaria che per la prima volta è stata offerta in una manifestazione fieristica italiana: l'allestimento di un'area che ospitava non-stop una vera video demo live dedicata alle IP Camera. Protagonisti di questa demo, oltre alle tecnologie e ai brand che hanno scelto di mettersi in gioco, sono stati tutti i visitatori e la giuria tecnica, che hanno espresso, con distinti criteri di peso, le loro valutazioni. L'area ha mostrato in modo uniforme le performance di ogni apparato presente: una grande opportunità per le aziende che il pubblico ha accolto con entusiasmo, con la raccolta di oltre 700 schede di valutazione. Il nostro grazie va quindi a tutti i partecipanti, veri "pionieri della security"! Parliamo di Assy, Bettini, Bosch Security Systems, Canon, Grundig, Hikvision Italy, JVC Professional Europe, Provision ISR - Mesa, SIQR.

secutech

Taipei Nangang Exhibition Center, Taiwan

28-30 aprile 2015

QUANDO UNA FIERA INVIA I SEGNALI GIUSTI



Non c'è niente di peggio di un contatto mancato
Potenzia la tua rete con Secutech

- Area dedicata a soluzioni e accessori per la trasmissione, per realizzare sistemi con una connessione chiara e affidabile mediante cavi coassiali, Ethernet e a fibre ottiche
- Seminari: vieni a scoprire i pro e i contro delle diverse tecnologie per la trasmissione
- Buyer's guide: contiene consigli pratici dedicati a installatori, rivenditori e distributori di qualsiasi livello, per comprendere i vantaggi di una tecnologia stabile ed economicamente vantaggiosa

Secutech @SecutechTaipei

Paul Hennings(*)

IP = Inevitabile Progresso

Tic tac, l'orologio ticchetta ormai impietosamente. La bella notizia è che non si tratta di un inarrestabile orologio biologico o di una sveglia molesta alle 5 del mattino. L'orologio di cui parliamo oggi scandisce il tempo delle opportunità e del business, e la sveglia che vedete nella foto sta suonando proprio per noi, che rappresentiamo il mercato della sicurezza. La parola chiave si chiama IP, che come tutti sanno sta per Internet Protocol. Ma in questo articolo illustreremo come IP significhi anche inevitable progress - progresso inevitabile. Assieme all'amico Paul Henning, Presidente di IP User Group, vi presentiamo un IP che ci richiama al progresso, all'evoluzione tecnologica, ad un cambio di mentalità e di approccio al business. Pronti? Via!

(*) Presidente di IP User Group **www.ipusergroup.com**

Partiamo dalla prima lettera che compone l'acronimo IP, la I. Tutti associano questa lettera, più che correttamente, alla tecnologia Internet. Ma per un attimo spostiamo l'attenzione alle lancette di quell'orologio che sta ticchettando per noi ed associamo la lettera I al termine Inevitabilità.
Flessibilità, scalabilità, modularità, sempre maggiori funzionalità dell'IP e piena integrazione, remotizzazione e ora anche prezzi in caduta libera rendono infatti la migrazione completa al video di rete non solo inevitabile, ma anche imminente. La diffusione sempre più ampia di una vera *cultura dell'IP* e delle sue enormi potenzialità ed opportunità di business per il mercato tradizionale della security stanno poi allargando a macchia d'olio gli operatori di canale ad essa dedicati, i quali a loro volta trasmettono sapere - quindi ingenerano nuovi bisogni - nella clientela. Clientela che è essa stessa sempre più preparata e attenta all'innovazione (ancora la lettera I!). La penetrazione tecnologica dell'IP è quindi anch'essa un fatto inevitabile. Come è inevitabile che il mercato, e soprattutto chi cerca nuove marginalità, si sposti verso l'IP, dal momento che chi sceglie la rete sceglie la strada dell'innovazione e quindi abbraccia un modello di business diverso, non più concentrato nel valore dei dispositivi tecnologici (in costante calo), bensì sul knowhow che egli possiede, quindi sulla sua capacità di fornire servizi originali che lo leghino al cliente in maniera fiduciaria e potenzialmente... a vita. Il video di rete sarà quindi, presto o tardi, un investimento obbligato e nel mercato vincerà chi saprà spostare il proprio core business, da vendita dei componenti e loro installazione verso analisi del rischio, consulenza, progettazione, integrazione.
La tendenza sempre più spinta verso un concetto olistico di security, che comprenda sia la parte fisica che quella logica, porterà poi ad un cambio dell'interlocutore – buyer che si farà sempre più radicale. A breve il fatto di doversi rapportare con dei manager di area IT diventerà la norma: sarà quindi essenziale imparare a conoscere il loro linguaggio e la loro logica, che spesso vede nelle telecamere degli intrusi (per giunta pericolosi) nelle "loro" infrastrutture di rete. Ma anche questo sarà inevitabile. E tuttavia farà parte di quel Progresso (non dimentichiamo la lettera P dell'acronimo IP) che porterà il comparto della security a nuovi obiettivi e risultati. Ecco dunque che IP significa *Inevitable Progress*, progresso inevitabile. Tic tac, tic tac.

TORNA IIPSEC

A grande richiesta, torna IIPSEC, International IP in Security Exhibition and Conference, evento dedicato alle tecnologie per la sicurezza fisica e la safety a base network. Negli anni IIPSEC ha accolto 15,000 visitatori, delegati ed espositori. Alla sua nona edizione, IIPSEC 2015 sarà presentato dalla rodata squadra di IP UserGroup security technology forum, IP-in-Action LIVE roadshow e IP focus magazine e eZine. Appuntamento dal 17 al 19 Novembre 2015 a Birmingham!

www.iipseconline.com

Emanuel Monticelli(*)

SDN e infrastrutture convergenti:
due tendenze in conflitto?

Se dovessimo individuare il fattore di cambiamento principale che al giorno d'oggi è di spinta per la trasformazione del business – e che a sua volta è il motore dell'innovazione tecnologica che si sviluppa - io sarei pronto a proporre il concetto di flessibilità. Le aziende hanno più che mai bisogno di essere flessibili, e tutta l'innovazione tecnologica segue proprio questa direzione: offrire alle imprese gli strumenti per poter rendere più flessibili i propri processi produttivi.

Oggi le imprese necessitano di tecnologie che possano fornire loro una buona flessibilità, ossia la capacità di adattarsi rapidamente ai cambiamenti, per essere in grado di convertire, aggiungere, eliminare e aggiustare rapidamente servizi o applicazioni per il mercato. Necessitano anche di individuare quali parti dell'infrastruttura tecnologica siano strategiche per potervi investire, e di disporre di strutture abbastanza dinamiche da modificare il mix "in house"-outsourcing/cloud a seconda delle esigenze dell'azienda. Se si parla di flessibilità in materia di infrastrutture IT e di rete, è chiaro che la tecnologia SDN risulta avere un ruolo chiave. Prendendo in esame i diversi approcci del mercato, e mettendo da parte quelli chiusi e privati, che a mio parere non alimentano

(*) System Engineer North Italy Extreme Networks **www.extremenetworks.com**

l'innovazione e si adattano male a questa ricerca di soluzioni flessibili, ci possiamo concentrare su quegli approcci basati su standard e open source. In questo ambito tuttavia ci sono anche alcune controversie riguardo alle reti SDN, soprattutto riguardo a dove si debba effettuare questa "separazione" di implementazioni nella rete per poter usufruire delle proprietà SDN, o quali sviluppi dell'architettura siano quelli che effettivamente favoriscono apertura e programmabilità.

SDN VS INFRASTRUTTURE CONVERGENTI

Uno dei grandi temi di discussione riguardo alla tecnologia SDN è se l'"astrazione" dell'intelligenza di rete sia efficace in tutte le situazioni e fino a che livello possa spingersi. A quei produttori che scommettono per l'astrazione totale sarebbe da chiedere per quale motivo talvolta si registra un crescente interesse per le infrastrutture convergenti, che rispondono ad una filosofia apparentemente contraria a quella della tecnologia SDN, nel senso che si cerca in questo caso di aggiungere componenti - parliamo di ambiente di rete del data center – al posto di scomporre o astrarre l'intelligenza dell'infrastruttura. Esaminiamo più in dettaglio le due soluzioni:

a) **Infrastruttura Convergente.** Questo approccio parte dal presupposto che si possa eliminare una certa complessità del data center, se si è in grado di astrarre la configurazione dell'intero ambiente mediante la precedente integrazione di tutti gli elementi che lo compongono: rete, server e storage, in modo che al cliente venga offerta una specie di data center "in-a-box". Indubbiamente questo approccio consente di esternalizzare la complessità verso il fornitore, e di ridurre il tempo necessario ad implementare o ad ampliare il data center. L'inconveniente è che ci si trova però di fronte ad una soluzione chiusa. Io credo invece che si possano sfruttare i benefici di un'infrastruttura convergente senza che essa debba per forza essere una soluzione chiusa.

b) **Software Defined Networking (SDN)**. Dall'altra parte abbiamo l'SDN, che di base separa l'hardware di rete dall'intelligenza di rete, creando strati intermedi che favoriscono flessibilità, controllo e automazione. Molti produttori, incluse molte nuove aziende che offrono software SDN, adottano questa separazione dei livelli nella parte inferiore dell'architettura, e ciò è noto come "southbound API". Tuttavia, a mio parere, le capacità di programmazione di rete che apporta la tecnologia SDN, vanno ben oltre questo livello, salendo in alto, verso i piani di applicazione. Ad esempio, possiamo programmare il modo in cui le applicazioni comunicano con la rete – chiedendo più risorse, fornendo informazioni di come l'utente utilizza un'applicazione, oppure quando questa applicazione utilizza nuove porte TCP. Tutto questo è ciò che in termini SDN si definisce "northbound API".

Ma esiste realmente un conflitto tra queste due soluzioni? A prima vista, possono sembrare due impostazioni contrastanti: integrare e assemblare componenti da un lato, disgregare e mantenere più elementi intercambiabili nell'infrastruttura dall'altro. In ogni caso entrambi gli approcci tentano di eliminare la complessità o almeno di ottenere maggiore flessibilità all'interno dell'infrastruttura. Coloro che hanno molta fretta di ristrutturare il proprio data center possono optare per la soluzione convergente "in-a-box", mentre coloro che sono interessati a reti aperte e dinamiche, più orientati verso l'innovazione a lungo termine, possono usufruire della tecnologia SDN.
La verità è che non si tratta di una scelta tra tutto o niente, non sono soluzioni che si escludono reciprocamente, sempre che si opti per tecnologie aperte. Dopotutto a cosa serve la tecnologia SDN se le componenti non funzionano bene insieme? Molti sono alla ricerca di soluzioni SDN testate e con un alto tasso di integrazione all'interno di un ecosistema più elevato. Grazie al crescente numero di iniziative open source come OpenDaylight, Open Networking Lab o ON.Lab si ha un impulso crescente di soluzioni aperte, e grazie alle architetture di riferimento come VSPEX e a driver come OpenDaylight, i vantaggi di ciascun approccio possono essere personalizzati a seconda della rete.

intersec

January 18 – 20, 2015
Dubai, UAE

Visit the world's leading trade fair for Security, Safety & Fire Protection

It's your opportunity to meet over 1,300 local and international exhibitors who will showcase the best security solutions.

Product Sections:

- Commercial Security
- Information Security
- Fire & Rescue
- Safety & Health
- Homeland Security and Policing

2015 Highlights:

- Confirmed participation of the world's top 10 security companies
- New GPEC Pavilion for police & special equipment
- ESSA Pavilion for safes, strongrooms & deposit systems
- Dubai SME Pavilion for small & medium enterprises
- Techtextil Pavilion for technical textiles & nonwovens
- 13 Country Pavilions
- Enlightening conference programmes

Register online today
www.intersecexpo.com

messe frankfurt

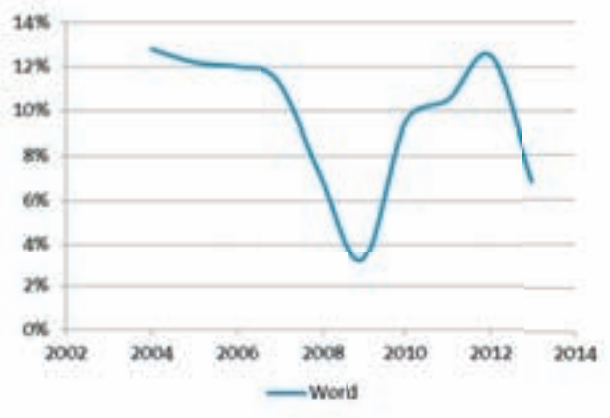
Aaron Dale(*)

guarda il video

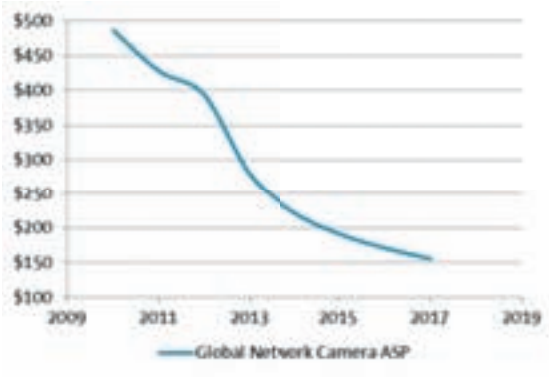
2013 e 2014: anni dirompenti per la videosorveglianza

Negli ultimi dieci anni il mercato della videosorveglianza è cresciuto notevolmente ed altrettanto notevolmente si è evoluto, non solo tecnologicamente ma anche a livello strutturale-dimensionale. Basti pensare che nel 2013 le telecamere di sicurezza vendute hanno superato di oltre 8 volte quelle vendute nel già lontano 2003. I cambiamenti che hanno interessato il settore hanno seguito alcune direttrici di fondo, con la congiuntura economica negativa in testa. Purtroppo ...ma talvolta anche per fortuna. Con l'aiuto di Aaron Dale, analista di IHS, abbiamo ripercorso questi ultimi dieci anni per individuarne i trend, capire la lezione e formulare anche qualche previsione per il futuro.

(*) Aaron Dale è un analista di IHS specializzato nel segmento videosorveglianza **https://technology.ihs.com/.**



CRESCITA GLOBALE DEL TVCC (2002-2014)
La crisi economica mondiale ha frenato la crescita, ma il 2013 ha registrato un anomalo picco di vendite. Fonte: IHS, per gentile concessione. Tutti i diritti riservati.



PREZZI MEDI PER TELECAMERE DI RETE (GLOBALE)
Nel 2012 e 2013 i prezzi hanno subito un brusco calo. Il processo di erosione dei prezzi è però destinato a stabilizzarsi. Fonte: IHS, per gentile concessione. Tutti i diritti riservati.

È semplice: quando l'economia gira bene, in genere le aziende hanno più liquidità e quindi più interesse ad investire in beni infungibili come le tecnologie per la security. Gli effetti della crisi finanziaria del 2007 si ricavano dalla curva che rappresenta lo storico del mercato della videosorveglianza, la cui crescita sul target privato si è ridotta del 65%. Nel settore pubblico, crescita o decrescita del TVCC dipendono anch'essi dagli investimenti centrali o locali, ma questi ultimi sono strettamente legati agli investimenti già in corso o già preventivati in infrastrutture di più ampio respiro e, aspetto assolutamente non irrilevante, sono strettamente connessi alla percezione di sicurezza che si respira nel tessuto sociale. Sebbene I cordoni di ormai tutte le borse governative si siano stretti, in tempi di spending review e patti di stabilità, la criminalità (o meglio la percezione della stessa) sono invece cresciuti. Risultato: il mercato della vidosorveglianza si è mostrato più resiliente agli scossoni economici rispetto alla generalità dei mercati. Negli ultimi dieci anni, due anni si sono però mostrati articolarmente significativi: il 2013 e il 2014. Vediamo perchè.

2013: UN ANNO ECCEZIONALE

Il forte calo dei prezzi dei componenti del 2013 ha avuto un immediato e benefico impatto sul mercato della videosorveglianza (analogico e IP), tanto che a livello mondiale si è registrata una crescita del 7% (inferiore comunque alle attese). Ma il fatto interessante è che la transizione da TVCC analogica a network video ha subìto una forte accelerazione, portando nel video IP dei fatturati più alti in tutte e quattro le macro aree analizzate da IHS (EMEA, Americhe, Cina, Asia). Il calo dei prezzi si è però rivelato un'arma a doppio taglio: se da un lato la richiesta di telecamere nel 2013 ha subito una vera e propria impennata, come rovescio della medaglia però I ricavi sono stati inferiori alle aspettative. La transizione verso l'IP, proseguita nel 2014, continuerà a ritmi sostenuti anche per tutto il 2015, salvo poi affievolirsi gradualmente dal 2016 in avanti. I vendor si concentreranno sempre più verso il video di rete, a discapito dell'obsoleta tecnologia analogica.

HD ANALOGICA E QUALITÀ

Il 2013 è stato anche l'anno del lancio della tecnologia HD CVI, che si è mostrata un agguerrito competitor della precedente tecnologia HD SDI soprattutto sul fattore prezzo, portando la cosiddetta *alta definizione analogica* (che rientra nella più vasta denominazione lessicale di HD CCTV) ad un livello più alto della nicchia cui sembrava inizialmente destinata. Se l'HD SDI si era infatti scontrata con un forte problema di costi, in particolare per la sostituzione di cavi coassiali quasi sempre inadeguati a portare un segnale ad alta definzione, la *seconda generazione* di tecnologie HD CCTV sembra invece aver posto rimedio ai problemi più rilevanti (dal prezzo alle distanze di 300-100 m per la trasmissione). Non è un caso che, dopo il lancio della tecnologia HD CVI nel 2013, l'anno successivo sia seguito il lancio di altre due tecnologie analoghe (AHD e TVI) e al contempo l'HDcctv Alliance abbia perfezionato il suo standard 2.0.
Un altro aspetto tecnologico che ha dominato gli anni 2013 e 2014 è stata la ricerca spasmodica di una qualità dell'immagine video sempre più performante ed affidabile in qualunque condizione di luce e movimento. Un dato per tutti: nel 2014 oltre il 90% delle network cameras di nuova produzione disponevano di risoluzione megapixel.

IL CASO ITALIA

La singolarità degli anni 2013 e 2014 ha prodotto effetti diversi sui diversi sistemi paese.
Nei paesi, come l'Italia, dove le restrizioni dei budget si sono fatte sentire nel modo peggiore, il crollo dei prezzi del video IP potrebbe portare nuova linfa vitale e rifocalizzare il mercato sulla qualità, anche se il duro colpo della crisi ridurrà notevolmente la crescita del mercato della videosorveglianza rispetto agli altri paesi della stessa area EMEA. Ciononostante, stando alle analisi di IHS, è tuttora prevista una crescita - non eccelsa ma costante – ad un tasso medio del 3.2% fino al 2018. Se il mercato italiano dei dispositivi di videosorveglianza (analogici e digitali) nel 2013 valeva, sempre secondo IHS, 130 milioni di dollari USA, è lecito quindi attestare le stime di chiusura del 2014 sui 135 milioni di dollari.
Va comunque ricordato che il 2013 è stato un anno irripetibile – un tale crollo dei prezzi non può che essere irripetibile - quindi occorre prevedere una stabilizzazione dei prezzi nei prossimi anni. Tuttavia, la rivoluzione legata all'anno 2013, pur portando sul piatto nuove ed interessanti opportunità per I vendor, al contempo metterà a dura prova la capacità di adattamento dei produttori di TVCC. E quello che abbiamo visto finora è solo l'inizio: le implicazioni del processo innescato nel 2013 si manifesteranno infatti con sempre maggior evidenza nel 2015 e negli anni a seguire. Estote parati.

La Redazione

Retail:
meno cybercrime ma più dannoso

Secondo risultati recentemente pubblicati da IBM, nonostante la riduzione del 50% degli attacchi informatici perpetrati nei confronti dei retailer statunitensi, il numero di dati rubati continua a mantenersi a livelli di record. I ricercatori di IBM Security riferiscono che, nel 2014, gli hacker sono riusciti comunque a rubare alle aziende del retail più di 61 milioni di dati clienti, nonostante la diminuzione degli attacchi, a dimostrazione del crescente grado di sofisticatezza e di efficienza del crimine informatico.

Gli studi IBM 2014 Retail Research and Intelligence Report e Holiday Trends: Black Friday/Cyber Monday Research and Intelligence Report parlano di hacker sempre più sofisticati che ottengono enormi quantità di dati riservati con modalità sempre più efficienti. Dal 2012 il numero di violazioni segnalate dai retailer è sceso del 50%, tuttavia gli autori dei cyber-attacchi sono riusciti a colpire, con ogni singolo attacco, un numero molto maggiore di vittime.

BLACK FRIDAY E CYBER MONDAY

Anziché intensificarla, i cyber-criminali hanno infatti ridotto la loro attività in tutti i settori durante il Black Friday e il Cyber Monday, i due principali giorni di shopping dell'anno secondo il Digital Analytics Benchmark di IBM. Nonostante questa diminuzione, i settori delle vendite al dettaglio e delle vendite all'ingrosso sono stati i principali bersagli degli hacker nel 2014, conseguenza dell'ondata di incidenti di alto profilo che hanno colpito i grossi rivenditori di marca. Nei due anni precedenti, il settore manifatturiero è risultato il primo dei cinque settori presi di mira, mentre quelli delle vendite al dettaglio e all'ingrosso si trovavano in ultima posizione. In quest'ultimo anno, la modalità di attacco principale è stata l'accesso non autorizzato tramite attacchi di tipo "Secure Shell Brute Force", che hanno superato i codici malevoli (scelta di punta nel 2012 e nel 2013).

LE VIOLAZIONI PRINCIPALI METTONO IN OMBRA UNA TENDENZA IN CRESCITA

Gli hacker sono riusciti a impossessarsi di più di 61 milioni di dati nel 2014, in calo rispetto ai quasi 73 milioni nel 2013. Tuttavia, se si restringono i dati ai soli incidenti che coinvolgono meno di 10 milioni di record (ossia escludendo i due attacchi principali nel corso di questo periodo, Target Corporation e The Home Depot), il numero di record del retail compromessi nel 2014 è aumentato di più del 43%, rispetto al 2013.

METODI DI ATTACCO SOFISTICATI

Anche se vi è stato un aumento del numero di attacchi di malware ai Point of Sale (POS), la grande maggioranza di incidenti diretti al settore delle vendite al dettaglio è stata causata da Command Injection o SQL injection. La complessità delle istruzioni SQL e la mancata validazione dei dati da parte degli amministratori della sicurezza hanno reso i database del settore retail un bersaglio primario. Nel corso del 2014, il metodo di Command Injection è stato usato in quasi 6.000 attacchi nei confronti di retailers. Tra gli altri metodi figurano Shellshock, oltre a malware per POS come BlackPOS, Dexter, vSkimmer, Alina e Citadel.

More at **www.ibm.com/security**

SMA home

Smart Home Int'l Conference & Exhibition 2015

YOUR

Wonderland

TO SOURCE

Technology Service Providers

OF

HOME SECURITY & SMART HOME

The expo connects global smart home & security pros to:

- Taiwan's IT and networking leading makers, eg. D-Link, Sercomm, Inventec, Chicony, Quanta, Gemtek, Accton, Pegatron, etc.
- Asia's top 100 manufacturers of home cameras, smart locks, doorbells, sensors, gateways, etc.
- Full product selections from DIY home gadgets to project-based solutions

April 28-30, 2015 | Taipei, Taiwan

Register Now! www.secutech.com/smahome

Concurrent with

secutech

Organizer
Messe Frankfurt New Era Business Media Ltd.
+886-2-26599080 SMA-pr@newera.messefrankfurt.com

La Redazione

Orientare domanda e offerta:
indagine conoscitiva per gli installatori

Assotel, Associazione che rappresenta le imprese che realizzano Impianti di Telecomunicazioni (fonia/dati) e Impianti Speciali di Sicurezza (con Inter-Networking Protocol), ha elaborato alcune semplici domande al fine di determinare le dinamiche di mercato che oggi spingono gli IT Manager a selezionare il fornitore/partner al quale affidare le infrastrutture e i sistemi ricetrasmissivi e di sicurezza dell'azienda. Obiettivo: raccogliere ed elaborare le informazioni necessarie per orientare al meglio domanda e offerta. Le riportiamo di seguito, specificando che le stesse sono scaricabili sul portale www.secsolution.com e che i moduli compilati andranno restituiti a info@assotel.it

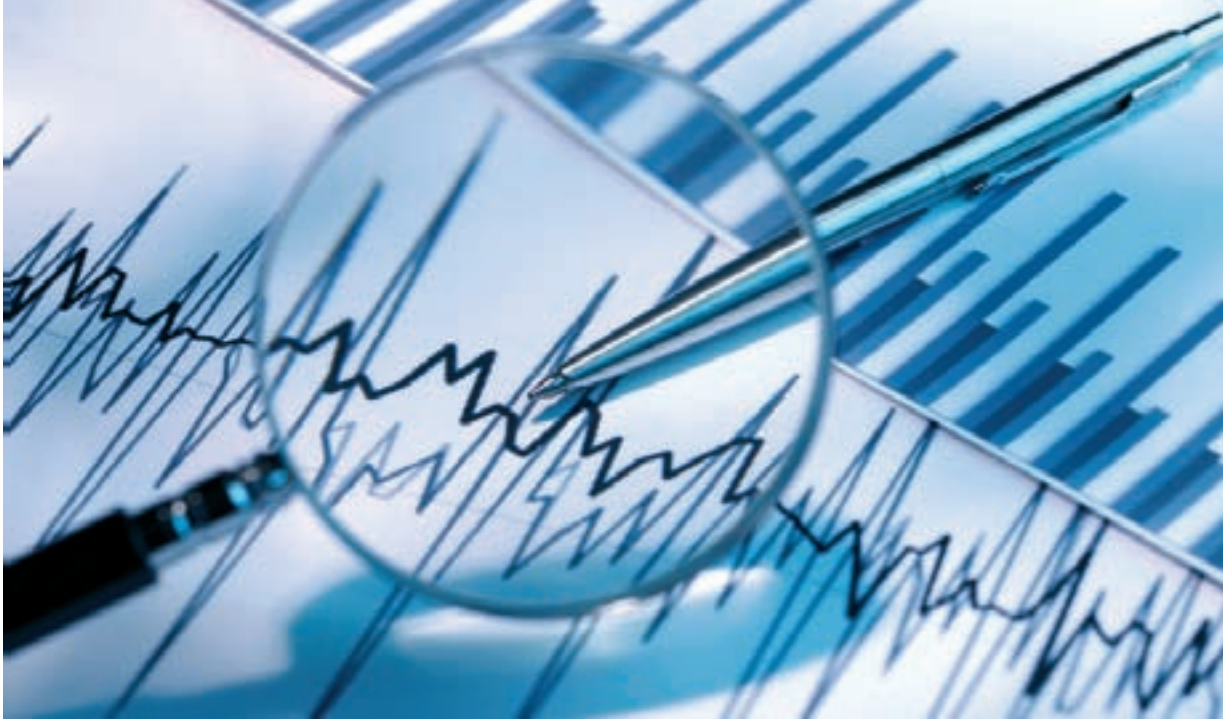
In fase di trattativa per ottenere l'assegnazione di una commessa quale partner tecnico per il progetto e la realizzazione di un'infrastruttura di rete o di un sistema TLC/ICT/IP Security...

...Qual è, a vostro avviso, il principale motivo che spinge un committente a richiedervi un'offerta esecutiva e/o progettuale?

	Esecutiva	Progettuale
Consuetudine		
Reputazione		
Passa parola		
Dimensione aziendale		
Referenze		
Disponibilità		
Altro		

...Qual è, a vostro avviso, il principale motivo che spinge un committente a richiedervi un'offerta esecutiva e/o progettuale?

- ☐ Professionalità
- ☐ Competenza
- ☐ Aggiornamento tecnico
- ☐ Capacità di interpretare le esigenze presenti e future
- ☐ Rispondenza agli standard
- ☐ Rispetto delle normative e della legislazione
- ☐ Ottimizzazione dei costi
- ☐ Rigore etico
- ☐ Altro .....



Ordinate, numerandoli, i documenti che i committenti maggiormente richiedono in fase di contratto:

- ☐ La conformità al Progetto
- ☐ Una relazione tecnico/esecutiva di fine lavori
- ☐ Lo schema di numerazione delle connessioni
- ☐ Una certificazione strumentale che certifichi quanto realizzato
- ☐ Uno schema a blocchi di posizionamento apparati
- ☐ Uno schema delle interconnessioni alla Rete pubblica
- ☐ Il coordinamento esecutivo con Certificazioni preesistenti
- ☐ Manuali d'uso e manutenzione
- ☐ Formazione di personale interno
- ☐ Altro .....

Quando un'infrastruttura di rete o un sistema TLC/ICT/IP Security è direttamente o indirettamente interconnesso a rete pubblica...

- ☐ nessuno
- ☐ il progetto
- ☐ una dichiarazione di conformità alla regola dell'arte
- ☐ una relazione tecnico/esecutiva di fine lavori
- ☐ lo schema di numerazione delle connessioni
- ☐ una certificazione strumentale che certifichi quanto realizzato
- ☐ uno schema a blocchi di posizionamento apparati
- ☐ uno schema delle interconnessioni alla Rete pubblica
- ☐ una certificazione di continuità operativa con quanti preesistente
- ☐ manuali d'uso e manutenzione
- ☐ Proposta di formazione di personale interno
- ☐ Proposta di un contratto di manutenzione
- ☐ Altro .....

Grazie a tutti voi!

037 SMITT SRL · 2 N TELEKOMUNIKACE A.S. · A.I. TECH SRL · A.I.P.S. - ASSOCIAZIONE INSTALLATORI PROFESSIONALI DI SICUREZZA · A.I.PRO.S. - ASSOCIAZIONE ITALIANA PROFESSIONISTI · A.M.C. ELETTRONICA SRL · AASSET SECURITY ITALIA SPA · AB TECNO SRL - BRAND "APERIO" · ABESE · ACAL BFI ITALY SRL · ACCU ITALIA SPA · ACOTEL NET · ACUT SERVIZI SRL · AD CONSULTING SRL · ADVANCED INNOVATIONS SRL · ADVANTAGE AUSTRIA - CONSOLATO GENERALE D'AUSTRIA - SEZIONE COMMERCIALE · ADVANTEC SRL · AELETTRONICA GROUP SRL · AETHERNA SRL · AIIC - ASSOCIAZIONE ITALIANA ESPERTI IN INFRASTRUTTURE CRITICHE · AIPSA - ASSOCIAZIONE ITALIANA PROFESSIONISTI SECURITY AZIENDALE · ALLNET.ITALIA SPA · ALLUSER INDUSTRIE SRL · ANCI SERVIZI SRL SEZIONE CIMAC · ANIE SICUREZZA · ANJUBAO DIGITAL · AOYODI ELECTRONIC CO. LTD. · ARECONT VISION · AREU LOMBARDIA - AZIENDA REGIONALE EMERGENZA URGENZA · ARMA DEI CARABINIERI · ASS.I.V. - ASSOCIAZIONE ITALIANA VIGILANZA E SERVIZI FIDUCIARI · ASSICUREZZA CONFESERCENTI · ASSISTAL - ASSOCIAZIONE NAZIONALE COSTRUTTORI DI IMPIANTI · ASSOCIAZIONE FEDERPRIVACY · ASSOSICUREZZA · ASSOTEL · ASSY · AVIGILON · AVOTEC SRL · AVS ELECTRONICS SPA · AXEL SRL · AXIS COMMUNICATIONS SRL · BANDIT ITALIA SRL · BEMA EDITRICE SRL · BENTEL SECURITY SRL · BETA CAVI SRL · BETAFENCE ITALIA SPA · BETTINI SRL · BIOSEC ITALIA · BORDOGNA SPA · BORINATO SECURITY SRL · BOSCH SECURITY SYSTEMS SPA · BY DEMES SL · C.E.CAM. SRL · C.E.I.A. SPA · C.R. SERRATURE SPA · CAMANO SRL · CAME SPA · CANON ITALIA SPA · CANTONK CORPORATION LIMITED · CARAMELLA MULTIMEDIA SRL · CAVEL - ITALIANA CONDUTTORI · CEI - COMITATO ELETTROTECNICO ITALIANO · CHT SRL · CHUANGO EUROPE B.V. · CITEL SPA · CO.GEN. SPA · CO.I.S. - CONSORZIO ITALIANO SICUREZZA · CODARINI TUEGA · COMETA SPA · COMNET · COMPASS DISTRIBUTION · CONNESSIONI SRL · CONRAD ELECTRONIC · CONSORZIO GOSS ITALIA · CONSORZIO NAZIONALE SICUREZZA S.C.A.R.L. · CONTROLTEC SRL · CRISMA SECURITY SRL · D-LINK MEDITERRANEO SRL · DAEWON DIGITECH SRL · DAHUA VISION TECHNOLOGY CO LTD · DAITEM ATRAL ITALIA · DATA MOBILE THOMAS VOGLER · DBINFORMATION SPA · DEFENCE SYSTEM SRL · DEFENDERTECH BY TEK GROUP SRL · DELTA DORE SRL · DELTA-OPTI MONIKA MATYSIAK · DETECH SRL · DIAS SRL · DIGIMAX SRL · DISEC SRL · DOINGSECURITY SAS DI SABATO GIANNI E C. · DOMOTEC SRL · DOPPLER SRL · DUEVI SNC · EASYDOM · EBOO SOLUTIONS · ECOSAFE - TEKNIKPLAS PLASTIK LTD · EDITRICE MAESTRI SRL · EDSLAN SPA · EEA SRL · EGA MASTER S.A. · EGYTEC ENGINEERING CO. · EKEY BIOMETRIC SYSTEMS SRL · EL.MO. SPA · ELAN SRL · ELECTRONIC'S TIME SRL · ELIMOS SRL · ELP SNC · EMERCOM OF RUSSIA · ENVIO SECURITY SYSTEMS SRL · EPC PERIODICI SRL · ERMES ELETTRONICA SRL · ERSI · ESI GROUP · ESIWELMA SRL · ESSE-TI SRL · ESSECOME - WWW.SECURINDEX.COM · ESSEGIBI · ESURV · ETER BIOMETRIC TECHNOLOGIES SRL · ETHOS MEDIA GROUP SRL (A&S ITALY) · EUROCOM TELECOMUNICAZIONI SRL · EUROGROUP SRL · EUROPLANET SRL · EUROTEK SRL · EVAC+CHAIR INTERNATIONAL LTD · EVOFORCE SRL · EVVA ITALIA SRL · FIAMM SPA · FIERA MILANO BRASIL · FLIR COMMERCIAL SYSTEMS · FOGLIA ENGINEERING · FOLKSAFE INTERNATIONAL CO. LIMITED · FONDAZIONE ENZO HRUBY · FONTANA SICUREZZA SRL · FOSCAM ITALIA LOOKATHOME SNC · G. OSTI SISTEMI SRL · GESCO SRL · GEWISS SPA · GLIAD SRL · GLOBE MASTER KFT. · GO SYSTEMS SRL · GPS STANDARD SPA · GT LINE SRL · GUANGZHOU ZHONGPAI SECURITY TECNOLOGY CO. LTD · GUARDIA DI FINANZA · HELLATRON SPA · HESA SPA · HIKVISION ITALY SRL · HIS SRL · IBIT SRL · IL CANTINIERE D'ITALIA SAS · IL RICARICABILE SNC · IMQ SPA · IMX SRL · INFOPROGET SRL · INFORDATA SISTEMI SRL · INIM ELECTRONICS SRL · INNOVA EDITORE SRL · INTELLIA SRL · INTERTECHNO FUNK-TECHNIK GMBH · INTERTEL SRL · IPDOOR ROBOVISION ENGINEERING SRL · ISEO SERRATURE SPA · ITALFILE SRL · ITALIANA SENSORI SAS · IVECO SPA · IVRI · JABLOTRON ALARMS A.S. · JVC PROFESSIONAL EUROPE LTD · KBLUE SRL · KEYLINE · KLEMI CONTACT SRL · KRONOTECH SRL · KSENIA SECURITY SRL · LA SONORA SRL · LASERLINE SAFETY AND SECURITY SYSTEMS SRL · LBM ITALIA SPA · LION'S TECH SRL · LOUIS SECURE INDUSTRIAL LTD · LUCEAT SRL · MAGGIOLI EDITORE · MARCH NETWORKS SPA · MARCO POLO SNC · MARCUCCI SPA · MARSS IP & SECURITY SRL · MAS MEKANIK LTD · MATOOMA · MATROX ELECTRONIC SYSTEMS GMBH · MERIT LILIN ITALIA SRL · MESA SRL · META SYSTEM SPA · METAREC SRL · MICRO TEK SRL · MICROCONTROL ELECTRONIC SRL · MICROLOGIC SRL · MICRONTEL SPA · MICROTEL SRL · MICROVIDEO SRL · MILESTONE ITALIA SRL · MITECH SRL · MMEDIA SRL · MTT · NAI SRL · NEDAP N.V. · NETGEAR INTERNATIONAL INC. · NETICOM SRL · NEW BUSINESS MEDIA · NEW VOICE INTERNATIONAL SA · NEXTTEC SRL · NII PROGETTI · NOTIFIER ITALIA SRL · OMNIA PLASTICA · OPERA SRL · OPTEA SRL · OVERSEC SRL · PANASONIC ITALIA BRANCH OFFICE DI PANASONIC MARKETING EUROPE · PASO SPA · PELCO BY SCHNEIDER ELECTRIC · PEPLINK ITALIA · PESS TECHNOLOGIES SRL · PFANNENBERG ITALIA SRL · PHILIPPEIT GMBH · PHOEBUS SPA UNIPERSONALE · PIERRE SRL · PILOMAT SRL · POLITEC SRL · POLIZIA DI STATO · POLIZIA LOCALE MILANO · POWERFLEX SRL · POWERVIEW ITALIA SRL · PREVOR · PROD.EL.CO SRL · PROTECT ITALIA SRL · PWM SEMICONDUCTORS SRL · PYRONIX LTD · QUBIX SPA · R. PIERRE DIGITAL SPA · RAFI SRL · RISCO GROUP SRL · ROFINOR TEXTEIS, LDA · S NEWS SRL · S.I.C.E. SRL · S.P.E. STUDIO PROG. ELETTRONICHE · S&A SRL · SAIMA SICUREZZA SPA · SALTO SYSTEMS SRL · SAMSUNG TECHWIN EUROPE LTD · SATEL ITALIA SRL · SAVV SRL · SDC MANAGEMENT SRL · SECON 2015 · SECUREMME · SECURITALY SRL · SECURITY ITALIA SRL · SECURMATICA SECURITY MANAGEMENT SRL · SELESTA INGEGNERIA SPA · SERTEC SRL · SHENYANG WM TECH CO. LTD · SHENZHEN ANVOX ALARM SYSTEMS CO. LTD · SHENZHEN BXS ELECTRONICS CO. LTD · SHENZHEN CPSE EXHIBITION CO. LTD · SHENZHEN STARTVISION TECHNOLOGY CO LTD · SHENZHEN WINSTAR TECHNOLOGY CO. LTD · SHENZHEN XENON INDUSTRIAL LTD · SHENZHEN XIAOERDUO POWER ADAPTER CO LTD · SICE TECH SRL · SICEP SPA · SICUR 2016 - IFEMA FERIA DE MADRID · SICUREZZA ROTONI SRL · SICURIT ALARMITALIA SPA · SICURTEC LAMINATGLASTECHNIK GMBH · SICURTIME SRL · SIGITAL SRL · SILENTRON SPA · SIMONSVOSS TECHNOLOGIES GMBH · SINTESI SRL · SIRENA SPA · SMITHS DETECTION ITALIA SRL · SOFTGUARD TECHNOLOGIES CORPORATION · SOIEL INTERNATIONAL · SOLCAVI SNC DI MUSELLA SANTOLO · SONY EUROPE LTD · SPARK · SYAC-TB - TECHBOARD SECURITY DIVISION · T+B ELECTRONIC GMBH · TECHNOMAX SRL · TECNA EDITRICE SRL · TECNOALARM SRL · TEKNOMEDIA EDIZIONI SRL · TELECOM & SECURITY · TELLSYSTEM COMMUNICATION LTD · TERVIS SRL · THERMOSTICK ELETTROTECNICA SRL · TINY GREEN PC · TIRASSA GIUSEPPE SRL - MORSE WATCHMANS INC · TRANS AUDIO VIDEO SRL · TRE I SYSTEMS SRL · TSEC SPA · TUTONDO BY A.T.E.C. SRL · TYCO SECURITY PRODUCTS · UMBRA CONTROL SRL UNIPERSONALE · UNITEK ITALIA SRL · UR FOG SRL · URMET ATE SRL · URMET SPA · UTC FIRE & SECURITY ITALIA SRL · VALFORD SRL · VENITEM SRL · VIDEOFIED · VIDEOTECNOLOGIE SRL · VIDEOTREND SRL · VIDEX ELECTRONICS SPA · VIGILI DEL FUOCO COMANDO PROVINCIALE · VIMO ELETTRONICA SNC DI CAVALLERI R&C · VISE SRL · VISIOTECH · VIVOTEK INC. · VOLTA SPA · VOYAGER SRL · WEY TECHNOLOGY SRL · ZHEJIANG DALI TECHNOLOGY CO. LTD · ZUCCHETTI AXESS SPA

Ci rivediamo nel 2015.

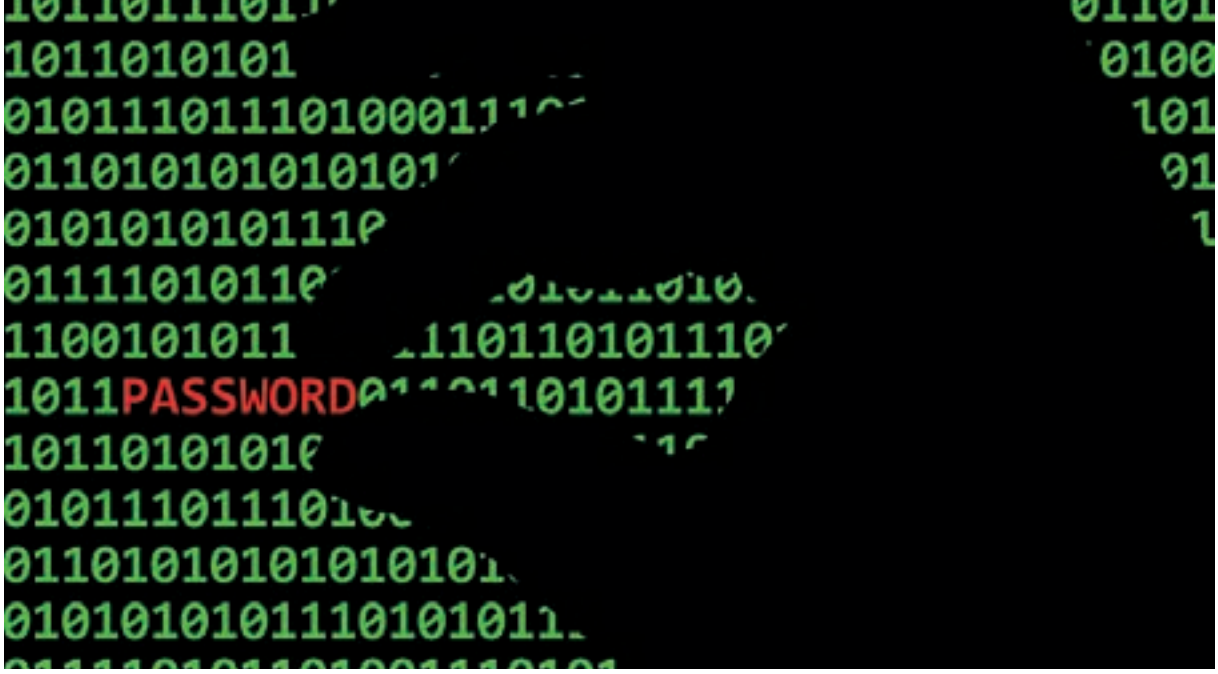
SICUREZZA

www.sicurezza.it

EXPO MILANO 2015

FIERA MILANO

Official Partner



La Redazione

Cybercrime:
sempre più costoso risolverlo

Condotto da Ponemon Institute per conto di HP Enterprise Security, lo studio 2014 Cost of Cyber Crime rileva come il campione di riferimento di aziende statunitensi vittime di attacchi informatici abbia subito danni per un costo medio annualizzato pari a 12,7 milioni di dollari, cifra che segna un incremento del 96% rispetto al primo studio realizzato per la prima volta cinque anni fa. Questi risultati rivelano, inoltre, come il tempo necessario per risolvere un attacco informatico sia aumentato del 33% nel medesimo periodo, mentre il costo medio sostenuto per la risoluzione di un singolo attacco ammonta a oltre 1,6 milioni di dollari.

Nel periodo preso in esame dallo studio si sono verificati gravi attacchi informatici negli Stati Uniti, che hanno coinvolto il furto di milioni di carte di pagamento, credenziali Internet, proprietà intellettuale e conti correnti bancari online. Secondo lo studio 2014 Cost of Cyber Crime, strumenti di security intelligence avanzati, come le soluzioni Security Information and Event Management (SIEM), Intrusion Prevention Systems (IPS), insieme a dati sulla reputazione, sistemi di network intelligence e analisi dei Big Data aiutano le aziende ad intercettare e arginare gli attacchi informatici, riducendo in maniera significativa il costo annualizzato del cyber-crimine.

"Se per i criminali informatici è sufficiente far breccia una sola volta nel sistema di un'organizzazione per carpirne i dati, le aziende devono riuscire tutte le volte a fermare la massa di attacchi sferrati ogni giorno nei loro confronti", ha affermato Art Gilliland, Senior Vice President and General Manager, Enterprise Security Products, HP. "Nessuna entità di investimento potrà mai proteggere completamente le aziende da attacchi informatici altamente sofisticati. Tuttavia, migliorando e rendendo prioritaria la propria capacità di contrastare le attività fraudolente attraverso soluzioni di intelligence quali SIEM, le organizzazioni potranno essere più efficaci nel limitare gli attacchi e ridurne l'impatto finanziario".

PRINCIPALI RISULTATI DELLO STUDIO 2014 COST OF CYBER CRIME

Il costo dei crimini informatici rimane molto alto. Il costo medio annualizzato del crimine informatico si attesta a 12,7 milioni di dollari, con picchi fra 1,6 e 61 milioni di dollari. Rispetto all'anno 2013, questo risultato segna un incremento del 9%del costo medio degli attacchi, pari a 1,1 milioni di dollari. I crimini informatici sono generalizzati e frequenti. Le aziende hanno segnalato un incremento del 176% nel numero di attacchi informatici, con una media di 138 attacchi riusciti alla settimana, rispetto ai 50 attacchi alla settimana riportati nella prima edizione di questo studio, nel 2010. La risoluzione dei crimini informatici richiede più tempo. Secondo il campione di aziende prese in considerazione, il tempo medio per identificare un attacco è di 170 giorni. Se si segmentano le tipologie di attacco, in media il tempo più lungo ammonta a 259 giorni e riguarda eventi collegati ad attacchi interni. Il tempo medio per risolvere un crimine informatico è di 45 giorni, mentre il costo medio causato durante tale periodo è di 1.593.627 dollari, dati che segnano un incremento del 33% rispetto allo scorso anno, in cui il costo medio era di 1.035.769 di dollari per una durata di 32 giorni.

I CRIMINI INFORMATICI IMPATTANO TUTTI I SETTORI

Dei 17 mercati compresi nello studio, tutti hanno riportato di esser stati colpiti da crimini informatici. Negli Stati Uniti il costo annualizzato più alto per organizzazione è stato registrato dai settori Energy & Utilities e Difesa. Il costo medio annualizzato per azienda nei mercati Energy & Utilities, Tecnologia e Retail è cresciuto in maniera più significativa negli Stati Uniti se confrontato al costo medio annualizzato registrato nei 5 anni in cui è stato pubblicato lo studio. In questo stesso periodo di tempo nel solo settore Retail il costo medio è più che raddoppiato.

I CRIMINI INFORMATICI PIÙ COSTOSI

I crimini informatici più costosi sono quelli causati da attacchi denial-of-service, insider malevoli e codice maligno. Questi attacchi costituiscono più del 55% del costo complessivo annuo del cyber-crimine per azienda. Il furto di informazioni continua a rappresentare la voce di costo esterna più rilevante, seguita dai costi correlati all'interruzione dell'attività. Su base annua, il furto di informazioni rappresenta il 40% dei costi esterni totali (in diminuzione del 2% rispetto alla media di cinque anni), mentre i costi correlati all'interruzione dell'attività o alla perdita di produttività ammontano al 38% dei costi esterni totali (in aumento del 7% rispetto alla media di cinque anni).
Rilevamento e ripristino risultano le attività interne più costose, che ammontano al 49% del costo totale annuo delle attività interne, le cui voci di costo più significative sono gli esborsi di cassa e la manodopera diretta.

L'IMPLEMENTAZIONE DI SOLUZIONI DI SECURITY INTELLIGENCE FA LA DIFFERENZA

Le aziende che utilizzano tecnologie di security intelligence sono risultate più efficienti nell'identificare e contenere gli attacchi informatici. Quelle che hanno implementato una soluzione SIEM, hanno ottenuto un risparmio medio sui costi pari a 5,3 milioni di dollari all'anno, con un incremento nei risparmi del 32% rispetto allo scorso anno. Le aziende dotate di tecnologie quali Intrusion Prevention System (IPS) e Next-generation Firewall (NGFW) hanno ottenuto un ritorno dell'investimento del 15%.

More at **www.hp.com/go/Ponemon**

IP Security FORUM

MARZO 2015
• VERONA •

GIUGNO 2015
• CATANIA •

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

www.ipsecurityforum.it - ethos@etosmedia.it

Fernando Pires(*)

Sistemi di gestione delle chiavi
nel settore educational

Le misure di sicurezza all'interno degli edifici universitari sono in rapida evoluzione. Non si tratta soltanto dell'evoluzione e del cambiamento della tecnologia per la sicurezza, dal controllo degli accessi alla videosorveglianza, ma anche del riconoscimento di un bisogno sempre crescente di misure di sicurezza più efficaci per mantenere un ambiente sicuro nelle università, come in ambienti "educational". Alcuni dei cambiamenti più importanti sono avvenuti nel campo del controllo degli accessi. Vediamoli.

Molte scuole si sono automatizzate grazie all'utilizzo di schede che possono essere scansionate o strisciate per ottenere l'accesso ad un edificio o un'aula. Tuttavia, in ogni università ci sarà sempre un ampio numero di chiavi fisiche in uso, provenienti da impianti originari e presenti nelle nuove costruzioni, che non fanno parte dell'impianto elettronico di controllo degli accessi. C'è ancora una gamma molto ampia di applicazioni convenzionali per sistemi di chiavi/lucchetti e questi dispositivi sono eccezionalmente vantaggiosi.

(*) Vice Presidente commerciale e marketing Morse Watchmans - **www.morsewatchmans.com**

DALLE CHIAVI AL CONTROLLO ACCESSI

L'utilizzo funzionale tipico di un ampio numero di chiavi fisiche in una struttura è quello di conservarle tutte in una sola collocazione controllata. Il termine "armadietto per chiavi" una volta si riferiva a un armadietto appeso al muro in cui le chiavi venivano disposte su ganci. Ed è proprio qui che è intervenuta un'importante evoluzione nell'utilizzo delle chiavi fisiche e nel bisogno di un livello superiore di controllo degli accessi, che ha portato progressi tecnologici nella forma e nella funzione degli armadietti per le chiavi. Oggi i sistemi di gestione delle chiavi sono di per sé sistemi per il controllo degli accessi completamente integrati che comunicano attraverso reti convergenti e offrono ai dirigenti delle università una gran mole di informazioni, che possono essere utilizzate per gestire e migliorare la sicurezza all'interno degli edifici universitari.
Nei sistemi più avanzati[1], ogni chiave viene bloccata all'interno dell'armadietto con una SmartKey che contiene un chip integrato: in questo modo un utente può rimuovere soltanto la chiave per la quale ha l'autorizzazione all'utilizzo. Le altre chiavi rimangono bloccate nel momento in cui l'utente inserisce il proprio codice di accesso o scansiona la propria o scheda o impronta digitale.

INTEGRAZIONE NEL SISTEMA DI SICUREZZA

Oltre alla custodia delle chiavi, i sistemi di gestione delle chiavi oggi disponibili possono essere integrati all'interno dell'impianto di sicurezza generale in uso nelle università. Il sistema di gestione delle chiavi può essere modulabile; più armadietti possono costituire un sistema unico completamente integrato per contenere centinaia di chiavi e altri oggetti in posizioni diverse, il tutto controllato con una singola interfaccia da PC. Attraverso l'integrazione di un software di gestione, gli utenti possono controllare il sistema e massimizzare le sue capacità di reportistica e programmazione degli accessi. Ad esempio, i responsabili del sistema possono stabilire i livelli di autorizzazione relativi al codice di ciascun utente e monitorare i dati da qualunque desktop collegato alla rete. I responsabili della sicurezza possono visionare i report con i dati su tutte le chiavi che sono state rimosse, per quanto tempo sono state rimosse, chi l'ha fatto e il luogo e

l'armadietto in cui sono state riportate. Inoltre, è possibile inviare ai responsabili della sicurezza avvisi via email prioritaria in base a parametri preimpostati. I responsabili della sicurezza possono quindi generare report utili e pratici sulla gestione della sicurezza per poi analizzare le informazioni e mantenere il massimo controllo sugli accessi e su tutte le questioni relative alla sicurezza. Gli allarmi possono essere innescati anche in alcune circostanze prestabilite come l'uso della forza per accedere o rimuovere le chiavi, codici utente non validi, una porta lasciata aperta per più di 10 secondi dopo l'uso, l'interruzione dell'alimentazione elettrica, una chiave mancante o non restituita in tempo oppure una chiave restituita da parte di un utente errato, ecc.

OLTRE IL CONTROLLO CHIAVI

Ma i sistemi di gestione delle chiavi si sono evoluti per fornire soluzioni che vanno addirittura oltre il controllo delle chiavi. Una tendenza emergente è quella di passare da chiavi fisiche ad altri oggetti ai quali è possibile accedere solo tramite accessi controllati. Ad esempio, alcune università hanno adottato la norma secondo cui le armi da fuoco degli addetti alla sicurezza devono essere messe sotto chiave e controllate quando non sono utilizzate. Altri dispositivi come radio, cellulari, palmari, ecc., utilizzati dai vari dipendenti nel corso di una data giornata, oltre a essere costosi rappresentano anche un potenziale rischio di violazione della sicurezza in caso di furto o smarrimento. Alcuni sistemi di gestione delle chiavi oggi dispongono di armadietti che possono contenere e controllare l'accesso alle armi da fuoco e a piccoli dispositivi con un registro di controllo per annotare quando e da chi vengono rimossi gli oggetti.

SECURITY EXPO 2015

25-28.03.

МЕЖДУНАРОДНА СПЕЦИАЛИЗИРАНА ИЗЛОЖБА ЗА ОХРАНА, СИГУРНОСТ, БЕЗОПАСНОСТ

ИНТЕР ЕКСПО ЦЕНТЪР • IEC

www.securityexpo.bg

Riccardo Brizzi(*)

Cominciamo dalla sicurezza

In un mondo dove i criminali informatici diventano ogni giorno più scaltri, e le conseguenze di un furto di dati possono portare alla distruzione di un'azienda, è evidente che la sicurezza è un fattore cruciale quando si parla di sviluppo del software. Peraltro, le complessità delle attuali minacce proibiscono di pensare alla semplice aggiunta di un livello di sicurezza nella fase finale del progetto, e di fare affidamento sui test prima che il progetto stesso entri in produzione, perché si tratterebbe in ogni caso di misure ampiamente insufficienti. Bisogna far diventare la sicurezza, e tutti i test associati alla sicurezza, una parte integrante del processo di sviluppo, per poter puntare a un risultato in linea con le aspettative. Invece moltissime aziende non riescono a raggiungere questo obiettivo, in quanto si tratta di un processo molto più facile da descrivere che da mettere in atto.

Prima di tutto, esaminiamo le conseguenze a cui va incontro un'azienda se il proprio software non è sicuro oppure è vulnerabile. Il rischio più grande, ovviamente, è quello della penetrazione all'interno dei server e del furto dei dati. Gli effetti di questi eventi sono spesso catastrofici, in quanto si associano costi interni per la perdita della produttività a costi esterni per la soluzione del problema, oltre all'impatto devastante della perdita di credibilità e di fiducia da parte degli utenti.

(*) Chief Operating Officer di SQS **http://www.sqs.ch/en**

Con il rapido aumento del volume dei dati, e i criminali informatici che diventano sempre più sofisticati, i costi possono solo salire. Un report di Ponemon Institute ha rivelato che - nonostante un aumento della spesa per la sicurezza da parte delle aziende, che è arrivata a 46 miliardi di dollari - il numero delle intrusioni è cresciuto del 20% e il costo medio di ciascuna intrusione è cresciuto del 30%1. Questo dimostra che la spesa per la sicurezza viene concentrata nel punto sbagliato, ovvero sulla sicurezza perimetrale e sull'infrastruttura, i due punti che i criminali informatici sanno come aggirare, per cui le aziende devono evolvere per far fronte alle nuove minacce con un approccio proattivo. Se le conseguenze sono così disastrose, perché la sicurezza continua a essere affrontata solo nell'ultima parte di un progetto? Spesso, sono i vincoli di tempo e di budget a impedire che venga considerata una priorità. Con questo approccio, però, è possibile effettuare solamente un rapido test di penetrazione prima di andare in produzione, e questa mancanza di "due diligence" spesso si trasforma in vulnerabilità facili da sfruttare da parte dei criminali informatici.

FARE TUTTI I PASSI NECESSARI

La sicurezza deve essere proattiva piuttosto che reattiva, deve partire durante il ciclo di sviluppo del software, e deve essere continuamente testata e misurata durante tutto il ciclo di vita. Tutto questo parte dalla definizione di parametri di sicurezza sia funzionali che non funzionali, il che si traduce in un progetto su cui gli specialisti dei test di sicurezza possono operare utilizzando il loro approccio (ovvero, simulando il comportamento dei criminali) e applicare i modelli delle minacce informatiche, per assicurare che siano presenti tutte le misure contro gli attacchi.

Durante tutto il processo la programmazione deve essere tenuta sotto controllo e analizzata, per verificare che i problemi siano stati risolti prima di passare alla fase successiva. Poi, durante la fase di test, gli specialisti possono cominciare ad attaccare il sistema per portare allo scoperto le vulnerabilità o i problemi più comuni. Questo significa che i test di penetrazione conclusivi (eseguiti da una terza parte indipendente) non dovrebbero essere che una verifica di routine, e non dovrebbero ritardare il rilascio per la presenza di problemi di sicurezza che non sono stati ancora affrontati e risolti. In ogni caso, sapere cosa fare è solo il primo passo. La sfida più importante è quella di verificare che i test sulla sicurezza vengano eseguiti durante ogni fase dello sviluppo, perché tutta l'organizzazione è allineata sullo stesso obiettivo e anche il management comprende i motivi per cui la sicurezza è un elemento fondamentale del processo. La responsabilità della sicurezza e dei test non dovrebbe ricadere solo sulle spalle del team di sviluppo, ma dovrebbe essere condivisa a tutti i livelli dell'organizzazione, e sostenuta da chi detiene i budget di spesa.
Fortunatamente, esistono strumenti che permettono di tenere sotto controllo il processo dall'inizio. L'Open Software Assurance Maturity Model (OpenSAMM) è un framework aperto e indipendente che aiuta le organizzazioni a strutturare e implementare una strategia per la sicurezza del software personalizzata in base ai rischi specifici del proprio settore, per cui una pubblica amministrazione avrà esigenze diverse da quelle di una finanziaria o di un'azienda in franchising. Le risorse fornite da OpenSAMM permettono di valutare le pratiche di sicurezza esistenti, e di sviluppare un programma bilanciato in grado di apportare dei miglioramenti concreti al programma di assicurazione della qualità e definire – e misurare – le attività legate alla sicurezza all'interno dell'organizzazione. Cominciare i progetti dalla sicurezza dovrebbe essere l'opzione più semplice, perché è quella che permette di risparmiare tempo e denaro, e proteggere l'azienda e le informazioni degli utenti dai rischi più importanti. Come abbiamo già detto, però, la sfida più importante è quella di portare tutta l'azienda a "pensare" in termini di sicurezza, soprattutto quando si parla di sicurezza del software. Peraltro, le aziende che rimangono indietro senza cambiare il proprio atteggiamento rispetto alla sicurezza sono quelle che rischiano di assistere a un collasso dei propri sitemi IT sotto agli attacchi sempre più sofisticati ed efficaci dei criminali informatici.

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

ANNO 4 – Numero 15 – DICEMBRE 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

Fallo subito!

sec solution