essecome ONLINE 08/19

Periodico digitale di informazione di security & safety

2019 · ANNO XXXIX

Sommario Interattivo

CLICCA SULL'ICONA PER SCARICARE L'ARTICOLO CHE TI INTERESSA

Guardie giurate autonome, a chi si deve la frittata?

Dedichiamo l'ultimo editoriale del 2019 al fatto dell'anno, la sentenza del TAR dell'Emilia Romagna (n. 118/2018) che, passando inaspettatamente in giudicato, ha confermato la possibilità che le guardie giurate possano essere lavoratori autonomi e non solamente lavoratori dipendenti da istituti di vigilanza.

E' una questione che in apparenza riguarda solo il settore della vigilanza ma che, in realtà, potrebbe impattare sull'intero sistema della sicurezza privata, alla luce del processo di integrazione sempre più spinta tra il mondo dei servizi e quello delle tecnologie.

Diversi sono gli aspetti da analizzare, comprese alcune stranezze.

1. Sul piano strettamente giuridico, la sentenza del TAR dell'Emilia non pare eccepibile. E' stato accolto il ricorso di un privato contro il decreto di diniego della prefettura di Modena alla nomina a guardia giurata come lavoratore autonomo, in quanto il giudice non ha ravvisato alcun motivo ostativo negli artt. 133 e 134 del TU LPS nè, tanto meno, nel diritto costituzionale e in quello comunitario. Non essendo stata impugnata entro i termini dalle controparti, la sentenza è passata in giudicato. Il Ministero dell'Interno ha quindi richiesto un parere al Consiglio di Stato che ha confermato l'applicabilità della sentenza *erga omnes* e, di conseguenza, lo stesso Ministero ha diramato alle Prefetture il 17 ottobre scorso la **circolare n. 14334/10089**,

2. Sul piano pratico, già tra le righe della circolare traspare la preoccupazione per le conseguenze che potrebbero derivare all'intero sistema della vigilanza privata, a partire dalle incombenze in capo a Prefetture e Questure. Come faranno infatti a rilasciare e controllare le licenze individuali, in potenza a migliaia? Sull'altro versante, come potrà un lavoratore autonomo dotarsi degli strumenti indispensabili per svolgere una qualsiasi attività di vigilanza a favore di altri, a cominciare dalla centrale operativa di supporto? Come provvederà alle sostituzioni di se stesso per riposi, ferie e malattie? Quali garanzie assicurative e patrimoniali potrà offrire ai clienti per le responsabilità contrattuali?

In prima battuta, verrebbe da pensare che le guardie autonome potranno solo offrirsi come turnisti agli istituti di vigilanza che li utilizzeranno *on-demand*, magari a costi inferiori delle guardie dipendenti. Lo si vedrà nel prosieguo.

Appare invece bizzarra l'affermazione, contenuta nella circolare sopra menzionata, che *"La sentenza è stata comunicata alla Prefettura di Modena dopo che erano già trascorsi i termini per la presentazione dell'appello, per cui essa è diventata inoppugnabile."* Notoriamente, nel diritto amministrativo gli appelli vengono presentati dall'Avvocatura dello Stato alla quale la sentenza del TAR viene notificata, e non dall'organo statale direttamente coinvolto. Essendo piuttosto inverosimile che l'Avvocatura abbia perso il termine dell'appello o che abbia omesso di informare tempestivamente la prefettura di Modena, sorge il dubbio che sia stata questa a far scadere inutilmente il termine per inerzia o, addirittura, per una consapevole opzione di non presentare appello.

Anche se la frittata è ormai fatta, vorremmo sapere:

- *è dovuta a colpa o volontà dell'Avvocatura dello Stato, come la circolare sembra voler adombrare?*
- *oppure è dovuta a colpa o volontà della prefettura di Modena?*
- *se così fosse, perchè il Ministero cercherebbe di far ricadere la responsabilità su altri organi dello Stato?*

Sarebbe apprezzabile che il prefetto Gambacurta, che ha firmato la circolare, chiarisse il motivo reale che ha impedito il ricorso nei termini, per un dovere di trasparenza e di tutela della credibilità di importanti istituzioni del Paese.

A SICUREZZA 2019 premiati i vincitori del Premio securindex Installatore Certificato

a cura della Redazione

Premiati a **SICUREZZA 2019** i vincitori della prima edizione del concorso organizzato da **essecome-securindex** per incentivare l'utilizzo del web da parte degli installatori certificati per promuovere la propria azienda.
Il riconoscimento è stato assegnato alle aziende installatrici (nelle categorie ditte individuali e società) che hanno ottenuto il maggior numero di visualizzazioni della propria scheda pubblicata nella pagina di securindex.com **Trova il tuo Installatore Certificato** nel periodo 1 aprile - 31 ottobre 2019.
La premiazione è avvenuta alla presenza di **Paolo Pizzocaro**, Exhibition Manager di SICUREZZA, e di Luca Baldin, Project Manager di Smart Building Expo, che hanno sottolineato l'importanza delle professionalizzazione e della formazione continua per gli operatori della sicurezza e della Building Automation, settori sempre più integrati e in fase di continua evoluzione.
Giancarlo Liberatore, Presidente del Gruppo di **VIGILO4YOU**, Main Partner del Premio securindex Installatore Certificato, ha consegnato i premi messi in palio per i vincitori dalla società di Brescia che si propone come partner degli installatori professionali per completare l'offerta tecnologica con servizi di intervento on-demand.
Proclamato vincitore assoluto dell'edizione 2019 Electronic System di Monza Brianza con 701 visualizzazioni, mentre nelle categorie territoriali hanno vinto:

Nord: Elettronica Ferrario di Varese - 562 visualizzazioni | **TS Lario** di Como - 559 visualizzazioni

Centro: ITS di Frosinone - 694 visualizzazioni | **Ge.Va** di Roma - 520 visualizzazioni

Sud: Tecnosecurity di Oristano - 631 visualizzazioni | **Telesicurezza Service** di Agrigento con 558 visualizzazioni

Giordano Turati, CEO di **TSec**, ha quindi consegnato a **Vincenzo Ferrigno** (Telesicurezza Service) il Premio speciale TSec per l'azienda propria cliente certificata che ha ottenuto il miglior piazzamento nella classifica finale del Premio securindex.
Giancarlo Liberatore ha dichiarato: *"Abbiamo colto al volo l'opportunità del premio essecome-securindex legato all'iniziativa Trova il tuo installatore Certificato come strumento per avvicinarci sempre più al mondo degli Installatori professionali che oggi rappresentano il futuro della Sicurezza sia in ambito B2B che B2C.*
VIGILO4YOU, società che offre un servizio innovativo di vigilanza grazie all'esperienza di oltre 70 anni maturati nel settore della sicurezza, è convinta che questo rapporto sinergico darà la possibilità agli installatori di poter approcciare in modo efficace un mercato molto vasto come quello del residenziale e dello small busines, offrendo a prezzi competitivi un pacchetto completo formato da impianto di allarme, servizio di pronto intervento a consumo e copertura assicurativa."

"È stato bello incontrare molti degli installatori certificati nel nostro stand a SICUREZZA - ha infine commentato **Francesca Dalla Torre**, coordinatrice della Community - *che stanno dimostrando di apprezzare il nostro impegno per sostenerli nell'attività quotidiana. Anche il gruppo che abbiamo attivato su whatsapp sta generando scambi di informazioni e di contatti tra colleghi, uno strumento utile anche per generare opportunità di lavoro".*

Gli incontri di securindex formazione a SICUREZZA 2019, una partecipazione superiore alle aspettative

a cura della Redazione

Sono stati oltre 200 i partecipanti ai dieci incontri organizzati il 13 e il 14 novembre nello stand di essecome a SICUREZZA 2019 con i docenti di securindex formazione, oltre il doppio di quanti si erano iscritti online nei giorni precedenti la fiera. Ogni docente ha tenuto due incontri di 30' ognuno per presentare una sintesi della propria lezione inserita nel programma dei corsi organizzati da securindex formazione nel primo trimestre 2020 (vedi box).

Incontri che sono stati apprezzati sia dagli operatori che hanno già ottenuto la certificazione in base alla Norma CEI 79.3, utili per ricevere l'attestato di partecipazione da esibire per il mantenimento della certificazione, ma anche per ripassare argomenti in continua evoluzione, sia da coloro che stanno valutando l'opportunità di accrescere le proprie competenze e di accedere successivamente alla certificazione.

Una partecipazione così elevata nei giorni di fiera, proprio quando i visitatori cercano di dedicare tutto il tempo di permanenza alla ricerca di novità e di contatti utili, conferma la crescente attenzione per la formazione continua nel campo della sicurezza, delle reti IP e degli aspetti legali del contratto di fornitura, sempre più determinanti nei rapporti con i clienti soprattutto da quanto è entrato in vigore il GDPR.

Roberto Dalla Torre, coordinatore dei corsi dell'Area Tecnica di securindex formazione, sottolinea: *"Sono diversi i motivi all'origine dell'interesse degli operatori del settore per le nostre proposte formative. Da una parte, la certificazione delle competenze sta diventando un fattore discriminante negli appalti dei grandi utenti pubblici e privati; dall'altra, la rapidissima evoluzione delle tecnologie e delle normative rende indispensabile l'aggiornamento continuo di chi opera in questo mercato. Infine, i sistemi antintrusione vengono oggi realizzati anche da installatori provenienti da altri settori come, ad esempio, domotica, energia, elettrico, illuminazione, antenne, reti, ecc, che necessitano delle conoscenze fondamentali delle regole dell'arte degli impianti di sicurezza per soddisfare il cliente e per tutelare se stessi".*

I CORSI DI SECURINDEX FORMAZIONE IN PROGRAMMA NEL PRIMO TRIMESTRE 2020
(vedi il calendario online)

Cod #AA - Corso propedeutico alla certificazione secondo la Norma CEI 79.3:2012 - 16 ore
Responsabilità del fornitore - Introduzione alle normative sul trattamento dei dati | 4 ore - docente **avv. Laura Lenchi**
Norma CEI 79.3:2012 - Introduzione - Impostazione di calcolo dei livelli di prestazione | 12 ore - docente **Roberto Dalla Torre**

Cod #AB - Corso propedeutico alla certificazione secondo la Norma CEI 79.3:2012 + Videosorveglianza - 24 ore
Responsabilità del fornitore - Introduzione alle normative sul trattamento dei dati | 4 ore - docente **avv. Laura Lenchi**
Norma CEI 79.3:2012 - Introduzione - Impostazione di calcolo dei livelli di prestazione | 12 ore - docente **Roberto Dalla Torre**
Reti IP - Introduzione e sicurezza - Videosorveglianza: progettazione | 8 ore - docente **Luca Girodo**

Cod #AC - Reti IP per sistemi di videosorveglianza - 8 ore
Reti IP - Introduzione e sicurezza - Videosorveglianza: progettazione | 8 ore - docente **Luca Girodo**

Cod #AD - La vendita dei sistemi di sicurezza - 16 ore
Le 7 tappe della vendita - colloquio telefonico - primo contatto - sequenza della vendita | 8 + 8 ore - docente **Maurizio Callegari**

Cad #AE - Telesorveglianza e GDPR
GDPR e Videosorveglianza - Soggetti coinvolti - Accontability, Privacy by Design, DPIA | 8 ore - docente **avv. Maria Cupolo**

SICUREZZA 2019 e Smart Building Expo chiudono con oltre 28.000 presenze

a cura della Redazione

SICUREZZA, manifestazione leader europea per security e antincendio, e **Smart Building Expo**, la fiera dell'integrazione tecnologica - a Fiera Milano (Rho) dal 13 al 15 novembre scorsi - si sono chiuse con **28.629 operatori professionali**. **Numeri in crescita del 12%** rispetto all'edizione precedente, con presenze internazionali da 88 Paesi, tra cui i dieci maggiormente rappresentati sono stati: Svizzera, Regno Unito, Grecia, Spagna, Tunisia, Francia, Germania, Federazione Russa, Ucraina e Croazia. Un incremento che testimonia come SICUREZZA sia ormai riconosciuta come hub di riferimento per i professionisti di tutta Europa e dell'area del Mediterraneo.

I 619 espositori - +33% rispetto alla scorsa edizione, per il 30% esteri da 37 Paesi - hanno presentato innovazione di prodotto e numerose anteprime a un pubblico di professionisti attento e motivato.

La profonda evoluzione che stanno vivendo il mondo della security e della building automation e lo scenario tecnologico in rapido cambiamento hanno fatto da sfondo ai tre giorni di fiera.

Integrazione, digitalizzazione, soluzioni smart si sono confermati i driver delle proposte in manifestazione.

La **security** vede soluzioni sempre più digitali, wireless (quindi facili da installare) e customizzate per tutti gli ambiti di applicazione - dalla casa alla città, fino all'industria, ai trasporti e ai luoghi del divertimento - ed espressione della ricerca tecnologica più avanzata: biometria, intelligenza artificiale, riconoscimento vocale, IoT sono ormai diffusi in tutti i comparti, dalla building automation alla videosorveglianza, fino al mondo del controllo accessi.

Sul fronte della **building automation** il processo di integrazione e le potenzialità del 5G hanno rappresentato il fil-rouge dell'offerta. La stretta collaborazione tra tutte le tecnologie ha eliminato le barriere tra le verticalizzazioni. Impiantistica, building automation, sistemi audio-video, risparmio energetico, piattaforme digitali, telecomunicazioni

lavorano ormai in sinergia come parti di un sistema unico e dinamico, incentrato sulla gestione intelligente e l'utilizzo dei cosiddetti "Big Data".

Con la partecipazione di oltre 4000 professionisti, grande riscontro ha ottenuto anche il ricco programma dedicato all'aggiornamento professionale.

Gli **oltre 100 convegni e incontri** - molti dei quali hanno consentito agli operatori di ottenere crediti formativi per diverse figure professionali (periti industriali, ingegneri, installatori, operatori della vigilanza) – hanno visto al centro della proposta il valore delle risorse umane e la centralità della formazione continua. Le tematiche di più stretta attualità per tutti i comparti sono state affrontate da esperti a livello internazionale, associazioni e realtà accademiche, con contenuti fortemente apprezzati in un momento in cui il mercato sta vivendo una vera e propria rivoluzione.

Grande interesse ha anche incontrato il debutto della **Cyber Arena**, la nuova area espositiva, formativa e informativa dedicata al tema della Cyber Security, nata con l'obiettivo di aiutare le aziende a gestire al meglio le minacce informatiche.

Tutto esaurito al convegno ANIVP a SICUREZZA 2019 sulla formazione delle guardie giurate

a cura della Redazione

All'evento del 15 novembre presso **Fiera Sicurezza** organizzato da **ANIVP** in collaborazione con **essecome-securindex** si è avuta una grande partecipazione di operatori della vigilanza. I relatori hanno fornito una rappresentazione precisa e professionale della realtà attuale in materia di formazione nel campo della sicurezza.

Importanti i dati forniti da **Paolo Furlan** con riferimento alla sicurezza sussidiaria e al numero di abilitazioni rilasciate dalle Commissioni specifiche costituite presso le Prefetture; utile l'approfondimento tematico da parte di **Marco Stratta** e dell'avv. **Ezio Moro** in materia di Decreto Formazione, ovvero il riferimento normativo che in un prossimo futuro cambierà le abilitazioni delle Guardie Particolari Giurate.

Di notevole interesse il focus fornito da **Cesarina Giani**, Vice Presidente EBIVEV, e da **Aldo Giammella**, Presidente EBIVER, con riferimento alle sempre più importanti iniziative in materia di formazione da parte degli Enti Bilaterali territoriali della vigilanza privata.

Ha chiuso la giornata **Gabriele Guarino**, amministratore di **San Giorgio Srl**, società specializzata in formazione nel campo della sicurezza, presentando in anteprima **X-BAG**, il più avanzato software per la formazione di operativi addetti allo screening merci.

Claudio Moro, Presidente di ANIVP, ha espresso il proprio ringraziamento ai relatori e ai partecipanti: *"La giornata di oggi è una nota di ottimismo per questo settore, perché ha potuto evidenziare come il business della sicurezza riesca ancora ad esprimere delle professionalità importanti e a generare una grande attenzione anche da parte della sua utenza più specializzata."*

Il Segretario Generale di ANIVP **Marco Stratta** ha commentato: *"La sala piena ha dimostrato che la formazione degli operatori è un tema di attualità che desta interesse. Ad oggi la formazione che riguarda la vigilanza privata, tra sicurezza sul lavoro, formazione operativa e specialistica si stima un giro di affari che si avvicina ai 10 ml di euro. E' stato pertanto un fatto positivo aver potuto illustrare le differenti proposte che oggi possono essere di riferimento per le società di vigilanza, fornendo dati, riferimenti, prospettive. Sono convinto che Il comparto della vigilanza, e della sicurezza più in generale, possa trovare una sua affermazione solo nella professionalizzazione e nella preparazione degli operatori. Il 15 novembre abbiamo messo un tassello in questa direzione."*

CONSORZIO STABILE
GossItalia

GESTIONE, ORGANIZZAZIONE E SERVIZI PER LA SICUREZZA

CONSORZIO STABILE GOSS ITALIA Via Torricelli, 15/B - Verona - Italia | Tel +39 045 8230738 | Fax +39 045 8231532
Mail direzione@gossitalia.it | Web www.gossitalia.it

Da ANSSAIF l'impegno per la diffusione della cultura della cyber security e il sostegno all'occupazione giovanile

intervista a Mario Sestito, Segretario Generale ANSSAIF - Ass. Nazionale Specialisti Sicurezza Aziende Intermediazione Finanziaria

ANSSAIF ha organizzato nel 2019 un corso a distanza sulla cyber security in collaborazione con ELIS riservato a giovani disoccupati/sottoccupati. Possiamo riassumere l'esito?
Premesso che tra gli obiettivi alla base dell'Associazione sono la conservazione e il miglioramento del patrimonio di esperienze accumulato negli anni dagli Associati per metterlo a disposizione degli altri, nel 2019 abbiamo avviato, in aggiunta alle lezioni che teniamo in aula per i ragazzi delle scuole medie, un progetto di *"diffusione delle conoscenze e competenze digitali"* tramite metodologie e processi formativi tesi ad una corretta cultura della gestione dei rischi insiti nell'utilizzo degli strumenti digitali. Quest'anno, in accordo con l'ELIS e grazie a CISCO Academy, abbiamo avviato oltre 100 giovani allo studio della cyber security. Il percorso formativo è articolato in tre corsi in successione: ***"Get connected"*** per acquisire conoscenze di base sulle principali componenti di un computer; ***"Introduzione alla cyber security"*** consistente in un corso generale sulla protezione dei dati personali, privacy online e social media. Per finire, ***"Cyber security essential"*** strutturato in lingua inglese, su temi di etica e cyber security, sicurezza dell'informazione e sicurezza dei sistemi e delle reti. Come risultato, abbiamo oltre 20 giovani che hanno concluso con esito positivo l'intero ciclo formativo.

Quali prospettive vengono offerte a coloro che hanno completato con successo il corso?
Il primo passo è la possibilità di frequentare l'Associazione per continuare nell'apprendimento della tematica non solo dal punto di vista della conoscenza ma, soprattutto, per assimilare competenze e abilità, cioè il *"saper fare"* per affrontare in modo efficace il mondo del lavoro. A chi acconsente, viene quindi offerta la possibilità di presentare il curriculum ad aziende conosciute per possibili opportunità di lavoro. Vorrei sottolineare a questo proposito che già alcuni dei giovani che hanno frequentato il primo corso hanno trovato occupazione. Per ultimo, non è da sottovalutare la possibilità di avviare dei progetti (sotto lo slogan *"conoscere e farsi conoscere"*) rivolti a specialisti di settore, con la tutela di Associati seniores di ANSSAIF che, come noi affermiamo, sono *"nati per servire da esempio"*.

Nel corso del XV Congresso di ANSSAIF è stato affrontato, tra gli altri, il problema della consapevolezza dei rischi cyber nelle PMI. Cosa intende fare l'Associazione per divulgare la cultura della sicurezza nelle aziende?
La consapevolezza sui rischi è fondamentale per poterli capire ed affrontare. L'ipotesi di poter parlare alle PMI, anche attraverso le associazioni di categoria o di settore, è un concreto passo verso la conoscenza dei rischi che si possono insidiare nei sistemi e nelle abitudini delle persone che li utilizzano ogni giorno, anche per sensibilizzarle nei confronti delle responsabilità che gli derivano nei confronti dei terzi, a partire dalla tutela dei dati personali.

È possibile pensare alla creazione di opportunità di lavoro presso le PMI per giovani formati sulla cyber security?
È uno dei nostri obiettivi. Come ho detto prima, questa è una grande opportunità per i giovani.

Consapevolezza, conoscenza, condivisione: le tre parole chiave per proteggersi dai rischi della rete

intervista al Prefetto Domenico Vulpiani, già responsabile per il Ministero dell'Interno della transizione alla modalità operativa digitale | a cura di Raffaello Juvara

Possiamo fare un punto in generale sulle nuove minacce provenienti dalla rete?
A cinquant'anni dalla nascita di Internet, cioè dalla prima trasmissione di un pacchetto di dati tra due computer, assistiamo oggi ad una diffusione pervasiva di apparati mobili interconnessi che, unita all'avvento di nuovi oggetti tecnologici anch'essi collegati alla rete (c.d. *Internet of Things*), ha ridimensionato il concetto di *cybersecurity* e ampliato il perimetro da difendere. Si è passati cioè, dalla necessità di proteggere un sistema di elaborazione dati "fisico" e le sue connessioni di rete, ad un sistema di informazioni e, quindi, di vulnerabilità "diffuse". Se poi riflettiamo sul fatto che, al centro di questo sistema, c'è sempre l'individuo con la sua ineffabile imperfezione e con in mano il suo inseparabile *device*, comprendiamo i molteplici rischi per la sicurezza.

Quali sono i "nuovi" crimini più diffusi e quali le categorie più esposte?
In questo "ecosistema digitale", quattro quinti degli attacchi effettuati (il 79%) sono finalizzati ad ottenere denaro o a sottrarre informazioni per monetizzarle successivamente, così come riportato nel rapporto Clusit 2019.
Alle tradizionali tecniche di cyber-attacco già note, vanno ad aggiungersi nuove tipologie di minacce orientate in primo luogo alle informazioni presenti nei sistemi più diffusi tra gli utenti, cioè alle applicazioni di *social network* e alle piattaforme per apparati mobili. Inoltre, si è assistito ad un'intensificazione delle attività di spionaggio e sabotaggio (queste ultime soprattutto attraverso *fake news*), sia a livello aziendale che istituzionale, a scapito delle preziose conoscenze e competenze di cui sono in possesso agli attori del contesto produttivo e mettendo a rischio la possibile tenuta del sistema democratico nazionale. In ultimo, ma non per ultimo, troviamo le nuove vulnerabilità connesse ai paradigmi dell'*Intelligenza Artificiale* e dell'automazione industriale avanzata (c.d. Industria 4.0). Da un lato, infatti, l'impiego di tali tecnologie potrebbe consentire la realizzazione di cyber-attacchi sempre più efficaci e meno costosi, mentre dall'altro tali sistemi potrebbero essere silenziosamente alterati e indotti in errore oltre che, più banalmente, attaccati e compromessi con tecniche tradizionali.

In che modo si è dovuto adeguare il metodo investigativo per contrastare la criminalità cibernetica?

Da anni, per contrastare le minacce provenienti dal cyber-spazio, gli attori (istituzionali e non) sono attivi, ciascuno nell'ambito delle proprie competenze, con strumenti tecnologici, investigativi, normativi ed informativi impiegati per "rincorrere" le sempre più sofisticate tecniche di attacco. In particolare, per quanto riguarda la difesa del perimetro cibernetico della propria azienda o istituzione, si è passati da una difesa tradizionale basata fondamentalmente sul monitoraggio del perimetro "logico" attraverso *firewall, antivirus, IDS/IPS*… ad una difesa "condivisa" fondata sull'*information sharing* (SOC, CERT,…). Ovviamente, le nuove frontiere della minaccia obbligano gli addetti del settore ad escogitare tecniche di contrasto sempre più sofisticate, che si spingono fino ad anticipare il possibile attacco attraverso il tracciamento, la ricerca e l'analisi degli avversari fuori dal perimetro: in sostanza, prima che questi costituiscano un pericolo attuale. Queste tecniche, definite di *cyber threat intelligence*, rappresentano una forma di analisi "prognostica" della minaccia, che consentono di neutralizzare o, quantomeno, di mitigare le azioni di malintenzionati nei confronti di un sistema informatico.

Quali sono i livelli di consapevolezza dei rischi della rete, in particolare da parte dei giovani?

Nessuna tecnologia, da sola, può rendere immuni da attacchi ostili o da eventi disastrosi poiché, torno a ricordare, al centro di qualunque sistema digitalizzato c'è sempre l'essere umano con le sue vulnerabilità e imperfezioni. Per tale ragione, è fondamentale diffondere la cultura della *cybersecurity* ad ogni livello di competenza, dall'utilizzatore di uno *smartphone* all'amministratore di una rete aziendale complessa. Tale esigenza di propagazione culturale può essere sintetizzata in tre parole: *consapevolezza, conoscenza e condivisione*, che sono relative ai rischi della rete e alle soluzioni adottate per difendersi. I giovani che si affacciano al mondo del cyber-spazio non possono prescindere da questi concetti, se vogliono uscirne indenni. Quelli che, invece, intendono approcciarsi ad attività lavorative legate alle tecnologie digitali, potranno sfruttarne le potenzialità se sapranno anticipare le esigenze dei cyber-consumatori con prodotti e servizi evoluti nei settori maggiormente deficitari come, ad esempio, semplificazione amministrativa, sanità, ecologia, supporto alle disabilità.

I nuovi paradigmi legislativi della compliance e le difficoltà di recepimento da parte degli operatori

intervista a Corrado Giustozzi, esperto di sicurezza cibernetica presso il CERT-PA (Agenzia per l'Italia Digitale) e componente l'Advisory Group di Enisa (Agenzia dell'Unione Europea per la cybersecurity)

GDPR, Direttiva NIS, Regolamento eIDAS cambiano radicalmente il paradigma della compliance, passando dal criterio dell'adempimento a quello della responsabilizzazione degli operatori. Quali sono i presupposti del legislatore europeo per questo cambiamento epocale, soprattutto per l'Italia?

Il paradigma adottato dal Legislatore europeo per normare gli obblighi di sicurezza in determinati settori regolati, quali ad esempio i fornitori di servizi critici per la società oppure i soggetti che trattano dati personali, è effettivamente molto cambiato o per dir meglio si è assai evoluto, in questi ultimi anni.

Si è passati infatti in modo abbastanza repentino da un approccio interamente prescrittivo, basato su una logica che potremmo definire "dell'adempimento", ad un approccio finalizzato ai risultati e basato su una logica "della responsabilizzazione". Ciò significa, in termini generali, che gli operatori non devono più limitarsi a seguire passivamente le indicazioni puntuali fornite dalle Autorità di vigilanza e controllo, come avveniva in passato, ma devono divenire parte attiva nel contribuire essi stessi a definire e migliorare i propri processi dal punto di vista della compliance e del raggiungimento degli obiettivi imposti.

Questo è un vero ribaltamento di prospettiva, perché il Legislatore oggi dice agli operatori "cosa devono ottenere" e non più "cosa devono fare e come", lasciando loro la libertà di decidere qual è il modo migliore per ottenere i risultati richiesti. Ciò ha comportato un certo disorientamento negli operatori, che in passato erano abituati a sentirsi dare indicazioni puntuali su come comportarsi, mentre oggi devono deciderlo da soli.

Ad esempio, in molti hanno lamentato il fatto che nelle leggi più recenti, quali il GDPR, manchino gli elenchi prescrittivi di "Misure minime" di sicurezza presenti in passato: questa tuttavia non è una dimenticanza del Legislatore ma una conseguenza diretta di questo nuovo approccio, secondo il quale è compito di ciascun operatore definire ed adottare le misure di sicurezza più idonee ed adeguate alla propria specifica situazione, derivandole da una attenta ed accurata analisi del proprio profilo di rischio.

In altre parole, il Legislatore ha finalmente riconosciuto ciò che gli esperti di sicurezza predicavano da anni: ossia che ciascun operatore è diverso dagli altri ed ha le sue proprie specificità, ed è dunque sbagliato imporre a tutti le medesime misure (minime) di sicurezza, le quali rischiano di essere insufficienti per qualcuno e sovrabbondanti per qualcun altro. L'approccio più corretto è invece quello nel quale ciascuno definisce le misure più adatte a sé, derivandole da una analisi del rischio che solo lui può fare; prendendosi così la responsabilità dell'intero processo, dalla fase di analisi a quella di implementazione e di esercizio. Si tratta ovviamente di un approccio molto difficile da seguire, in quanto richiede una grande maturità nell'operatore, ma è l'unico a fornire risultati efficaci; oltretutto, se affrontato con serietà, non solo mette l'operatore al riparo da eventuali problemi in caso di incidente (in quanto a quel punto egli dovrà poter sostenere davanti all'Autorità di vigilanza le proprie scelte) ma, soprattutto, consente di dosare gli investimenti in sicurezza secondo criteri oggettivi, consentendo così anche di operare risparmi non indifferenti.

È importante notare infine che questo approccio è ormai adottato in tutte le recenti normative rilevanti, quali il **Regolamento (UE) 910/2014 (eIDAS)** sul mercato comune per i servizi digitali (dove riguarda i fornitori di servizi fiduciari), il **Regolamento (UE) 679/2016 (GDPR)** sulla protezione dei dati personali (dove riguarda tutti i titolari di trattamento), ed infine la **Direttiva (UE) 1148/2016 (NIS)** sull'innalzamento della sicurezza di quelle che in passato venivano chiamate "infrastrutture critiche" (dove riguarda tutti i fornitori di servizi essenziali per il funzionamento della società).

E quali sono le risposte delle funzioni interessate nel nostro Paese, dal suo punto di osservazione?

L'Italia ha prontamente messo a punto gli apparati di gestione previsti da queste normative, ad esempio costituendo le apposite Autorità nel caso della Direttiva NIS (mentre per il GDPR l'Autorità era già esistente, essendo lo stesso Garante della protezione dei dati personali), ma forse ha dato un po' per scontato che gli operatori avrebbero colto da soli la grande differenza di approccio e sarebbero stati in grado di adeguarsi prontamente ed autonomamente.

La mia sensazione è invece che gli operatori non si siano resi conto della portata del cambiamento, e delle nuove responsabilità che ora incombono su di loro, e non sappiano bene come regolarsi per rendersi conformi ai nuovi requisiti.

Quali dovrebbero essere le chiavi per divulgare in modo appropriato questo nuovo approccio e ottenere risultati positivi per la tutela delle informazioni?

Questo nuovo approccio, che rende l'analisi del rischio un elemento cruciale nella compliance di ogni operatore, non è purtroppo stato correttamente e tempestivamente divulgato e spiegato presso gli interessati. E, come al solito, sono soprattutto le imprese più piccole, quelle che non hanno una cultura specifica della sicurezza, a farne le spese, perché non sanno a chi rivolgersi per impostare un approccio corretto e finiscono magari preda di consulenti improvvisati e con pochi scrupoli.

Secondo me le associazioni di categoria dovrebbero darsi come obiettivo proprio quello di informare e formare i loro associati su questi temi, aiutandoli a crescere quel minimo necessario per dotarsi di sufficiente autoconsapevolezza e poter, magari, scegliere con cognizione di causa il miglior consulente ed il miglior percorso di adeguamento.

Quali sono le differenze più significative nelle reazioni tra le diverse generazioni?

È difficile generalizzare, tuttavia la mia impressione è che le imprese più giovani e innovative, le start-up, siano sempre più allergiche ai temi della compliance, della sicurezza e della privacy, che sono visti come inutili ed ingombranti retaggi di un passato analogico reso obsoleto dalle tecnologie digitali. In realtà è tutto l'opposto: usando male le straordinarie funzionalità messe a disposizione dalla Rete e dalla capillare diffusione delle tecnologie personali si possono recare enormi danni a terzi, siano essi i propri clienti o altri componenti della società civile (altre aziende, cittadini, eccetera). Per questo è tanto più importante che i concetti di "security by design", di analisi del rischio e di analisi di impatto, entrino a pieno diritto nel ciclo di sviluppo di tutti i prodotti e servizi, soprattutto quelli interamente digitali e network-centrici.

Store Sonification, una strada non intrusiva per la sicurezza dei negozi e la shopping experience

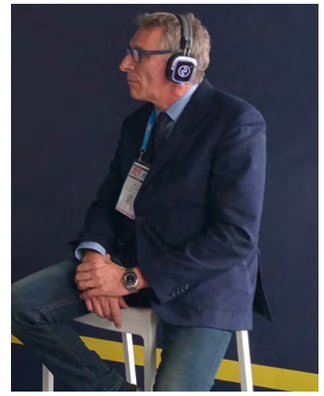
a cura della Redazione

Proseguendo nell'analisi delle opportunità per il mondo del retail di ottimizzare la gestione dei negozi utilizzando le prestazioni delle tecnologie digitali, iniziata con **SFR 2019**, il **Laboratorio per la Sicurezza** e **essecome-securindex** hanno organizzato in occasione di **Forum Retail 2019** un seminario con la partecipazione di **AXIS Communications** dedicato alla *Store Sonification*, intesa come utilizzo evoluto dell'audio all'interno dei punti vendita. Il 30 ottobre **Giuseppe Mastromattei**, Presidente del Laboratorio per la Sicurezza, **Kjetil K. Hansen**, professore associato al KTH - Royal Institute of Technology di Stoccolma - e **Pietro Tonussi**, BDM per il Sud Europa di AXIS Communications, hanno esaminato le potenzialità di una disciplina relativamente nuova, integrabile in un'unica piattaforma tecnologica che garantisce funzioni di security, safety e business intelligence migliorando l'esperienza di acquisto dei clienti in un quadro complessivo di ottimizzazione delle risorse umane e dei sistemi del negozio.

Giuseppe Mastromattei ha commentato: *"La Store Sonification è senza dubbio un tema di grande interesse per il mondo del Retail, in costante ricerca di nuove soluzioni in grado di ridurre i costi di gestione dei punti vendita, di attrarre e fidelizzare i clienti, di analizzarne i comportamenti e, allo stesso tempo, di proteggere il patrimonio aziendale. L'esplorazione delle possibilità di impiegare la "Sonification" anche ai fini di security è una nuova frontiera che corrisponde pienamente agli scopi del Laboratorio, da affrontare con l'apporto scientifico del mondo accademico. Abbiamo molto apprezzato il contributo in questa occasione del prof. Kjetil F. Hansen del KTH di Stoccolma, che studia gli effetti della musica sul comportamento delle persone, con il quale abbiamo condiviso le specifiche esigenze del settore Security. Daremo seguito a questo incontro sviluppando un percorso di collaborazione dal quale potrebbero derivare interessanti soluzioni da poter essere utilizzate dai gruppi internazionali del Retail; soluzioni che consentirebbero alla funzione Security di integrarsi ancora di più con il Business. Il Laboratorio crede molto nell'innovazione, e questo progetta rappresenta concretamente quanto sia fondamentale che tra Università, Clienti e Fornitori ci sia un costante confronto, affinché, insieme, diventino portatori di conoscenza, per consentire così alle aziende di attraversare i propri confini e gestire consapevolmente il cambiamento".*

Pietro Tonussi, BDM per il Sud Europa di AXIS Communications ha risposto alle seguenti domande:

Quali possibilità di integrazione si ritrovano tra i sistemi audio e quelli di raccolta/analisi delle immagini?
Il mondo del retail deve da sempre fronteggiare una duplice sfida: attrarre il maggior numero possibile di clienti e garantire il dovuto livello di sicurezza, sia in termini di loss prevention che di safety. Generalmente, la funzione di sorveglianza e di monitoraggio è affidata alle telecamere, mentre il compito di migliorare la customer experience è competenza dei sistemi audio. Grazie alle nuove tecnologie, questi due sistemi possono interagire e aiutarsi a vicenda a migliorare entrambe le performance.



La musica di sottofondo è ormai presente nella maggior parte dei negozi e il motivo è semplice: la musica, creando delle connessioni emotive che attivano determinati comportamenti, è una delle leve in grado di attirare i consumatori e di invogliarli ad effettuare acquisti. Le canzoni natalizie, ad esempio, contribuiscono a creare un'atmosfera di festa e inducono le persone a comprare regali e addobbi per la casa. Lo confermano anche i risultati della ricerca "Il Negozio del Futuro in Italia", recentemente commissionata da Axis ad Ipsos per rilevare le opinioni degli italiani riguardo l'esperienza d'acquisto nei punti vendita fisici. Il 75% degli intervistati considera, infatti, la musica un elemento in grado di rendere più piacevole la permanenza nel negozio e spera di poter ascoltare, in futuro, le proprie canzoni preferite, grazie a una personalizzazione della playlist.
Dall'integrazione del sistema audio con quello di analisi delle immagini, grazie all'unione di due tipi di analitiche, può derivare un notevole miglioramento sia della customer experience, in termini di ottimizzazione dei tempi e degli spazi di acquisto, che della loss prevention.
Il supporto delle analitiche permette un miglior servizio al cliente attraverso tempestive segnalazioni al personale che potrà prendere decisione rapide e precise.
Fondamentale è anche il supporto che l'integrazione delle due tecnologie può dare agli addetti alla sicurezza. Ad esempio, la possibilità di incrociare le immagini con il riconoscimento automatico di tracce audio preimpostate, come il rumore di uno sparo o un'aggressione verbale, permette di generare allarmi automatici e di intervenire rapidamente. Il rilevamento di una presenza non autorizzata in una certa area del negozio, permette invece di far scattare suoni o messaggi dissuasori, prevenendo eventuali furti o vandalismi.
E' evidente che questa ottimizzazione dei sistemi audio e video diventa ancor più rilevante nel caso di realtà che possiedono numerosi punti vendita come, ad esempio, la GDO.

Quali sono i driver di Axis, il principale produttore occidentale di videosorveglianza, nell'affrontare la nuova sfida della store sonification?
L'integrazione di audio e video è sicuramente il driver perfetto di Axis: le nostre soluzioni consentono di utilizzare questi due sistemi in modo congiunto e garantiscono un elevato livello di controllo su quanto accade all'interno del negozio. Un'esigenza pressante tanto per gli addetti del marketing quanto per i security manager.
Il beneficio forse più importante di questa integrazione è la possibilità di ottimizzare i costi, sia dal punto di vista della riduzione delle perdite sia di gestione del budget. Tradizionalmente, infatti, marketing e security sono due funzioni che dispongono di budget indipendenti e di entità diversa: speso le risorse economiche a disposizione del marketing sono maggiori rispetto a quelle stanziate per attività di sicurezza e loss prevention. Senza contare che i ruoli svolti sono apparentemente slegati tra loro e necessitano di informazioni diverse. La funzione marketing sarà interessata ai dati relativi ai clienti, dal loro numero, età e genere al tempo di permanenza in negozio, per ideare strategie di vendita adatte ad ogni situazione. La security è invece rivolta al mantenimento della safety e alla loss prevention, e necessiterà di informazioni in tempo reale su aspetti come la viabilità delle uscite di emergenza o la segnalazione di comportamenti sospetti. Le soluzioni di Axis permettono di utilizzare un unico sistema integrato in grado di raccogliere e trasferire le informazioni di cui hanno bisogno entrambe le funzioni trasferendole ai rispettivi responsabili e facilitando la loro collaborazione per uno store management sempre più smart.

Retail, l'apporto della ricerca universitaria sulle potenzialità della Store Sonification

intervista a Kjetil Falkenberg Hansen (*) - KTH Royal Institute of Technology - Stoccolma

Quali sono i contenuti della tua ricerca sugli effetti dei suoni sul comportamento delle persone?
In precedenza ho lavorato sui cambiamenti comportamentali dei bambini con disabilità cognitive. Questa ricerca era focalizzata sugli effetti del suono attivo anziché dell'ascolto passivo. Abbiamo realizzato anche altre ricerche nella stessa area, valutando i cambiamenti di umore quando ci impegniamo in attività musicali. E' stato osservato che la produzione attiva di suoni comporta una maggiore attenzione da parte dei soggetti monitorati e per un periodo più lungo. È tuttavia difficile interpretare i risultati perchè potrebbero essere condizionati da un "effetto novità" nella maggior parte dei partecipanti alla ricerca. Altri studi sul cambiamento comportamentale sono comuni nella psicologia della musica, in particolare sugli aspetti emotivi nella comunicazione non verbale. È molto interessante vedere come le manipolazioni musicali che catturano l'attenzione in una situazione di ascolto passivo alterino l'umore e modifichino i comportamenti. C'è motivo di credere che, in generale, le persone rispondano in modo simile alle medesime alterazioni di un segnale musicale ma, allo stato attuale, gli studi su questi effetti in un contesto di vita reale non sono ancora attendibili.

Si può pensare ad applicazioni nel settore del Retail finalizzate al miglioramento della customer experience ed eventualmente a nuove forme di prevenzione delle perdite?
Riteniamo che ci sia un potenziale sottoutilizzato nella progettazione del suono per informare i clienti e il personale sugli eventi del negozio. Negli ultimi due decenni, le aree di ricerca di sonificazione e display uditivi sono state affrontate da diverse angolazioni e con molte implementazioni di successo. Alcune di queste includono la sonificazione nello sport e nell'assistenza sanitaria con il monitoraggio dei dati.

Sottolineando che l'uso della sonificazione allo scopo di modificare il "sistema" di un negozio è un approccio nuovo e ci sono ancora molte sfide irrisolte, si deve tuttavia riconoscere che esiste già una solida base di conoscenze su cui lavorare, con una ragionevole certezza che si otterranno buoni risultati. Uno dei primi aspetti che ci aspettiamo di ottenere riguarda i miglioramenti nella percezione dell'atmosfera del negozio, rendendo così la customer experience più gradevole. L'uso della musica di sottofondo per divulgare anche informazioni di avviso di eventi potrebbe risultare meno invadente per tutti. In secondo luogo, un sistema di allerta sottile ma efficace avrà un effetto preventivo sui clienti con l'impulso di rubare. Da non trascurare, infine, che un efficace sistema di allerta diminuirà il carico cognitivo del personale del negozio che potrà così concentrarsi su ciò che conta, compresa l'osservazione del comportamento dei clienti.

**Kjetil Falkenberg Hansen lavora come assistente professore nel gruppo di Computer Sound and Music presso il KTH Royal Institute of Technology di Stoccolma. I suoi interessi di ricerca sono il suono e la musica per la riabilitazione e la salute, nuovi strumenti musicali espressivi e nuove interfacce per il sound design. Ha scritto il suo dottorato di ricerca su "DJ come musicisti" nel 2010.*

Le soluzioni audio di AXIS un'integrazione a 360°

a cura di Pietro Tonussi - Business Development Manager Sud Europa di AXIS Communications

L'integrazione delle analitiche audio nei sistemi di sorveglianza è una realtà sempre più diffusa, resa possibile dallo sviluppo di soluzioni scalabili come quelle di Axis. Le potenzialità di questo utilizzo congiunto sono numerose, grazie soprattutto all'influenza che i suoni possono esercitare sulle azioni delle persone.

La diffusione in negozio di una musica adatta all'ambiente, ad esempio, può incrementare la propensione all'acquisto. L'importanza dell'audio in ambito retail è emersa anche dalla ricerca "Il Negozio del Futuro in Italia", che Axis ha commissionato a IPSOS in merito all'esperienza d'acquisto degli italiani nei punti vendita fisici. Il 75% degli intervistati ritiene, infatti, che la musica possa migliorare l'esperienza in negozio.

Il tema è stato anche oggetto del workshop "Store sonification: una strada non intrusiva per la sicurezza dei negozi e la shopping experience", organizzato da Axis durante Forum Retail per approfondire il duplice ruolo dell'audio nel retail: miglioramento della customer experience e potenziamento della sicurezza del negozio. Gli ambiti di applicazione delle soluzioni Axis che integrano sistemi audio e video sono molti e destinati a crescere con l'evoluzione delle rispettive tecnologie.

Banking

Il timore maggiore delle persone nel momento in cui si trovano davanti ad uno sportello bancomat è che qualcuno possa sbirciare alle loro spalle per scoprire il PIN delle loro carte. Si tratta della pratica diffusa dello shouldering che gli istituti bancari si sforzano da sempre di contrastare. A questo scopo, alcune banche hanno iniziato a installare telecamere dotate di software di motion detection che rilevano quando qualcuno si avvicina troppo, e troppo a lungo, al cliente che sta effettuando il prelievo. L'analitica audio integrata attiva automaticamente una registrazione vocale, diffusa tramite altoparlante, che invita a rispettare la distanza minima di sicurezza. In questo modo eventuali malintenzionati possono rendersi conto di essere osservati e, in caso di mancato rispetto del messaggio, la sala di controllo può usare un microfono per replicare il messaggio in tempo reale.

Industrial

Molti stabilimenti industriali hanno fatto dell'integrazione tra audio e video una risorsa fondamentale per la tutela tanto degli asset quanto del personale. La protezione perimetrale e il controllo degli accessi sono resi più efficaci dalla presenza di altoparlanti connessi: collocati in corrispondenza delle uscite di locali con accesso limitato, sono in grado di emettere un suono quando la porta viene aperta e attivare così il sensore connesso, che invierà un alert visivo agli addetti per verificare la situazione e l'identità di chi sta varcando quella soglia. Nel caso si tratti di una persona non autorizzata, sarà possibile sfruttare gli altoparlanti per diffondere messaggi, preregistrati o in tempo reale, come deterrente. I sistemi audio contribuiscono anche ad agevolare le operazioni di manutenzione negli stabilimenti industriali: i tecnici nelle sale di controllo possono infatti monitorare l'andamento dei lavori e comunicare con il personale all'opera, riducendo notevolmente i tempi. Infine, l'audio può segnalare efficacemente se le uscite della struttura, soprattutto quelle di emergenza, sono ostruite, attivando un messaggio preregistrato o permettendo la diffusione di avvisi in diretta, una funzione vitale nel caso di eventuali evacuazioni.

Infrastrutture critiche

Nelle infrastrutture critiche è fondamentale impedire l'accesso di persone non autorizzate o, peggio, malintenzionate. Bisogna, inoltre, garantire una protezione su tre livelli: proteggere la proprietà, mantenere efficienti i processi che vi si svolgono e garantire la sicurezza del personale che vi opera. Le possibilità di integrazione offerte da Axis consentono di raggiungere questi tre obiettivi con un'unica soluzione. Accanto all'impiego, ormai comune, di dispositivi per la videosorveglianza sul terreno e sulle reti perimetrali, i sistemi audio si stanno affermando come ulteriore livello di protezione per rilevare gli accessi non autorizzati e avvertire i trasgressori dell'avvenuta individuazione, fungendo da deterrente. Hanno un ruolo importante anche nella tutela del personale: le infrastrutture critiche sono ambienti potenzialmente pericolosi per la presenza di fili ad alta tensione o prodotti chimici combustibili e le analitiche audio possono attivare avvisi quando le persone vengono rilevate in aree poco sicure o vietate, ad esempio gallerie, binari e ferrovie.

Carceri e istituti di correzione

I sistemi audio possono risultare cruciali nel mantenimento della sicurezza all'interno delle strutture di detenzione. Essendo basate su IP, possono integrarsi facilmente con gli altri strumenti di rete, come le telecamere Axis, permettendo di cogliere tempestivamente situazioni che potrebbero rivelarsi pericolose. Le analitiche audio sono infatti in grado di rilevare determinati pattern sonori, ad esempio associati con la coercizione, la rabbia o la paura e stabiliti in precedenza, come una persona che urla, e possono generare un segnale di allerta che raggiunge sia il centro di controllo sia gli smartphone degli agenti in servizio. L'allarme così trasmesso indica la zona della struttura in cui è stato rilevato il disturbo e, tramite le telecamere, consente di verificare efficacemente la causa dell'agitazione e se è necessario un intervento.

Healthcare

Nel settore sanitario possono verificarsi numerose situazioni critiche: improvvisi peggioramenti nelle condizioni dei pazienti, furti di medicinali, tensioni nelle sale d'attesa e atti di violenza nei confronti del personale, soprattutto in strutture più sensibili, sono soltanto alcuni esempi. Con un sistema di videosorveglianza che integri le analitiche audio è tuttavia possibile individuare e segnalare queste eventualità. Ma le possibilità del suono in questo contesto non sono limitate alla sicurezza: diffondere musica di sottofondo contribuisce sia a rendere più confortevole e umano l'ambiente ospedaliero sia ad aumentare la privacy, coprendo i discorsi tra dottore e paziente o tra paziente e famigliare. Infine, un sistema audio e video di alta qualità permette di registrare procedure mediche e simulazioni, ma anche di condividere dimostrazioni in tempo reale durante conferenze e condividere così conoscenze con altri ospedali e comunità di ricercatori.

Contatti:
Axis Communications
Tel. +39 02 8424 5762
www.axis.com

Digital Transformation, PSIM, ERP: i 3 focal point di Citel nel 2020

di Nils Fredrik Fazzini, CEO di Citel spa

L'informatizzazione è una forma di evoluzione delle attività umane consolidata e diffusa in ogni ambito e ad ogni livello della società attuale, che si è propagata senza sosta nel corso di una storia di ormai mezzo secolo, a partire dai sistemi gestionali per le grandi organizzazioni fino alle micro-attività nella sfera personale.
Quella che invece è in corso solo da pochi anni è l'evoluzione delle tecnologie digitali stesse, battezzata come ***Digital Transformation***. Un termine che non va tradotto (come capita spesso) in digitalizzazione (che è la tecnologia di base dell'informatica), perché in realtà vuol dire *trasformazione del mondo digitale* in sé, un mondo di tecnologia concepita originariamente per addetti ai lavori specializzati e che viene ora progressivamente sostituito da nuove piattaforme, più intelligenti, più economiche e, soprattutto, più ergonomiche ed intuitive per utilizzatori non esperti di informatica.
La Digital Transformation permette quindi di diffondere applicazioni informatiche sempre più utili e gestibili anche da persone prive di cultura informatica professionale, con la propagazione verso ogni tipologia di utente, tipicamente a bordo della telefonia mobile della generazione attuale in quanto piattaforma informatica portatile.
È quindi naturale che oggi la *Digital Transformation* con i suoi 6 pilastri tenda a trasformare anche il mondo della sicurezza fisica, non solo riguardo alle tecniche di interazione tra uomo e sistema ma anche – e in misura crescente – riguardo al contributo di esperienza intelligente dei processi di gestione degli eventi e, soprattutto, delle *situazioni*.

I due Convegni di Citel sulla Digital Transformation
La *Digital Transformation* della gestione della sicurezza fisica è oggetto di progettazione e sperimentazione già da tempo nel laboratorio di Citel e presso i suoi utenti, ed è stata illustrata nel corso del 2019 con due Convegni, organizzati in collaborazione con essecome-securindex, a valle del consolidamento e dell'annuncio di nuove specifiche funzioni.
Il primo rivolto agli utenti finali di grandi e medie dimensioni dotati di un SOC (Security Operation Centre) aziendale, il secondo ai fornitori di servizi in classe PSIM da Control Room, ovvero agli Istituti di Vigilanza, in particolare a quelli orientati ai moderni tele-servizi di security informatizzata secondo criteri di apertura architetturale e di integrazione multifunzionale e multimediale.
Il fatto di riempire delle grandi sale convegni in due occasioni consecutive a distanza di pochi mesi, è stata una chiara conferma dell'interesse attuale per le innovazioni tecnico-funzionali in corso nel settore della sicurezza fisica informatizzata, indipendentemente dal fatto che il PSIM si configuri come sistema dipartimentale interno, oppure che si tratti di una soluzione *as-a-service*.
D'altra parte, si tratta di un argomento che tocca tendenze di fondo in una fase di transizione di natura epocale riguardante il tema della sicurezza, che tende ad investire ogni settore della società attuale, fortunatamente con un comparto nazionale particolarmente dinamico e innovativo riguardo al tema, grazie alla predominanza di sistemi aperti multifornitore per la gestione dipartimentale della sicurezza fisica in chiave open-PSIM secondo linee di fondo adottate da sempre da Citel.

ERPsim, il paradigma che coniuga PSIM e il suo ERP
ERPsim è il *nickname* coniato da Citel per definire un modello di PSIM con un Ecosistema di utenti e fornitori complementari organizzato sul principio del ERP gestionale. L'Ecosistema di Centrax, il PSIM di Citel, è un caso unico nel mercato della sicurezza fisica: comprende comunità di utenti, di Terze parti di servizio, di produttori complementari, con numeri e nomi importanti ed una tradizione di interoperabilità aperta multifornitore iniziata 25 anni fa secondo criteri collaborativi che, nel tempo, si sono consolidati con l'adesione di un numero crescente di sostenitori delle architetture aperte e delle attività di servizio non vincolate alla marca.
L'adozione del modello ERPsim mette l'utente PSIM al centro di un Ecosistema con l'abilitazione a fare libere scelte accedendo a soluzioni, prodotti e servizi complementari, supportati o integrati da Citel, ma alimentati e filtrati dalla selezione naturale operata dall'utenza PSIM nell'ambito delle comunità degli utilizzatori e delle Terze Parti di servizio. Quella dell'ERP come formula organizzativa dell'Ecosistema di Centrax open-PSIM di Citel non è altro che la formalizzazione strutturata di un contesto che, di fatto, è operativo da anni, con un numero significativo di Utenti e di Terze Parti che, nel corso del tempo, hanno contribuito di fatto all'evoluzione delle tecnologie ed all'affinamento dei processi gestionali di Centrax e del suo corollario di applicazioni complementari.

La Digital Transformation: PSIM e Situation Management
Con il PSIM siamo nel terreno dei sistemi informatici dipartimentali, utilizzati professionalmente e, quindi, suscettibili di beneficiare naturalmente di ogni innovazione riferibile alla *Digital Transformation* che, nella fattispecie, è coinvolta soprattutto riguardo ai pilastri dell'***Edge Computing*** e del ***System of Engagement*** cui appartengono le specializzazioni riferibili all'interazione tra dispositivi periferici ed all'analisi intelligente dei comportamenti.
Tecnologie attualmente implementate nella versione ***Centrax SM – Situation Manager*** che Citel ha messo al centro di un cambio di paradigma, con il passaggio dalla gestione dell'evento alla *gestione della situazione*.
Un cambio di paradigma accelerato dai massicci interventi evolutivi richiesti negli ultimi anni dal settore bancario, che hanno portato all'azzeramento degli eventi rapina tra le banche utenti di Citel.
Si è trattato di un caso eclatante sul piano del risultato ma, anche, di un esempio virtuoso di sinergia tra utente e progettista e di collaborazione tra produttori diversi visto che Citel, in quanto progettista e produttore, integrava in questo caso più marche e tecnologie nel campo degli erogatori di banconote, delle bussole, degli apparati multimediali, dei sistemi informatici.
Un caso di scuola per il settore della sicurezza fisica informatizzata, che conferma e mette a fuoco l'importanza decisiva di una struttura da vera e propria ***System & Software House*** specializzata nel settore specifico del PSIM inteso come progetto permanente di un Sistema Informatico dipartimentale della sicurezza basato sull'integrazione multifornitore; e quindi al centro di un Ecosistema di utenti evoluti, costruttori complementari collaborativi e fornitori di servizi qualificati.

CITEL

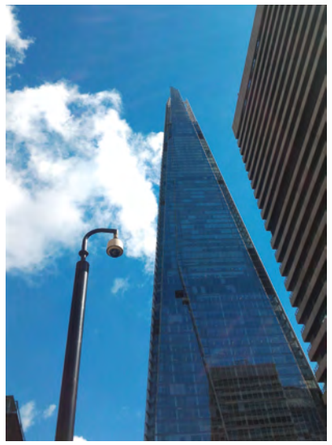
Contatti:
Citel spa
info@citel.it
www.citel.it

Videosorveglianza in cloud, un obbligo per le P.A.?

di Angelo Carpani (*)

1. INTRODUZIONE

Nella mia attività professionale, nella quale mi occupo quasi esclusivamente di progettazione di impianti di videosorveglianza in ambito comunale, mi sono imbattuto di recente per la prima volta in un Comune il quale, nel proprio "Piano triennale per l'informatica" (dopo vedremo di cosa si tratta), ha stabilito di non ricorrere più all'adozione di server "fisici" per la gestione e l'archiviazione dei dati ritenendo di ottenere notevoli risparmi in termini di hardware, energia consumata, manutenzione, ecc. senza la necessità di avere locali idonei ed annullando qualsiasi generazione di rumore e di calore.



Si tratta di un passaggio importante e che può contrassegnare l'inizio di una vera e propria ***rivoluzione*** nell'ambito delle Pubbliche Amministrazioni che sceglieranno i servizi Cloud, sia per infrastrutture che per quanto riguarda le soluzioni software e le piattaforme.

Senza la pretesa di trattare in modo esaustivo l'argomento, vediamo di cosa si tratta, sia da un punto di vista legislativo che tecnico, anche perché sul sito web dell'**AgID** (**A**genzia per l'Italia **D**igitale) si trovano molte informazioni al riguardo.

2. L'AGID ED IL PIANO TRIENNALE PER L'INFORMATICA NELLA PUBBLICA AMMINISTRAZIONE 2019 -2021

L'Agenzia per l'Italia Digitale (AgiD) è un'agenzia tecnica che fa capo alla Presidenza del Consiglio, che ha il compito di garantire la realizzazione degli obiettivi dell'Agenda digitale italiana e contribuire alla diffusione dell'utilizzo delle tecnologie dell'informazione e della comunicazione, favorendo l'innovazione e la crescita economica. AgID ha il compito di coordinare le amministrazioni nel percorso di attuazione del **Piano Triennale per l'informatica della Pubblica Amministrazione**, favorendo la trasformazione digitale del Paese.

La **strategia Cloud della PA** nasce per favorire l'adozione del modello del *cloud computing* nelle pubbliche amministrazioni italiane, in linea con le indicazioni della Strategia per la Crescita digitale del Paese e con le previsioni del Piano Triennale per l'Informatica nella Pubblica Amministrazione 2019 - 2021, e per qualificare servizi e infrastrutture cloud secondo specifici parametri di sicurezza e affidabilità idonei per le esigenze della PA.

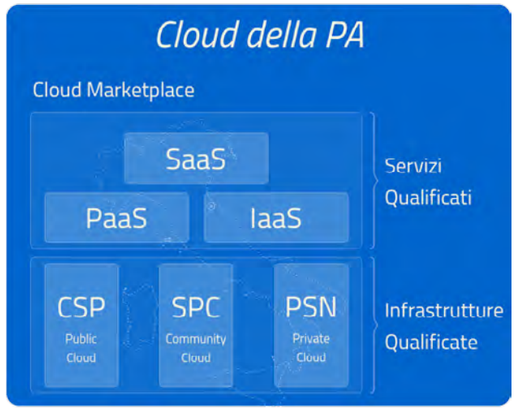
La strategia cloud delineata da AGID prevede un percorso di qualificazione per i soggetti pubblici e privati che intendono fornire infrastrutture e servizi Cloud alla Pubblica Amministrazione, affinchè queste ultime possano adottare servizi e infrastrutture di cloud computing omogenei, che rispettino elevati standard di sicurezza, efficienza ed affidabilità.

A decorrere dal 1° aprile 2019, le Amministrazioni Pubbliche (PA) possono acquisire esclusivamente servizi cloud qualificati da AgID e pubblicati nel **Cloud Marketplace** (il catalogo dei servizi cloud qualificati).

(*) Angelo Carpani, libero professionista, laureato in Ingegneria elettronica presso il Politecnico di Milano, iscritto all'Ordine degli Ingegneri della Provincia di Como (n. 2368 sez.A), esperto nella progettazione di impianti di videosorveglianza in ambito comunale.

3. IL MODELLO CLOUD DELLA PA

Al fine di incrementare l'adozione del cloud nella PA, il **Piano Triennale per l'informatica nella Pubblica Amministrazione 2017 - 2019** ha introdotto il **Modello Cloud della PA** che descrive l'insieme di infrastrutture IT e servizi cloud qualificati da AGID a disposizione della PA, secondo una strategia che prevede la realizzazione di tale modello, la definizione e attuazione del programma nazionale di abilitazione al Cloud della PA e l'applicazione del *principio* ***cloud first***.



Come illustrato nella figura, il Modello Cloud della PA è composto da:

- **Servizi Qualificati** da AgID consultabili mediante il *Cloud Marketplace* suddivisi in ***IaaS*** *(**I**nfrastructure **a**s **a** **S**ervice),* ***PaaS*** *(**P**latform **a**s **a** **S**ervice) e* ***SaaS*** *(**S**oftware **a**s **a** **S**ervice).*
- **Infrastrutture Qualificate** da AgID quali i ***C**loud **S**ervice **P**rovider (CSP)*, i ***P**oli **S**trategici **N**azionali (PSN)* e l'infrastruttura di *Community Cloud*.

3.1 I Servizi Qualificati

IaaS, SaaS e PaaS possono essere considerati gli elementi centrali dell'informatica moderna, non più legata esclusivamente a macchine fisiche e a logiche "on premise", ovvero di server e apparecchiature possedute e controllate privatamente, ma che sempre più trova il suo sviluppo nel *cloud computing* tradizionale, fatto di **infrastrutture** IT controllate da provider di servizi esterni che mettono a disposizione risorse di elaborazione in funzione delle necessità.

Qual è quindi la differenza tra servizi cloud IaaS, PaaS e SaaS?

SaaS (Software as a Service)

Per *Software as a Service* si intendono quelle applicazioni **Software** accessibili tramite Internet sfruttando diverse tipologie di dispositivi (Desktop, Mobile, etc). La facoltà fornita al consumatore è quindi quella di utilizzare le applicazioni del fornitore funzionanti su un'infrastruttura cloud. Le applicazioni sono accessibili da diversi dispositivi attraverso un'interfaccia leggera come, ad esempio, un'applicazione email su browser, oppure da programmi dotati di apposita interfaccia. L'obiettivo del **cloud Saas** è quindi quello di fornire agli utenti, siano essi *consumer o business*, un'applicazione accessibile ovunque sia disponibile una connessione a Internet. Il software e i dati risiedono su cluster di server che erogano il servizio senza la necessità di memorizzare i dati in locale sulla macchina.

IaaS (Infrastructure as a Service)

Per I*nfrastructure as a Service* si intendono quelle **Infrastrutture** tecnologiche fisiche e virtuali in grado di fornire risorse di computing, networking e storage da remoto e mediante API (Application Programming Interface). La facoltà fornita al consumatore è quindi quella di acquisire elaborazione, memoria, rete e altre risorse fondamentali di calcolo, inclusi sistemi operativi e applicazioni. Chi si affida a un servizio **cloud IaaS** non ha quindi più alcuna necessità di possedere le macchine e manutenerle: è il provider di servizi, infatti, a mettere a disposizione delle risorse computazionali sotto forma di **macchine virtuali** affittate in base alle singole esigenze e sulle quali possono essere installati sistemi operativi e software esattamente come su un'infrastruttura proprietaria, con l'enorme vantaggio di non doversi più preoccupare di alcun aspetto legato al possesso fisico di un parco macchine.

PaaS (Platform as a Service)
Per *Platform as a Service* si intendono le **Piattaforme** per sviluppare, testare e distribuire le applicazioni su internet. La facoltà fornita al consumatore è quindi quella di distribuire sull'infrastruttura *cloud* applicazioni create in proprio oppure acquisite da terzi, utilizzando linguaggi di programmazione, librerie, servizi e strumenti supportati dal fornitore. Il **cloud PaaS** offre quindi tutti gli strumenti necessari per la creazione, lo sviluppo e la distribuzione delle applicazioni senza la necessità di disporre di un'infrastruttura fisica né di dover installare sistemi operativi o ambienti di sviluppo, lasciando così piena libertà di sviluppo all'interno delle caratteristiche offerte dalla piattaforma.

3.2 Le Infrastrutture Qualificate

Il fornitore di servizi cloud – Cloud Service Provider (CSP)
I Cloud service provider (CSP) sono i fornitori di servizi cloud qualificati da AGID, che possono erogare servizi di tipo **Public Cloud** alle amministrazioni. Le qualificazioni AGID assicurano che le infrastrutture e i servizi dei CSP siano sviluppati ed operanti secondo criteri minimi di affidabilità e sicurezza considerati necessari per i servizi digitali della PA.

Il Sistema Pubblico di Connettività (SPC)
E' un insieme di infrastrutture tecnologiche e di regole tecniche che ha lo scopo di "federare" le infrastrutture ICT delle Pubbliche amministrazioni al fine di realizzare servizi integrati mediante regole e servizi condivisi. Tale integrazione permette di risparmiare sui costi e sui tempi e di realizzare i servizi finali centrati sull'utente, evitando richieste continue di dati da parte delle amministrazioni, oltre che duplicazioni di informazioni e controlli.

I Poli Strategici Nazionali (PSN)
Per **PSN** si intende il soggetto titolare dell'insieme di infrastrutture IT (centralizzate o distribuite), ad alta disponibilità, di proprietà pubblica, eletto a Polo Strategico Nazionale dalla Presidenza del Consiglio dei Ministri e qualificato da AgID ad erogare, in maniera continuativa e sistematica, ad altre amministrazioni:

- servizi infrastrutturali on-demand (es. housing, hosting, IaaS, PaaS, SaaS, ecc.);
- servizi di disaster recovery e business continuity;
- servizi di gestione della sicurezza IT;
- servizi di assistenza ai fruitori dei servizi erogati.

Presso i PSN dovranno essere presenti e gestite le principali infrastrutture ICT (hardware, software, connettività) messe a disposizione delle altre amministrazioni, senza vincoli rispetto alla localizzazione sul territorio nazionale.

4. La videosorveglianza e il principio del "cloud first"
Veniamo allora alla fatidica domanda: l**a videosorveglianza in cloud è un obbligo per le PA?**
Il nuovo Piano triennale per l'informatica nella pubblica amministrazione (2019-2021) prevede l'applicazione del **principio "cloud first"**: "Le pubbliche amministrazioni, in fase di definizione di un nuovo progetto, e/o di sviluppo di nuovi servizi, in via prioritaria devono valutare l'adozione del paradigma cloud prima di qualsiasi altra tecnologia, tenendo conto della necessità di prevenire il rischio di *lock-in*[1]. Dovranno altresì valutare il ricorso al cloud di tipo pubblico, privato o ibrido in relazione alla natura dei dati trattati e ai relativi requisiti di confidenzialità".

1 Rischio di dipendenza esclusiva dal fornitore

Sulla base tale principio, questo non significa che l'impiego di server o NVR in loco, nelle applicazioni di videosorveglianza, siano vietati, ma che l'impiego del cloud deve essere prioritariamente valutato. Solo qualora il *"cloud first"* non soddisfi i criteri enunciati, si possono sempre utilizzare i sistemi tradizionali, anche con nuovi acquisti che, però, debbono essere adeguatamente giustificati (la mancata giustificazione può essere elemento di responsabilità contabile).
Il termine del 1° aprile, infatti, si riferisce solo agli acquisti dei servizi cloud, che debbono essere obbligatoriamente qualificati da AgID, e non ai casi, residui, nei quali si sia proceduto alla valutazione del *cloud first*" con esito negativo.

4. Criticità del cloud computing per la videosorveglianza

Il cloud, nell'ambito della trasformazione digitale, rappresenta una delle tecnologie cosiddette *disruptive*[2], che comporta notevoli vantaggi in termini di incremento di affidabilità dei sistemi, qualità dei servizi erogati, risparmi di spesa realizzabili attraverso l'opportunità della migrazione dei servizi esistenti verso il cloud e la possibilità di pagare soltanto gli effettivi consumi in cui, all'atto pratico, il Cliente paga solo ciò che usa *(pay-per-use)* e gli unici costi da sostenere dipendono dallo spazio utilizzato *(storage)* e dal traffico in uscita *(connettività richiesta)*. Le tecnologie Cloud, oltre alla flessibilità, dispongono di una potenza di calcolo e risorse irraggiungibili dalle solite infrastrutture *on-premise*, mettendo in sicurezza le informazioni più importanti, secondo uno schema di salvataggio e ripristino tipico delle infrastrutture di *Disaster Recovery*[3].

Tuttavia, nella realizzazione di impianti di videosorveglianza in cloud, soprattutto in ambito cittadino, per via della presenza di numerose telecamere impiegate, per di più a risoluzione sempre più elevata (ad es. Ultra HD – 4K), vanno tenute in conto alcune criticità.

La **prima criticità** è legata al *networking* e all'internet service provider (ISP) utilizzato per l'accesso al cloud provider; il numero delle telecamere che possono essere collegate dipende dal tipo di connessione (es. fibra, adsl, ecc.) e anche sfruttando l'algoritmo di compressione H.265 (ad es. per le telecamere 4K) il numero delle stesse che possono essere collegate è sicuramente non elevato e dipende comunque dalle prestazioni e dalla qualità della connessione.

La **seconda criticità** riguarda lo *storage*. Anche se attualmente le memorie hanno un trend di costo per Terabyte continuamente in calo, lo storage richiesto è molto elevato in quanto, in base alla ***Direttiva del Ministero dell'Interno n.558/SICP ART/421.2/70 del 2 marzo 2012***, avente per oggetto i *Sistemi di videosorveglianza in ambito comunale*, i sistemi di videosorveglianza dovranno rispettare in ogni caso i requisiti di seguito riportati:

- capacità di banda necessaria al trasferimento delle immagini in funzione delle caratteristiche delle telecamere e della tecnologia della rete di trasporto;
- la memorizzazione delle immagini provenienti da tutte le telecamere al massimo frame rate possibile;

2 Il concetto di "disruptive technology" è stato introdotto per la prima volta da un articolo di Christensen ed altri, pubblicato su Harvard Business Review, nel 1995. Secondo gli autori "disruption" descrive un processo per cui un'impresa più piccola e con meno risorse è in grado di sfidare con successo le imprese dominanti un certo settore. Le imprese dominanti nel concentrarsi su come migliorare i propri prodotti e servizi per i clienti più esigenti (e di solito più redditizi), eccedono le esigenze di alcuni segmenti e ignorano i bisogni degli altri. I nuovi entranti, con intenti "disruptive", iniziano a soddisfare con successo quei segmenti trascurati e si ritagliano una posizione fornendo le funzionalità richieste dai segmenti ignorati dai dominanti, spesso a un prezzo inferiore. Le imprese dominanti, a caccia di una maggiore redditività nei segmenti più esigenti, non rispondono in maniera adeguata a questo attacco. I nuovi entranti quindi evolvono per soddisfare segmenti più elevati del mercato, offrendo le prestazioni che i clienti principali delle imprese dominanti richiedono, pur mantenendo i vantaggi che hanno determinato il loro primo successo. Quando i clienti tradizionali iniziano ad abbandonare le imprese dominanti per adottare in volumi le soluzioni offerte dai nuovi entranti, avviene la "disruption".

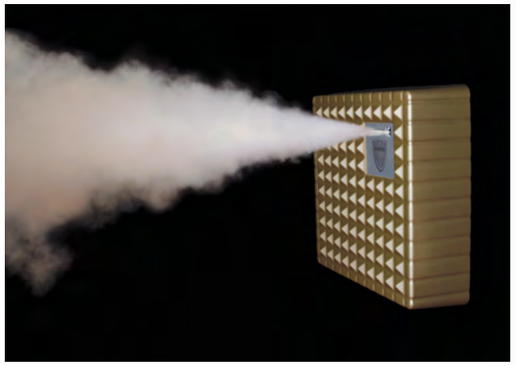
3 Con "disaster recovery" (in italiano: Recupero dal Disastro), in informatica ed in particolare nell'ambito della sicurezza informatica, si intende l'insieme delle misure tecnologiche e logistico/organizzative atte a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi di business per imprese, associazioni o enti, a fronte di gravi emergenze che ne intacchino la regolare attività.

- la registrazione delle immagini deve avvenire in forma cifrata, in accordo a quanto richiesto al paragrafo 3.3.1 comma t del "Provvedimento in materia di videosorveglianza" dell'8 Aprile 2010 del Garante per la Privacy (utilizzo di reti pubbliche e connessioni wireless), per garantirne la riservatezza e l'integrità;
- la capacità di storage deve essere dimensionata per la registrazione contemporanea di tutte le telecamere al massimo frame rate consentito dalle stesse e/o dalla connettività per un periodo di almeno 7 gg 24h.

La **terza criticità** riguarda l'aspetto regolatorio e le norme che i sistemi di videosorveglianza sono tenuti ad osservare, in particolare quelli legati alla *sicurezza* dei dati e alla *privacy* (GDPR). Usufruire di un servizio di cloud storage per la memorizzazione dei dati, in particolare per quelli personali o sensibili, può esporre il cliente a potenziali problemi di violazione della privacy: infatti i dati personali del cliente o delle immagini registrate dal sistema cliente vengono di fatto affidate ad un soggetto terzo con tutte le implicazioni del caso. In ottica **privacy e GDPR**, il provider deve rispondere in modo trasparente e prevedere che tutti i dati memorizzati rimangano di proprietà esclusiva del cliente. Stante questa logica, eventuali attività di accesso, condivisione, modifica e trasferimento devono essere ad esclusivo appannaggio del cliente stesso.

Defendertech presenta il nebbiogeno DT-200 “TURBO”

a cura della Redazione



Il nebbiogeno DT-200 “TURBO” è la novità presentata da Defendertech in occasione della Fiera SICUREZZA 2019 che può coprire 75 metri cubi in 30”, fino a 200 metri cubi con l’espansione totale della nebbia ad ogni erogazione. Certamente accattivante per le ridotte e gradevoli dimensioni con un rapporto qualità/prezzo competitivo, il nebbiogeno DT-200 lavora con glicole alimentare e acqua demineralizzata. Queste le sue caratteristiche:

- ugello prolungabile per installazioni nascoste fino a 50cm (front o back), senza perdere potenza nell’erogazione. E’ l’unica proposta nel mercato;
- serbatoio ricaricabile manualmente ed in maniera autonoma, avendo sempre la certezza del livello di liquido presente nel serbatoio;
- massima flessibità per l’integrazione con sistemi di allarme, 2 ingressi (arm/disarm), 5 uscite (preallarme livello liquido, guasto generale, monitoraggio batteria, segnalazione stato arm/disarm, monitoraggio temperatura caldaia);
- consumo elettrico solo quando è armato;
- bruciatore garantito 5 anni. Temperatura di funzionamento superiore rispetto alla concorrenza, quindi con maggiore densità e persistenza della nebbia;
- diverse protezioni sul funzionamento accidentale;
- conformità EN50131-8. Il liquido e la nebbia non sono infiammabili e sono certificati dal Centro Nazionale Antiveleni di Pavia. Il serbatoio non potrà mai detonare.

NEBBIOGENO
SECURITY FOG SYSTEM
www.defendertech.eu

Contatti:
Tek Group Srl
Tel. +39 0721 1626113
www.defendertech.eu

Hanwha Techwin presenta telecamere termiche QVGA Wisenet

a cura della Redazione

Hanwha Techwin è ora in grado di offrire una gamma ancora più ampia di telecamere, grazie all’introduzione di 3 nuovi modelli termici con risoluzione QVGA.
A differenza delle telecamere tradizionali, la cui efficacia dipende anche dal livello luminoso e da disturbi atmosferici, le telecamere termiche acquisiscono le tracce termiche degli oggetti e non sono influenzate dalle condizioni estreme, come buio totale, clima rigido, luci intense, nebbia e fumo. Inoltre, offrono una soluzione efficace per le applicazioni in cui si teme la presenza di inquinamento luminoso.

Funzionalità principali
Le tre nuove termocamere antivandalo, parte della serie **Wisenet T**, sono in grado di acquisire immagini con una risoluzione fino a 320 x 240.
Come per tutte le telecamere della serie Wisenet T di ultima generazione, le nuove termocamere **QVGA TNO-3010T, TNO-3020T e TNO-3030T** sono dotate della funzione di analisi audio che riconosce suoni critici come spari, esplosioni, urla e vetri rotti, oltre a funzionalità di analisi video avanzata. Altre caratteristiche comprendono diverse abilità di rilevamento, come cambiamento di temperatura, urti, direzione di oggetti/persone, stazionamento e manomissione.
I sensori giroscopici integrati garantiscono inoltre una correzione più accurata dei disturbi in caso di vibrazioni, fornendo immagini più stabili quando la telecamera è disturbata da vento o vibrazioni.
Tra le altre funzionalità incluse come standard troviamo anche audio bidirezionale, rilevamento dei movimenti e handover, così come la capacità di memorizzare fino a 256 GB di dati su una scheda SD/SDHC/SDXC per poter registrare automaticamente a bordo camera in caso di interruzione della rete.

Queste telecamere offrono la possibilità di scegliere tra compressione H.265, H.264 e MJPEG e sono dotate di **WiseStream II**, una tecnologia di compressione complementare che controlla dinamicamente la codifica dei dati, bilanciando qualità e livello di compressione in base alla quantità di movimento presente nella ripresa. Quando WiseStream II viene combinata alla compressione H.265, infatti, le risorse di rete possono essere utilizzate in maniera fino al 99% più efficiente rispetto all’attuale tecnologia H.264.

Le tre nuove termocamere QVGA Wisenet sono:
• Wisenet TNO-3010T: Obiettivo fisso da 2,7 mm Distanza min. ripresa oggetti: 0,3 m
• Wisenet TNO-3020T: Obiettivo fisso da 4,7 mm Distanza min. ripresa oggetti: 1 m
• Wisenet TNO-3030T: Obiettivo fisso da 13,7 mm Distanza min. ripresa oggetti: 8 m

Hanwha Techwin Europe

Contatti:
Hanwha Techwin Europe LTD
Tel. +39 02 36572 890
www.hanwha-security.eu/it

Travel Risk Management

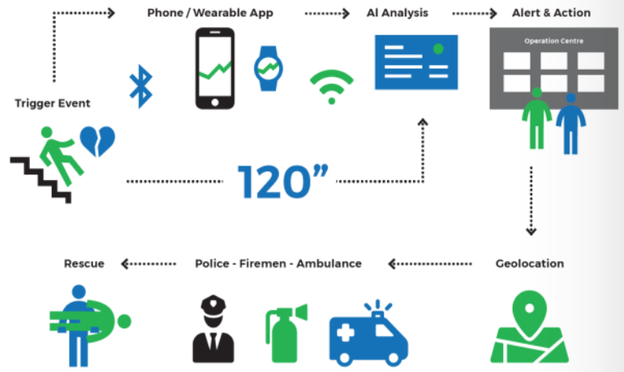
UMBRELLA GROUP
SECURITY & LOGISTIC

Per la Safety e la Security dei tuoi Asset ovunque nel mondo

Soluzioni tecnologiche

Dashboard
Travel Risk Management

Country Risk Assessment
Travel Alerts & Travel News
Pre-Travel Advisory
Personal Safety Report
Vital Signs Monitoring



Centrale Operativa: coordinamento e supporto da remoto H24 365 gg/anno

Umbrella Group Ltd.
www.umbrella-security.com | info@umbrella-security.com
A Company of Cittadini dell’Ordine S.p.A. www.cittadinidellordine.com

CDO
A safe world

Bentel Security presenta BW-IO

BENTEL SECURITY S.R.L.
(+39) 0861 839060
www.bentelsecurity.com

Bentel Security presenta il dispositivo **BW-IO** della Serie Wireless BW e accresce così la gamma dei rilevatori magnetici multi funzione disponibili.
Il **BW-IO**, infatti, non è solo un contatto magnetico ma anche un modulo con due pin di ingresso indipendenti per poter collegare sensori cablati e supervisionati e ogni ingresso può essere configurato come ingresso 'Normalmente Chiuso', 'Normalmente Aperto', 'Bilanciamento Singolo' o 'Bilanciamento Doppio'.
E' possibile registrare più di un **BW-IO** e avere ingressi cablati fino al massimo numero di zone disponibili in centrale.
Il **BW-IO** dispone anche di due pin di uscita per poter attivare/disattivare l'illuminazione, il cancello, il garage, le tapparelle, i generatori di fumo, il condizionatore piuttosto che la caldaia: tutto questo in modo semplice e veloce direttamente dall'APP Utente BW!
Tramite il **BW-IO** le centrali **Bentel Wireless Serie BW** possono gestire fino a 16 uscite aumentando notevolmente le opportunità installative, soddisfacendo le più ampie e diversificate esigenze degli utenti, degli installatori e degli istituti di vigilanza e ampliando l'offerta di funzionalità da proporre al cliente finale.
Il **BW-IO** è provvisto di un LED che indica visivamente la qualità del segnale; l'installatore può così scegliere facilmente la posizione ottimale senza spostarsi ripetutamente tra il dispositivo e la tastiera. Anche la configurazione risulta facile e veloce, perché non richiede regolazioni hardware e tutte le impostazioni di configurazione possono essere gestite dalla tastiera.

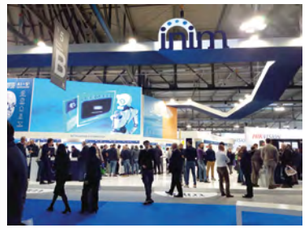
Soluzione innovativa di rivelazione incendio all'interno di tunnel stradali. Un nuovo firmware per AVIOTEC IP Starlight 8000!

BOSCH SECURITY SYSTEMS S.P.A.
(+39) 02 36961
www.boschsecurity.it

Le tecnologie di rivelazione utilizzate all'interno dei tunnel stradali rilevano principalmente la presenza di fiamma (es. cavi termosensibili in fibra ottica) segnalando quindi la presenza di incendio in una fase molto avanzata a discapito della sicurezza generale.
La telecamera **AVIOTEC IP Starlight 8000** di **Bosch** oltre alla fiamma è in grado di rilevare anche il fumo. Si tratta di una rivelazione affidabile e tempestiva anche nella condizione in cui il fumo non raggiunga il punto più alto del tunnel. La presenza di flussi d'aria all'interno delle gallerie, infatti, rende difficile la rilevazione da parte delle comuni tecnologie utilizzate. Grazie al nuovo firmware 7.50, la telecamera AVIOTEC riesce a rivelare anche la presenza di fumo con stratificazioni laterali.
L'algoritmo di video analisi a bordo camera garantisce una totale affidabilità del sistema rispetto a soluzioni dove l'algoritmo risiede all'interno di PC Server centrali che, in caso di guasto, comprometterebbero la corretta funzionalità di tutte le telecamere del sistema.
AVIOTEC IP Starlight 8000, oltre ad essere un dispositivo di rivelazione incendio efficace ed innovativo, dispone di avanzati algoritmi di Video Analisi con specifiche funzioni di Safety & Security utilizzabili in parallelo. Può riconoscere, ad esempio, un'auto ferma che rallenta in direzione opposta al verso di marcia, la presenza di pedoni in carreggiata, l'attraversamento linea bordo carreggiata, incidenti, coda, ecc.
AVIOTEC è un alleato perfetto non solo in ambito stradale ma anche industriale e logistico, dotato di certificazione VdS.

A SICUREZZA 2019 INIM Electronics presenta l'Augumented Intelligence applicata al mondo della sicurezza

INIM ELECTRONICS S.R.L.
(+39) 0735 705007
www.inim.biz



INIM si è presentata a SICUREZZA con un approccio "Total protection for Life": un fornitore globale in grado offrire soluzioni in ogni ambito del building, dal residenziale all'industriale ed al professionale.
I sistemi INIM sono sistemi di ultima generazione. Semplicità d'uso, automazione e integrazione sono le parole d'ordine, oggi, quando si parla di sicurezza. Ed è su questa consapevolezza che INIM Electronics ha basato gran parte del lavoro svolto e sviluppa sistemi di ultima generazione in ambito antintrusione, rivelazione incendio, domotica e illuminazione di emergenza. Sistemi integrati e dal design attuale che proteggono e automatizzano strutture abitative, commerciali e istituzionali.
A Fiera SICUREZZA INIM ha parlato di Augumented Intelligence. INIM ha infatti in essere progetti di studio e ricerca sull'intelligenza artificiale applicati al mondo della sicurezza in collaborazione con l'Università Politecnica delle Marche, proprio per essere sempre all'avanguardia ed offrire un prodotto altamente tecnologico.
Parlando di prodotti e servizi, una novità assoluta nella rivelazione incendio è il il Cloud incendio, un servizio unico che consente al progettista, all'impiantista ed al responsabile della sicurezza di avere il totale controllo della propria attività.
Nell'ambito intrusione è stata presentata Sol, una centrale via radio pensata per il professionista protetta dalle vendite online, dal punto di vista tecnico e funzionale, per usare il via radio in tutta tranquillità.
Naturalmente grande valore alla centrale ammiraglia Prime con tutti gli addendum domotici che stanno arrivando.
Un occhio molto attento da parte di INIM anche alle richieste dell'utente finale che vuole automazione, sicurezza e chiede di controllare la propria abitazione con voce. Ecco che nasce Marilyn, sistema vocale integrato che si sposa perfettamente con le piattaforme Google ed Amazon, per fornire confort nell'uso del sistema domotico e nel sistema di sicurezza della propria casa.

RISCO Group presenta Piccolo

RISCO GROUP
(+39) 02 66590054
www.riscogroup.it

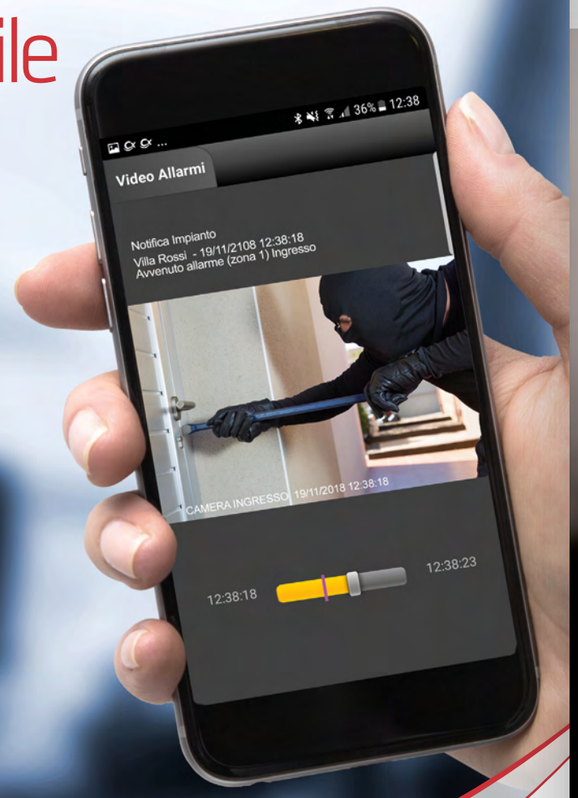
Piccolo è il nuovo e innovativo sensore di movimento radio di RISCO Group dalle dimensioni compatte, dotato di lenti convesse per offrire elevate prestazioni di rilevazione. Caratterizzato da un design innovativo ed elegante, Piccolo è pensato per gli utenti residenziali che per la loro proprietà scelgono uno stile contemporaneo.
Il sensore radio PIR è in grado di offrire una copertura fino a 10 m ed è progettato per semplificare installazione e manutenzione, grazie a configurazione e diagnosi da remoto. Inoltre, la sua staffa magnetica permette all'utente di effettuare la sostituzione delle batterie in tutta comodità.
Piccolo supporta una comunicazione in modalità sia mono che bidirezionale ed è compatibile con tutti i sistemi radio e ibridi di RISCO Group: Agility™4 dalla versione 5.17, LightSYS™ dalla versione 5.80, ProSYS™ Plus dalla versione 1.2.1.17.
A breve sarà disponibile anche una versione di Piccolo con immunità agli animali.

Un occhio sempre vigile sulla tua casa!

L'esclusiva VIDEOVERIFICA di Combivox per una gestione integrata ANTIFURTO+VIDEOSORVEGLIANZA.

combivox.it

MADE IN ITALY



Antifurto+ Videosorveglianza: associazione zona-telecamera per la videoverifica su allarme

Videoallarme (filmato 30s, con pre-recording configurabile fino a 10s)

Registrazione H24 in risoluzione VGA su SD, consultazione dei file da APP e da browser

8 telecamere IP ONVIF 2.0

S.O. **Linux Embedded**

Smartweb Video

Collegamento della centrale Combivox tramite **BUS RS485**.
Grazie all'associazione sensori-telecamere, è possibile attivare la funzione di **VIDEOALLARME**: in caso di allarme, il dispositivo registra un filmato della durata fino a 30 secondi, con 10 secondi di preallarme (immagini prima di avvenuta attivazione del sensore), trasmettendolo a più indirizzi email. Inoltre, a seguito di una notifica Push di segnalazione allarme, direttamente su APP Simplya Cloud si visualizza, in tempo reale, il Videoallarme in corso di registrazione con verifica live del pre-allarme.
Smartweb Video è anche un **VIDEOREGISTRATORE H24** in risoluzione VGA direttamente su memoria SD, con consultazione dei file da web browser o da APP.

COMBIVOX
ENJOY LIFE, SAFELY.

SICUREZZA
INTERNATIONAL SECURITY & FIRE EXHIBITION
13-15 NOVEMBER 2019
Pad. 7 - Stand E11 F20

100% MADE IN ITALY

COMPLETAMENTE GESTIBILE DA REMOTO

NON ESPLOSIVO **NON INFIAMMABILE** **NON TOSSICO** **NON CORROSIVO** **NON ENERGIVORO**

PROTEGGI I TUOI BENI CON LA PIU' COMPLETA GAMMA DI NEBBIOGENI

CON O SENZA CENTRALE D'ALLARME

LA **DIFESA** ASSOLUTA IN UN **ATTIMO**

essecome ONLINE

n. 08 dicembre 2019
Anno XXXIX
Periodico fondato da Paolo Tura

DIRETTORE RESPONSABILE E COORDINAMENTO EDITORIALE
Raffaello Juvara
editor@securindex.com

HANNO COLLABORATO A QUESTO NUMERO
Angelo Carpani
Nils Fredrik Fazzini

SEGRETERIA DI REDAZIONE
redazione@securindex.com

PUBBLICITÀ E ABBONAMENTI
marketing@securindex.com

EDITORE
essecome editore srls
Milano - Via Montegani, 23
Tel. +39 02 3675 7931

REGISTRAZIONE
Tribunale di Milano n. 21
del 31 gennaio 2018

GRAFICA/IMPAGINAZIONE
Lilian Visintainer Pinheiro
lilian@lilastudio.it