CONNESSIONI
THE INTEGRATED SYSTEMS MEDIA

Italiano
English

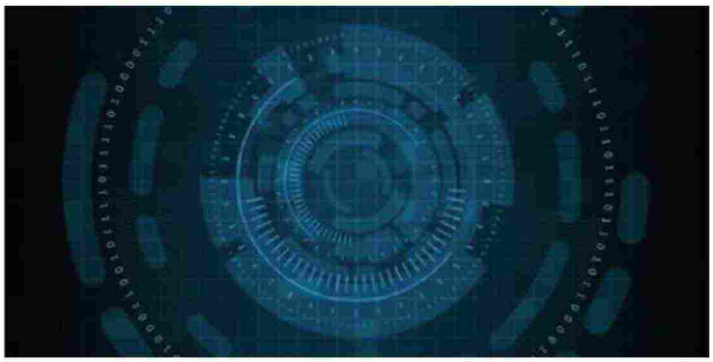
Seguici su....

ABOUT US | MAGAZINE | NEWSLETTER | WEBSITE | EVENTS | COMMUNICATION | REFERENCES | Cerca

Lavora con noi!
Iscriviti
Filosofia del Website
Reviews
Prodotti
Tecnologie
Applicazioni
Video-gallery

Convergenza digitale, parola chiave della "nuova" sicurezza

06-07-2018

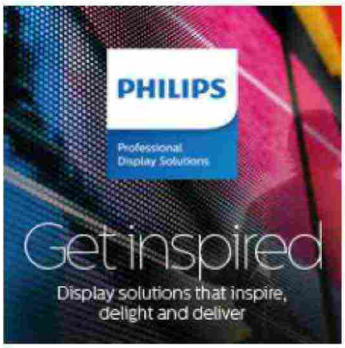


La visione sistemica di in un settore, quello della sicurezza, dove i confini tra security, safety e automazione risultano ormai sottili, nella nostra intervista a **Giulio lucci, presidente di** Anie Sicurezza. Un approfondimento su aspetti tecnici, normativi e "culturali", legati al cambiamento tecnologico in atto, che assume ancora più importanza in seguito alla recente entrata in vigore del nuovo GDPR per la protezione dei dati personali e alla maggiore attenzione del mercato verso soluzioni digitali e connesse.

Connessioni – La digitalizzazione dei processi, in una nuova era dove regnano integrazione e smart building, rappresenta una sfida anche per il mondo della sicurezza. Come giudica l'attuale situazione del mercato italiano? Cosa è cambiato e come si prospettano gli anni a venire?
GI – Il mercato della sicurezza ha avuto e sta avendo un profondo cambiamento che impatterà sia sulle architetture di sistema sia sui modelli di business, ma anche sugli aspetti procedurali e normativi/legali. Ciò è dovuto soprattutto a due fattori determinanti: l'elevato sviluppo delle tecnologie e la forte crescita della necessità di proteggere i beni (materiali, immateriali e umani). "Convergenza" è la parola d'ordine, in primo luogo tra sicurezza fisica e sicurezza logica. Tale aspetto ha avuto inizio e sta avendo una progressione esponenziale grazie alla "**digitalizzazione**" che consente a ogni sistema di essere collegato; da qui la crescita di soluzioni software che consentano l'interoperabilità dei sistemi. Tale sviluppo tecnologico è facilmente divenuto il driver che ha portato alla ulteriore convergenza di settori, appartenenti allo stesso mondo o limitrofi: **security, safety** e **automazione**. Tale convergenza non è più rimasta solo concettuale e/o di competenza specifica, ma è divenuta "sistemica" ed è questa la vera svolta e visione del futuro, se vogliamo la sfida. La sicurezza non può più essere percepita per settori e con un approccio azione-reazione, ma come un unico "ambiente" che consenta la supervisione del tutto, nell'ottica di quello che oggi viene chiamato **Early Warning**. Quanto al rapporto tra uomini e tecnologie, a mio avviso non vi sarà convergenza, come non dovrà esserci collisione, ma semplicemente una ridefinizione dei ruoli.

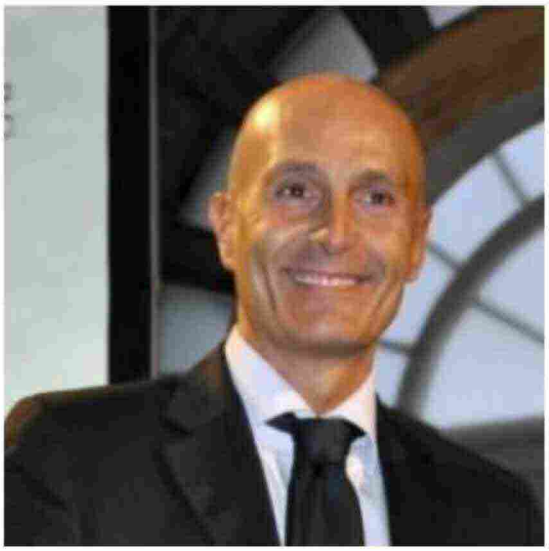
ADVERTISEMENT

zappiti.it Store



Codice abbonamento: 046087

Ritaglio stampa ad uso esclusivo del destinatario, non riproducibile.

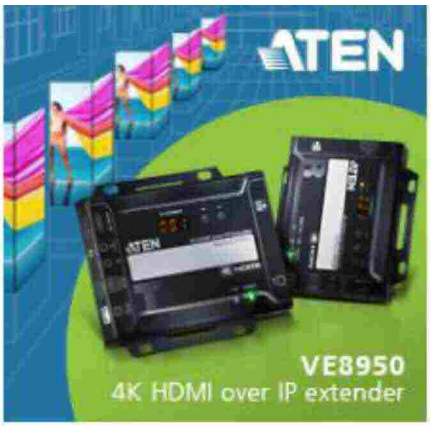


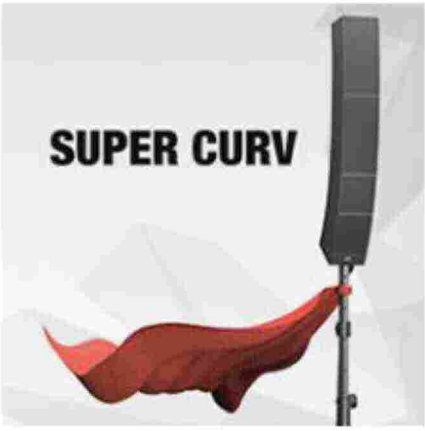
C – La convergenza tra due "tipi" di sicurezza – fisica e cyber – un tempo distinti richiede nuove competenze?
GI – Mi spiego meglio: la tecnologia non è e non sarà solo un sensore che invia un allarme, che viene preso in carico da un uomo il quale interviene tramite una procedura. La tecnologia è centrale, è in grado di intercettare un numero elevatissimo di informazioni, di correlarle e metterle a disposizione dell'uomo, il tutto ad una velocità elevatissima. La filiera nei sistemi complessi è la seguente: monitorare, intercettare, correlare, interpretare, intervenire, contenere, ripristinare, apprendere, implementare. La tecnologia non sostituisce quindi l'uomo, ma è un potentissimo mezzo di supporto alle decisioni. L'uomo c'è sempre: all'inizio, quando costruisce la logica e l'architettura del sistema; durante, quando programma la tecnologia e la manutiene; alla fine quando prende le decisioni e interviene, ma anche quando corregge e implementa.

C- Con quali strategie aziende, system integrator e clienti finali dovrebbero approcciare i nuovi rischi legati a sistemi aperti, cloud e IoT?
GI – Le strategie aziendali dovranno tener conto di un nuovo approccio alla progettazione, che diventa sempre più sistemica e globale. Il nuovo approccio progettuale non potrà prescindere dal seguire ferree regole architetturali, procedurali, normative e tecnologiche, tenendo conto di diversi aspetti, a cascata: dalla supervisione alla segmentazione, dalla protezione dei punti di accesso alle trasmissioni sicure; dai penetration test periodici all'aspetto, sempre più impattante del criterio di resilienza di tutto il sistema.

C – Che ruolo assume una realtà associativa come Anie Sicurezza in questo inedito paradigma?
GI – Assume un ruolo fondamentale, che si dipana seguendo tre linee direttrici. La prima riguarda la **focalizzazione sul mercato**: la nostra associazione, oltre ad avere l'obiettivo di qualificare le offerte professionali e tecnologiche, ha il dovere di "ascoltare" il mercato, di coglierne le esigenze e di "restituire", alla fine di tale processo, prodotti, sistemi e soluzioni efficaci e coerenti con le esigenze e le aspettative specifiche di ogni settore. In tal senso sono stati formati e si stanno formando gruppi di lavoro centrati sul mercato, prima ancora che sul prodotto, coinvolgendo direttamente le specifiche associazioni di mercato ad una partecipazione attiva in un tavolo comune di lavoro. Parliamo poi come già evidenziato di **convergenza** tra sicurezza fisica e sicurezza logica in ottica "digitalizzazione", dove l'interoperabilità dei sistemi è divenuto il driver che ha portato alla convergenza tra security, safety e automazione, con tutte le opportunità da cogliere e i rischi da scongiurare. Infine, Anie vuole essere **centro di competenza**. Le considerazioni fatte e che faremo ci confermano l'obiettivo primario di essere riconosciuti, dalle diverse associazioni di settore, dai relativi professionisti, ma soprattutto dal mercato di riferimento, come centro di competenza informativo e formativo, che ha anche la missione di "guidare" tale cambiamento nel rispetto della professionalità, delle regole e della migliore "visione" sugli sviluppi futuri della tecnologia e del mercato.

aniesicurezza.anie.it





Codice abbonamento: 046087

Ritaglio stampa ad uso esclusivo del destinatario, non riproducibile.