TSec, overview e risposte concrete alle esigenze di sicurezza integrata

a colloquio con Luca Salgarelli, presidente TSec
a cura di Raffaello Juvara

TSec e "Le Eccellenze per la Sicurezza", una collaborazione iniziata nella prima edizione del seminario nel 2015 dedicato ai decisori per la sicurezza dei Grandi Utilizzatori, che presuppone la condivisione della visione che ha ispirato il progetto: un momento esclusivo di incontro e di confronto tra chi progetta e sviluppa soluzioni di sicurezza ai massimi livelli e chi le utilizza, per individuare le linee guida del futuro del settore, anche dirompendo gli schemi consolidati. Quali provocazioni lancerà TSec nella prossima edizione del seminario?

Nessuna, perbacco! "Le Eccellenze per la Sicurezza" nasce come momento di incontro tra chi crea tecnologie per la sicurezza, i produttori, e chi queste tecnologie le usa per soddisfare un bisogno, ovvero i security manager, gli integratori e i decisori. In questo ambito, TSec nel passato come nel presente sta cercando di guardare a noi stessi ed al mercato della sicurezza con un occhio critico. Credo che la nostra giovane età (industrialmente parlando, s'intende) e la passione che ci guida ce lo permettano. Questo essere critici con noi stessi e con il nostro mercato, costruttivamente, ci porta qualche volta a fare analisi che possono sembrare provocazioni, ma non vogliono assolutamente esserlo. Gli spunti che ci guidano derivano da una visione della tecnologia per la sicurezza che crediamo debba necessariamente contaminarsi con la rapida evoluzione dei settori a noi vicini, innanzitutto quello dell'IoT, e cercare di investire il più rapidamente possibile in nuovi sistemi, nuove tecnologie e nuovi approcci alla sicurezza. Perché questo processo abbia successo, è però necessario slegarsi dall'approccio iper-frammentario e di contrapposizione tra concorrenti che il nostro settore (insieme ad altri) ha perseguito fino ad oggi. È invece utile guardare agli investimenti in nuove tecnologie attraverso la lente dell'open *innovation*, unendo capitali, conoscenze e strategie per innovare insieme, a livello di sistema. Io non penso che questa sia una provocazione, ma una necessità pressante se il settore della sicurezza vuole tornare a contare sia sul piano nazionale che su quello internazionale, non crede?

Uno dei leitmotiv del momento è la "scoperta" della vulnerabilità dei devices per la sicurezza fisica rispetto alle minacce informatiche, conseguente in particolare alla diffusione delle tecnologie IoT. Qual è il vostro punto di vista in merito?

Purtroppo la diffusione sempre più capillare di dispositivi "*always on, always connected*" sta portando alla superficie un problema finora dormiente: la sicurezza nelle comunicazioni. Finché si trattava di gestire la sicurezza di computer, la tecnologia ci ha aiutato, almeno in qualche modo: a livello professionale con architetture di rete, sistemi di *firewalling* e di antivirus tutto sommato efficaci; a livello consumer un po' meno, ma, con gli anni, anche gli utenti meno professionali hanno imparato a cavarsela. Il processo in corso sta portando lo stesso livello di connettività IP fino a ieri riservato ai computer, anche alla miriade di dispositivi che rendono "intelligenti" gli edifici, gli spazi di lavoro e le città, dai termostati alle telecamere, dagli apriporta ai sistemi di condizionamento dell'aria fino ad arrivare ai semafori e ai sistemi di illuminazione cittadina. In virtù di questo processo, immediatamente si moltiplicano i vettori di possibile attacco, e contemporaneamente le ricompense per gli attaccanti diventano più allettanti: con un attacco di successo, diventa infatti possibile monitorare e condizionare in maniera capillare non più solo i nostri computer, ma la nostra vita quotidiana. Credo sia necessario pensare ad una infrastruttura di sicurezza informatica e delle telecomunicazioni nuova, progettata esplicitamente per il mondo IoT che sta arrivando. Ad ogni processore (CPU), sia esso in un termostato, in uno smartphone o in una centrale d'allarme, è necessario affiancare un processore dedicato alla sicurezza e, in particolare, alla comunicazione sicura. Sono dell'opinione che solo con una nuova architettura basata su sistemi hardware dedicati alla sicurezza si possa scongiurare quello che potrebbe essere un vero e proprio disastro informatico, e che altrimenti rischiamo di subire a causa dell'introduzione capillare di dispositivi connessi. Purtroppo, un disastro tecnologico di tale portata porterebbe con se' anche ricadute economiche molto significative, che non ci possiamo permettere, specialmente in questo momento storico.

Aumenta la richiesta a livello globale di "protezioni perimetrali intelligenti" dalle abitazioni private agli obiettivi sensibili, con soluzioni che integrano rilevamento, immagini, analisi dei dati, sistemi di risposta. Quali sono le proposte di TSec?

Nei prossimi mesi presenteremo due soluzioni perimetrali esterne basate su tecnologie che stiamo sviluppando da tempo: la prima si basa su concetti di *signal processing* evoluto, applicati all'analisi delle vibrazioni; la seconda su sistemi radar avanzati. In entrambi i casi, i sistemi permetteranno di rilevare con precisione luoghi e tipologie di effrazione perimetrale, minimizzando contemporaneamente i falsi allarmi. Entrambe le soluzioni sono state ingegnerizzate non per funzionare isolate da altri sistemi di protezione, in primo luogo la video sorveglianza e la video analisi, bensì per divenirne strumenti di supporto, in grado di coadiuvare la loro funzione e, allo stesso tempo, di moltiplicarne l'utilità. Anche qui, come in quello dell'open *innovation* citato sopra, crediamo che l'unione, in questo caso di sistemi tecnologici diversi anche provenienti da produttori diversi, faccia la forza.

Quali sono gli altri ambiti ai quali il vostro Gruppo si sta dedicando?

TSec non è un gruppo industriale propriamente definito, ed è focalizzata in maniera estremamente verticale sul mercato della sicurezza fisica, quindi non ci dedichiamo esplicitamente ad ambiti diversi da quello delle tecnologie per la sicurezza. È però vero che collaboriamo in maniera molto stretta con una serie di aziende, alcune delle quali nostre socie, che ci permettono da un lato di "contaminare" i nostri prodotti con esigenze, tecnologie e funzionalità che provengono da altri settori industriali, come quello dell'automazione; dall'altro, di lavorare insieme a nuove piattaforme tecnologiche come, ad esempio, quelle legate alla sicurezza delle telecomunicazioni, condividendo esperienze, costi, rischi e benefici. In questo senso, non ci stiamo dedicando ad altri ambiti, ma lavoriamo a stretto contatto con aziende, piccole e grandi, che lavorano in diversi settori tecnologici, dalla building automation, alla safety industriale, al medicale per finire con il mondo dei servizi informativi.

Come si articolano e si integrano, dal vostro punto di vista, i concetti di "Sicurezza" e di "Intelligenza" della Casa, dell'Edificio, della Città?

Credo che vedremo una rapida evoluzione di questi sistemi in due direzioni. Da un lato, ci sarà un processo di veloce integrazione dei sistemi di building/campus/city automation con quelli che ne gestiscono la sicurezza. Dall'altro, tutte le piattaforme tecnologiche per la sicurezza dovranno evolvere per orientarsi sempre più all'erogazione dei servizi. Queste due forze di cambiamento sono già in atto, parte di un processo di evoluzione che non solo è inarrestabile, ma si sta velocizzando sempre più. Stiamo vedendo l'alba di quella che molti definiscono come la prossima rivoluzione industriale: sulle fondamenta dell'ultima rivoluzione che abbiamo vissuto, quella di Internet, stiamo per costruire il prossimo strato tecnologico che guiderà il progresso nel prossimo decennio. L'integrazione di funzioni diverse su questo strato, nello specifico la sicurezza, l'intelligenza e l'automazione, aprono opportunità davvero strabilianti, sia per i produttori, che per gli utilizzatori di queste tecnologie. Sta a noi tutti fare in modo che le opportunità non si trasformino in problemi, e qui faccio riferimento al problema della sicurezza delle comunicazioni citata poco fa, e che gli attori del mercato si muovano a livello di sistema per guidare questo processo di integrazione, anziché subirlo.