Cybersecurity e privacy by design dei produttori, consapevolezza degli utenti finali: i punti chiave di Genetec contro le minacce informatiche

intervista a Gianluca Mauriello, Regional Sales Manager Italia, Genetec Inc.

Ci può parlare di Genetec, della sua storia e delle sue linee di prodotto?

Genetec Inc. è un provider innovativo con un ampio portafoglio di soluzioni nel campo delle tecnologie per la sicurezza unificata, per la protezione delle operations e nelle soluzioni di business intelligence. Fondata nel 1997, e con sede a Montreal, Canada, Genetec raggiunge i propri clienti grazie a un'estesa rete di rivenditori, integratori, partner di canale certificati e consulenti in oltre 80 paesi.

Il prodotto di punta dell'azienda è **Security Center**, una piattaforma dall'architettura aperta che è in grado di unificare sistemi di videosorveglianza su IP, controllo accessi, riconoscimento targhe (ALPR), comunicazioni e analitica.

Genetec sviluppa, inoltre, soluzioni e servizi cloud-based progettati per migliorare la sicurezza e contribuire a nuovi livelli di intelligenza operativa in strutture governative, aziende, trasporti e le comunità in cui viviamo.

L'esempio più chiaro di questa intelligenza operativa è rappresentato da **Mission Control**, un sistema collaborativo di gestione delle decisioni che fornisce una supervisione completa su tutti i sistemi, dispositivi e sensori.

In combinazione con procedure guidate, tracciamento visivo e capacità di collaborazione, Mission Control offre un quadro operativo comune nelle organizzazioni in cui affidabilità e tempi di risposta rapidi sono fondamentali.

A quali categorie di utenti si rivolge in Italia e come è strutturata sul piano organizzativo?

In Italia ci rivolgiamo principalmente a end-user che lavorano in vari mercati, dall'industria agli enti governativi, dalle aziende alla public safety (mi riferisco a trasporti, sorveglianza

cittadina estesa, strutture sanitarie) e poi infrastrutture critiche (porti, aeroporti, energia e utility, Building & Industrial) e retail (centri commerciali e punti vendita, banche).

Negli ultimi mesi molti end-user, operanti in settori strategici per la sicurezza (trasporti, energy utility e retail), si sono avvicinati alle nostre soluzioni di sicurezza unificata e con molti di questi stiamo sviluppando, attraverso i nostri system integrator e consulenti, progetti sempre più complessi.

Per quanto riguarda la nostra organizzazione in Italia, mi confronto giornalmente con il Direttore Vendite Sud Europa Rafael Martin Enriquez, ed insieme possiamo contare sulla competenza di Vito Candiloro, Channel Sales Specialist e di Jordi Charles Rodriguez, Sales Engineer.

Infine, stiamo cercando nuovi talenti per ampliare il nostro team, garantendo così una maggiore e più tempestiva presenza sul territorio, potendo sempre contare sul supporto tecnico della filiale di Parigi e della sede a Montreal.

Qual è la vostra visione del mercato globale della sicurezza fisica nel 2021?

Negli ultimi mesi, abbiamo osservato notevoli prove di resilienza e intraprendenza da parte di molte imprese, che si sono adattate alle necessità imposte dalla COVID-19, utilizzando le tecnologie di sicurezza fisica come strumento strategico per la lotta alla pandemia. Ecco perché sarà necessario andare oltre alle applicazioni tradizionali, per offrire sempre più innovazione.

Ma questa innovazione dovrà necessariamente andare di pari passo con la privacy e la sicurezza informatica, aspetti, questi, che imporranno ai vendor la creazione di soluzioni software sempre più sicure contro gli attacchi informatici e sempre più resilienti, per garantire la protezione dei dati senza comprometterne la disponibilità.

Ci aspettano ancora mesi di tracciamento dei contagi, oltre a tutta una serie di sfide sociali che andranno affrontate con trasparenza, progettando prodotti responsabili e innovativi che abbraccino le metodologie della privacy by design così che non sia più necessario dover scegliere tra proteggere la privacy individuale e tutelare la sicurezza fisica.

Il tutto in un mondo in cui l'infrastruttura cloud pubblica diventerà sempre più diffusa. Pensiamo all'aumento del lavoro da remoto dell'ultimo anno.

Ecco perché dovremo superare la presunta dualità cloud/sistemi di sicurezza on-premise: per andare sempre più verso un uso ibrido dell'infrastruttura di sicurezza fisica, implementando applicazioni specifiche sul cloud e mantenendo i sistemi on-premise esistenti. Questo permetterà di stare al passo con l'evoluzione delle organizzazioni, lavorando, di concerto con i dipartimenti IT, su scalabilità, ridondanza e disponibilità.

Infine, ma non per importanza, proprio per questo sodalizio ormai consolidato fra sicurezza fisica e strategia IT, le aziende dovranno realizzare una selezione oculata di produttori, fornitori e distributori. Tutta la supply chain dovrà rendere conto della sicurezza e affidabilità dei propri sistemi, fornendo risposte trasparenti sulle vulnerabilità dei propri prodotti, i partner con cui lavorano e le politiche privacy e dati.

Dal vostro punto di osservazione, come valutate il livello di consapevolezza del rischio cyber nel nostro paese?

Fino ad oggi il rischio di un attacco hacker esterno è sempre stato snobbato dagli addetti ai lavori con la giustificazione della disconnessione della rete LAN aziendale da quella utilizzata dalle telecamere, perché la security IP era relegata alla sola videosorveglianza o poco più. Oggi lo scenario sta rapidamente evolvendo verso un'integrazione di sistemi di sicurezza che vanno oltre il semplice video. Le reti interconnettono sistemi di controllo accessi, impianti tecnologici, interfonia che generano ingenti quantità di dati che spesso vengono utilizzati anche da sistemi di gestione aziendale al fine di produrre, monitorare e gestire processi molto complessi.

Genetec, da sempre, è attenta alla cybersecurity - sin dalla fase di progettazione - di qualsiasi suo prodotto software e hardware, che sottopone a test specifici tramite aziende indipendenti e specializzate.

Credo vi sia un gran bisogno di sensibilizzare e fare più formazione sui rischi legati alla sicurezza informatica. Nel contesto attuale e con il numero di attacchi in continuo aumento, certamente c'è più consapevolezza rispetto al passato, ma forse non è ancora sufficiente.

Prendiamo molto sul serio la cybersecurity e già da molti anni operiamo attivamente in questo ambito, muovendoci su quattro pilastri: identificazione e mitigazione del rischio, offerta di soluzioni affidabili, costruzione di una rete fidata, trasparenza e apertura.

Contatto:
Genetec Inc.
www.genetec.com