Cosa significa convergenza tra sicurezza fisica e sicurezza IT per Axis Communications

a colloquio con Andrea Monteleone, National Sales Manager Axis Communications srl
a cura della Redazione

Parlando della convergenza tra sicurezza fisica e sicurezza IT, qual è la visione di Axis, uno dei leader a livello globale dei sistemi di videosorveglianza IP?
La visione di Axis su questo argomento è molto chiara: non si può e non si deve pensare alla sicurezza se non come ad un unicum, dove elementi fisici e informatici rappresentano le due facce della stessa medaglia. Sicurezza fisica e sicurezza IT, ambiti fino a poco tempo fa ben distinti, sono oggi invece realtà che condividono strumenti comuni e lavorano in sinergia per mitigare le minacce, sia fisiche che informatiche, per una determinata azienda o istituzione. Se pensiamo a come sono strutturati oggi i sistemi di sicurezza, e sempre di più lo saranno in futuro, ci si rende immediatamente conto di come i risultati migliori si ottengano nei casi in cui ogni scelta venga fatta ponderando tutte queste variabili, senza dimenticare ovviamente il fattore umano che rappresenta, nella stragrande maggioranza dei casi, l'anello debole della catena. La definizione di un livello di protezione accettabile dipende dalla situazione, dal livello di minaccia e dal costo di possibili violazioni. Ben consapevoli, però, che non sia possibile creare un sistema sicuro al 100%, almeno non un sistema utilizzabile. Tuttavia, è possibile rendere un sistema più sicuro, riducendo le aree di esposizione e attenuando i rischi, che ci saranno sempre, ma devono essere conosciuti e gestiti.

Dalla vostra posizione, quali sono i punti di convergenza più frequenti e significativi oggi e nel prossimo futuro, con la prevista diffusione su larga dei dispositivi IoT?
Difficile dare una risposta esaustiva a una domanda di

questo genere, perché il tema è in costante e rapido divenire. Volendo focalizzarsi sull'ambito IoT, gli elementi che consideriamo cruciali sono sostanzialmente tre: in primo luogo la sicurezza intrinseca dei device in campo. Saranno gli "oggetti" più significativi dal punto di vista numerico e, come i recenti attacchi di tipo DDoS hanno dimostrato, sono già quelli più esposti alle logiche di attacco massivo. In seconda istanza, l'infrastruttura di trasporto e memorizzazione delle informazioni che sono, in molti casi, l'asset più importante da difendere. Nell'immaginario collettivo si parla spesso di dispositivi IoT, di Cloud, ma è doveroso occuparsi anche del 'come' le nostre informazioni vengano gestite. In conclusione, ma non per questo meno importante, il fattore umano. La sicurezza si ottiene anche e soprattutto attraverso una minuziosa progettazione e una altrettanto attenta gestione

della installazione dei sistemi, oltre ad una costante e continuativa formazione delle persone coinvolte, siano esse gli addetti ai lavori o gli stessi utenti finali.

In concreto, quali soluzioni propone Axis per la protezione delle componenti fisiche dei sistemi adibiti al trattamento dei dati?

Se parliamo di componenti fisiche, nel nostro caso, parliamo di una grandissima quantità di dispositivi sia edge che server. Da questo punto di vista, Axis si è impegnata a far sì che venissero adottati tutti gli accorgimenti possibili già all'origine, progettando dispositivi sicuri "by design". Ma è altrettanto vero che la nostra azienda veicola solo una parte dei sistemi. È importante capire che le minacce devono essere gestite a livello di sistema e non a livello di singolo prodotto: la Cyber Security è un processo, non un prodotto. È oggettivamente impossibile eliminare tutti i rischi, anzi questo tentativo potrebbe risultare estremamente costoso e, talvolta, inutile. La raccomandazione è, quindi, quella di identificare i dati più sensibili e proteggerli nel modo più efficace possibile. Il punto focale della questione, per Axis, è quello di contribuire a raggiungere un livello di sicurezza accettabile, ottimizzando i costi per raggiungere questo obiettivo. Al di là dell'attenzione posta sui singoli prodotti, Axis Communications, consapevole dell'importanza del tema Cyber Security anche nel settore della videosorveglianza, si impegna a fornire tutti gli strumenti per proteggere i propri clienti dagli attacchi sul web e per creare soluzioni sempre più sicure da questo punto di vista. Con i nostri Partner e Clienti manteniamo un costante scambio di informazioni e ci sforziamo di supportarli anche in tutte le fasi successive, che sono più legate allo hardening delle difese fisiche e informatiche in campo. Questo avviene tramite corsi online, webinar e pubblicazioni di aggiornamento specifiche che rendiamo disponibili in rete. In particolare, offriamo ai nostri clienti una guida tecnica per seguire le corrette procedure nell'installazione di un sistema di videosorveglianza: l'Axis Hardening Guide, un documento che facilita questo processo e contribuisce a proteggersi dagli attacchi informatici, scaricabile dal nostro sito web.

Con quali tipologie di interlocutori della filiera interagite ora ed intendete interagire prossimamente per realizzare soluzioni di sicurezza convergente in linea con i vostri standard?

Da anni, ormai, la sempre maggiore complessità dei sistemi di sicurezza comporta una costante e continuativa relazione tra i vendor, i progettisti, il canale distributivo e quello di installazione, in un'ottica di condivisione delle nuove opportunità offerte dall'avanzamento della tecnologia, dalle possibili sfide e dalle problematiche a cui ci si può trovare davanti e del know how necessario per risolverle. In uno scenario di questo tipo, sempre di più, sarà coinvolto anche l'utente finale, che è e soprattutto deve essere considerato come parte attiva del processo. Dobbiamo inoltre considerare che effettuare lo hardening di dispositivi IoT è più facile rispetto a dispositivi client o server, in quanto dispongono di un minor numero di servizi interni e di interfacce. La maggior parte dei device è protetta da infrastrutture accessibili solo attraverso specifici servizi cloud/server e i loro utenti non installano applicazioni non sicure, non aprono allegati di posta elettronica pericolosi o accedono a siti sospetti. Axis Communications, nella piena consapevolezza dell'importanza dell'argomento, ma consapevole al tempo stesso che i propri clienti stiano già seguendo delle regole di base in materia di Cyber Security, ha redatto la guida prima citata con l'obiettivo di agevolare, attraverso semplici passaggi, un fine tuning delle telecamere considerate come device della rete.

CONTATTI: AXIS COMMUNICATIONS
Tel. +39 02 84245762
www.axis.com