Idee e proposte da Axis Cybersecurity Summit 2023

intervista a Matteo Scomegna, Regional Director Southern Europe di Axis Communications

Possiamo tracciare un bilancio dell'edizione 2023 dell'AXIS Cybersecurity Summit?

L'Axis Cybersecurity Summit di Roma e di Milano si inserisce nel contesto più ampio di un ciclo di incontri che abbiamo organizzato in diversi paesi del Sud Europa, a partire da Parigi lo scorso giugno. Alla base di queste iniziative c'è la volontà di Axis di organizzare dei momenti di confronto tra tutti gli attori principali del nostro settore, nazionali e internazionali, con l'obiettivo di condividere ciascuno le proprie esperienze e, allo stesso tempo, sensibilizzare su quella che è una tematica molto attuale e complessa.

In questo senso, possiamo ritenerci soddisfatti, perché l'adesione al Cybersecurity Summit italiano è stata alta, così come l'interesse mostrato dai partecipanti e dagli speaker. Più nel dettaglio, nel corso dei tre panel di discussione sono emersi numerosi spunti che hanno permesso di approcciare la cybersecurity da diverse prospettive. Una prima occasione di confronto ha riguardato l'aumento preoccupante delle minacce informatiche e la definizione delle responsabilità; seguita da un approfondimento sul quadro normativo attuale e futuro, a partire dalle Direttive NIS I e II, dalla Direttiva CER, passando per il Regolamento DORA; fino alle proposte ancora oggetto di discussione del Cyber Resilience Act e del Cyber Solidarity Act.

A conclusione dell'evento si è quindi ripresentata con forza la domanda: come lavorare insieme per ridurre i rischi legati alla cybersecurity? La priorità per affrontare queste nuove sfide, dal nostro punto di vista, risiede infatti nella collaborazione e nel fare della sicurezza informatica una responsabilità condivisa tra produttori, system integrator e utenti finali, implementando le migliori pratiche e una vigilanza e manutenzione continua, all'insegna della massima trasparenza. Naturalmente, alla luce di quanto detto e della necessità di concepire la cybersecurity come un processo continuo, l'impegno di Axis in questa materia non si ferma di certo qui; al contrario, puntiamo a essere riconosciuti come centro focale nel nostro ecosistema e a dare sempre di più il nostro contributo.

Quest'anno è stata riproposta con forza la questione delle criticità in termini di sicurezza della supply chain, in altre parole della difficoltà delle PMI ad adeguarsi agli standard previsti dalle normative. Dal vostro punto di vista, i vendor possono avere un ruolo per migliorare la situazione?

Uno dei trend più evidenti degli ultimi anni è sicuramente quello della digital transformation di imprese e organizzazioni, in cui si assiste, da un lato, a una sempre maggiore convergenza tra mondo fisico e digitale, con un considerevole ampliamento della superficie di attacco, e, dall'altro, all'emergere di nuove tecnologie come l'AI, l'IoT e il multi-cloud, che creano nuove vulnerabilità per tutti i partner e i fornitori di quello che è ormai un ecosistema interconnesso. Ne deriva che la cybersecurity debba necessariamente essere una priorità a tutti i livelli della catena di collaborazione, dai produttori ai system integrator, fino agli end-user, e naturalmente anche i vendor svolgono un ruolo chiave, offrendo delle soluzioni progettate secondo il principio *secure by default*.

Ciascuno è chiamato a fare la sua parte, in un'ottica di massima trasparenza e collaborazione. Questa è la filosofia che guida anche noi di Axis nello svolgimento delle nostre attività e che ci porta a credere fermamente nel concetto di *shared responsibility.* Soprattutto all'interno di un quadro normativo articolato, che alza i requisiti di sicurezza per le organizzazioni, in particolare per quelle che operano nel segmento delle infrastrutture critiche, la rete di partner e clienti è fondamentale per rispettare gli standard ed essere *compliant*. Questo vale a maggior ragione per le PMI, che possono incontrare maggiori difficoltà nel reperire al proprio interno le risorse necessarie.

E quali potrebbero essere le leve per indurre le PMI ad essere compliant?

Come accennavo prima, le imprese e le organizzazioni non possono essere considerate a sé stanti, ma vanno osservate in quanto parte di un più ampio network, innovativo e digitale, in cui è necessario stabilire un continuativo e proficuo scambio di best practice tra tutti gli attori coinvolti per essere sempre aggiornati sulle normative e rendere le proprie soluzioni il più *cyber-safe* possibile. In questo modo anche le PMI possono trarre vantaggio da un contesto collaborativo, implementando misure di sicurezza più avanzate e diventando più resilienti.

Un altro tema emerso, determinante per le PMI, è quello della formazione, che riguarda sia la necessità di creare nuove figure altamente specializzate sia di diffondere una cultura sulla sicurezza informatica all'interno di tutte le organizzazioni interessate. Le PMI sono, infatti, tendenzialmente più propense a sottovalutare la gravità degli attacchi e la portata dei danni che ne possono derivare, in parte anche per una limitata cultura aziendale sulla tematica. In questo senso, la formazione e la messa a fattor comune delle esperienze degli altri player svolgono un ruolo cruciale nell'incrementare l'awareness sui rischi e sulle migliori best practice da implementare.

Più in generale, è però importante sottolineare come la formazione e l'educazione siano aspetti che interessano trasversalmente tutti gli operatori del comparto, non solo le PMI. Questo perché una delle sfide da affrontare risiede nella ricerca di professionisti con skill e competenze specifiche, verso cui si registra attualmente una forte richiesta, che il mercato non riesce ancora a soddisfare. La componente umana dovrebbe quindi essere una priorità, così che tutti possano agire e diventare loro stessi un fattore di sicurezza.

Dal punto di vista più tecnico invece, per aiutare PMI e non solo, ad essere compliant, noi di Axis e tutte le parti coinvolte nell'evento abbiamo chiarito che la cybersecurity deve essere la priorità assoluta per il management, identificando e comprendendo risorse, sistemi e obiettivi aziendali. Implementare un framework su cui innalzare la sicurezza e gestire il rischio delle risorse e delle operazioni sono i passi successivi. Infine, stabilire un processo di reporting conforme ai requisiti NIS2 e sfruttarlo attivamente contro le minacce.

È riaffiorata anche la questione della security by design dei device, con la questione dell'affidabilità degli stessi vendor. Come si potrebbe divulgare una maggiore consapevolezza presso le centrali di acquisto/procurement?

Certamente la questione della security by design dei device è emersa più volte nel corso dell'evento, come requisito in capo ai vendor per essere riconosciuti come partner di fiducia dagli end customer. Questi ultimi infatti sono i primi a richiedere specifiche e dettagli sulla progettazione delle soluzioni, al fine di assicurarsi che il prodotto di

interesse sia il più sicuro possibile. Una spinta affinché i vendor adottino questo approccio arriva quindi dai loro stessi clienti.

D'altra parte, però, gli end customer, così come i system integrator, devono avere ben chiare le feature di sicurezza di questi prodotti, in modo tale da poterli configurare nel modo più opportuno e adottando le migliori pratiche; quindi, rendere note le best practice, così come i rischi e le debolezze con l'obiettivi di aumentare la consapevolezza della security by design dei device per ogni parte coinvolta, è pertanto un altro fattore rilevante.

In sostanza, come dicevamo, non è solo la tecnologia a impattare sulla sicurezza di un prodotto, ma anche la sua corretta installazione e configurazione, ogni attore è quindi chiamato in causa per far sì che nei vari step si riducano al minimo le vulnerabilità e i rischi che potrebbero subentrare in un momento successivo, qualora non vengano adottate delle procedure adeguate. La parola chiave resta quindi sempre awareness, insieme alla condivisione di conoscenze e best practice.

AXIS COMMUNICATIONS

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