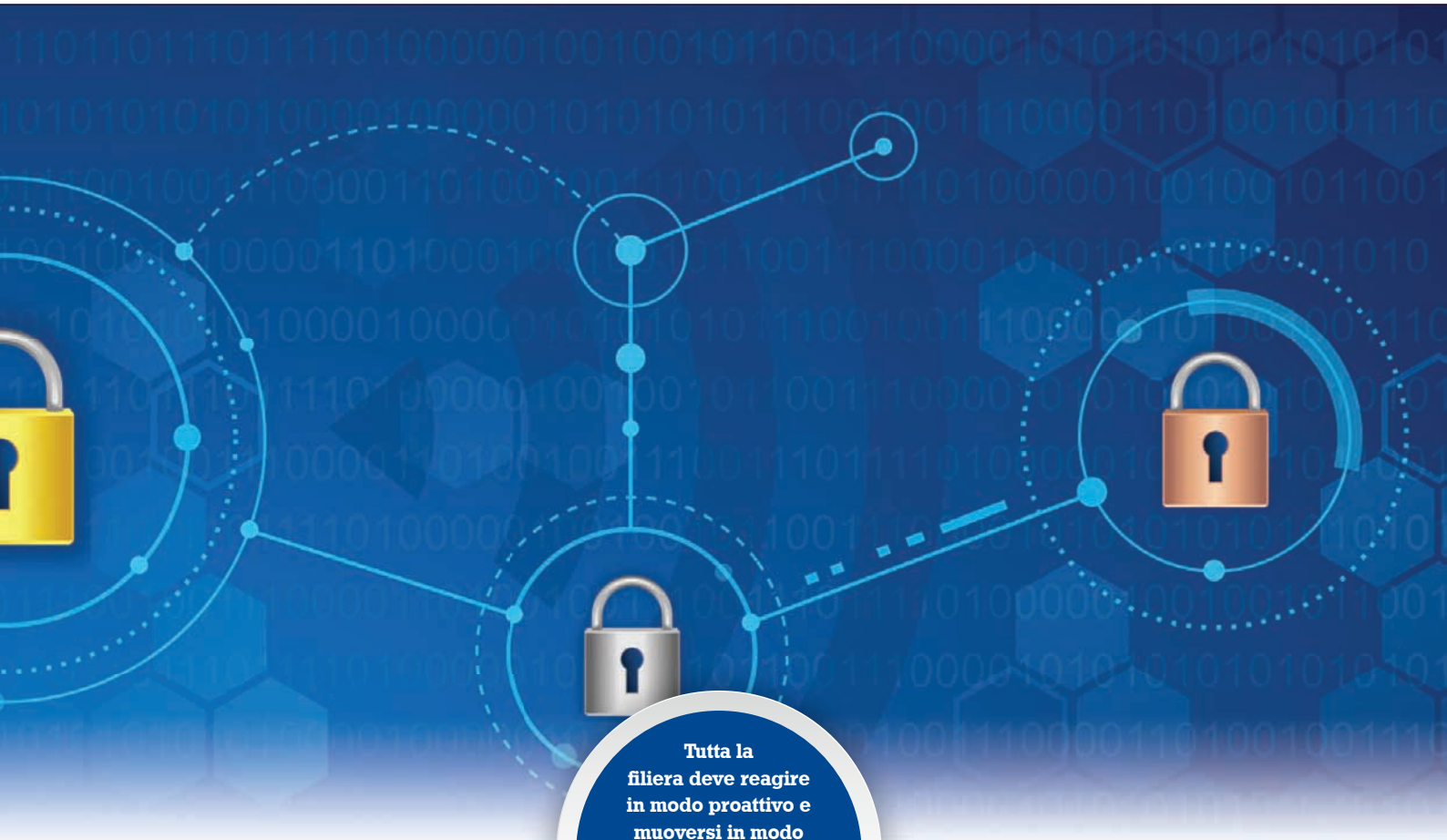
Andrea Monteleone (*)

Sicurezza logica e fisica: due facce della stessa medaglia

La direttiva europea NIS (Network and Information Security), recepita nell'ordinamento italiano nel giugno del 2018, definisce le misure utili a raggiungere un elevato livello di sicurezza delle reti e dei sistemi informativi. Si tratta di un provvedimento destinato ad avere un forte impatto sulla sicurezza logica, ma anche su quella fisica. I due aspetti sono infatti sempre più legati: se l'accesso fisico all'infrastruttura non è difeso, essa diventa di fatto vulnerabile nonostante tutte le protezioni ai sistemi informativi. Gestire, dunque, la sicurezza informatica senza prendersi cura di quella fisica non ha senso e diventa indispensabile trovare un equilibrio che bilanci entrambi gli aspetti.

(*) National Sales Manager Axis Communications **www.axis.com**



Tutta la filiera deve reagire in modo proattivo e muoversi in modo coordinato per raggiungere un livello di consapevolezza diffuso e condiviso

Per riuscire a difendere i propri asset, l'azienda deve quindi prendere in considerazione e analizzare tutta una serie di situazioni fisiche e logiche che riguardano e coinvolgono ogni tipo di attività. Per estensione, questo vale anche per il vendor che, per esempio, è chiamato a controllare tutta la sua catena logistica, a partire dai fornitori di componenti per passare al momento in cui un prodotto esce dagli stabilimenti e arrivare fino all'installazione finale presso il cliente. È in queste fasi di transizione che, spesso, la probabilità di subire un attacco diventa più elevata.

Ambito applicativo

La Direttiva NIS si rivolge a tutte le realtà che operano nell'ambito dell'erogazione dei servizi essenziali come la produzione e la distribuzione di energia, il trasporto su gomma, rotaia, acqua e aria (compresi gli aeroporti), la gestione dell'acqua, le banche, i data center e gli ospedali. Su questi mercati verticali la direttiva europea impone di mettere in atto scelte e valutazioni in merito alla sicurezza nella gestione e nell'utilizzo di tutte le infrastrutture ICT, a ogni livello. Nello specifico, parliamo di software e hardware che fanno parte delle infrastrutture di rete, ma anche delle persone che li gestiscono, li utilizzano, li implementano e li manutengono. È importante osservare che le aziende sono chiamate ad adeguarsi ai nuovi paradigmi di sicurezza e che, al contempo, esse devono pretendere che i loro fornitori adottino sistemi analoghi, uniformandosi al nuovo contesto. A cascata, allora, l'intera filiera di fornitura è chiamata a reagire in modo proattivo per riuscire a muoversi in modo coordinato, con l'obiettivo di raggiungere un livello di consapevolezza ampiamente diffuso e condiviso.

Direttiva europea NIS (Network and Information Security), recepita a giugno 2018: definisce le misure atte a raggiungere un alto livello di sicurezza di reti e sistemi informativi

Siamo pronti?

La domanda a questo punto è: il comparto della sicurezza fisica è pronto? In verità la strada è ancora lunga. Oggi, infatti, osserviamo che il comparto della sicurezza fisica non è pronto. In questo settore i responsabili della sicurezza fisica sono ancora lontani dal possedere le necessarie competenze informatiche. Viceversa chi è esperto di sicurezza informatica non conosce gli aspetti chiave della sicurezza fisica. In questa fase siamo invece chiamati a gestire le due cose come un tutt'uno. Occorre lavorare per fare sì che i due approcci si allineino e condividano best practice e knowhow.

Coinvolgere le figure chiave

In aggiunta, diventa sempre più importante il coinvolgimento delle figure aziendali che gestiscono le tematiche di security sui tavoli dove si discutono le scelte strategiche delle imprese. Non è ancora chiaro, o forse lo sta diventando in questi mesi a valle di tutti gli attacchi andati a buon segno, come gli investimenti in security possano avere un impatto enorme in termini di protezione della reputazione del brand o della fiducia che la clientela ripone in un certo fornitore. Emerge chiaramente, quindi, come scelte oculate ed investimenti strategici in ambito security, che garantiscano alle aziende elementi come la scalabilità, l'utilizzo di protocolli non proprietari e la facilità di integrazione, siano diventati tassativi.

Basta tuttologi

Allo stesso modo si deve guardare alle professionalità attualmente disponibili: pensare ad un one-man-band che sia in grado di governare questo livello di complessità è impensabile, al contrario è necessario traguardare al futuro facendo dialogare tutte gli attori coinvolti su tavoli che, per natura, saranno multidisciplinari. Su questi tavoli si costruirà la distribuzione delle responsabilità, come previsto dalla normativa, non nell'accezione di diminuzione del rischio che si corre in prima persona, ma al contrario nel senso del contributo di tutti verso livelli di sicurezza sempre più elevati.

Sicurezza fisica e logica andrebbero gestite come un tutt'uno e invece:

- **i responsabili della sicurezza fisica non hanno le necessarie competenze informatiche**
- **i responsabili della sicurezza informatica non conoscono gli aspetti chiave della sicurezza fisica**