Una nuova visione sulla cybersecurity: un approccio integrato di filiera per una crescita sicura del settore Energy & Utilities

a cura della Redazione

Il settore energetico, da sempre uno tra i comparti più importanti di un Paese, tanto da dover essere considerato una vera e propria infrastruttura critica, ha come obiettivo principale quello di garantire una capacità di fornitura sempre al 100%. Ma come fare ad assicurare che ciò avvenga se, secondo i dati dell'Associazione Italiana per la Sicurezza Informatica, in Italia i *cyber-attacchi* alle infrastrutture critiche sono aumentati dell'85% solo nel primo semestre del 2020?

Per far fronte all'aumento di questo tipo di minacce, diventa fondamentale incrementare e ottimizzare gli investimenti in sicurezza informatica che rappresentano un complemento ormai necessario degli investimenti in innovazione e nuove tecnologie.

In qualunque filiera del settore energetico, grazie all'applicazione tecnologica, si è potuto implementare un monitoraggio da remoto proattivo che offre migliore efficienza per un maggiore vantaggio competitivo sul mercato, ma che porta con sé anche un aumento delle criticità in tema *cybersecurity*.

È chiaro, infatti, come se da un lato l'introduzione di nuovi sensori e dispositivi connessi permetta di riconoscere difetti e malfunzionamenti di sistemi e macchinari, dall'altro, aumentino i rischi legati alla necessità di mantenere sicuri e protetti i dispositivi e i sistemi informatici su cui viaggiano informazioni sensibili.

In un ambiente digitale in continua evoluzione, non esiste un'unica soluzione ai problemi di *cybersecurity*, anche alla luce di un panorama che vede gli attacchi farsi ogni giorno più originali, imprevedibili e sofisticati. Ciò che oggi è necessario è l'individuazione di *partner* affidabili in cui tutti i membri della filiera o della *supply chain* – subfornitori, produttori, installatori, integratori e utenti finali – abbiano un ruolo chiaro e ben preciso e siano aperti ad un confronto costante in ottica di implementazione di sistema.

Ed è proprio il principio di responsabilità condivisa che emerge con forza dal costrutto normativo della NIS con cui vengono definiti i nuovi standard di sicurezza da rispettare. La Direttiva NIS, che si rivolge principalmente al comparto delle infrastrutture critiche, pur stabilendo i parametri da seguire, non entra nel merito su come fare per raggiungere tali standard, imponendo, quindi, in maniera implicita alle aziende una collaborazione tra tutti gli attori coinvolti con l'obiettivo di mettere a sistema in maniera integrata ogni aspetto.

Uno dei concetti chiave su cui tutti sono chiamati ad impegnarsi è quello di "salute informatica", vale a dire la capacità di un sistema di essere protetto e resiliente nei confronti di possibili violazioni da parte di malintenzionati o di errata gestione da parte di coloro che ne hanno accesso. Solo attraverso un'analisi continuativa dei processi con nuovi strumenti di gestione dei dispositivi le aziende possono visualizzare lo stato del loro ecosistema, in tempo reale e in modo approfondito.

L'introduzione di procedure mirate, una costante verifica dei firmware di tutti i dispositivi connessi alla rete, a

partire dai sensori, e la capacità di affidarsi a *partner* tecnologici esperti nelle strategie di mitigazione dei rischi informatici sono alcuni dei fattori determinanti con cui il settore *Energy&Utilities* può ridurre il più possibile i rischi di attacchi *cyber*.

Per i produttori energetici diviene essenziale, oltre ad individuare le soluzioni più adatte alle loro esigenze, concentrarsi sulla maturità della sicurezza informatica delle imprese all'interno della loro catena di approvvigionamento. Solo in questo modo si troveranno in una posizione di forza per trarre vantaggio dalle soluzioni tecnologiche emergenti, con effetti positivi non solo sulla sicurezza, ma anche sulla gestione e sul monitoraggio di tutte le operazioni aziendali.

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