Axians

Verso una PA cyber-sicura

Il modello Axians per la protezione del dato pubblico

Il modello a "silos", in un momento in cui non era ancora matura una visione di servizio pubblico integrato, ha avuto il merito di dare l'avvio ad importanti progetti di informatizzazione nella Pubblica Amministrazione, permettendo ai singoli dipartimenti di muoversi in autonomia in funzione di esigenze, tempi e risorse disponibili, con un approccio che, sebbene a macchia di leopardo, ha contribuito a portare innovazione.

Questo approccio con il passare degli anni ha manifestato tutti i suoi limiti, ma il modello a "silos" è un retaggio del passato e la Pubblica Amministrazione ha iniziato da tempo ad adottare paradigmi ICT basati sull'integrazione e sullo scambio dei dati.

Uno degli ambiti che ha tratto maggior vantaggio da questo approccio è la cybersecurity, poiché il presidio degli aspetti di sicurezza del dato in un contesto a "silos" è estremamente complesso e dispendioso in termini di risorse e strumenti, nonché poco efficace.

Oggi i nostri clienti della Pubblica Amministrazione gestiscono sistemi informativi eterogenei, composti da soluzioni e tecnologie diverse e integrate, e ci chiedono di poter fruire di servizi e soluzioni in ambito cybersecurity che garantiscano loro una visione completa, univoca e aggiornata delle minacce.

Francesco Pirastu
key account manager public administration Nord
di Axians Italia

Conoscere il livello di esposizione ad un potenziale attacco esterno ed avviare le azioni necessarie a minimizzarne l'impatto in anticipo. Questo è uno dei bisogni che sempre più cogliamo dagli IT manager che si rivolgono a noi.
La risposta di Axians è il servizio di Cyber Threat Intelligence (CTI) che si basa sulle più moderne soluzioni di EASM (External Attack Surface Management) e gestisce in toto i processi di monitoraggio della superficie di attacco esterno dell'ente. Il servizio, interamente gestito ed erogato in modalità reattiva e con copertura H24, avvisa l'IT manager ed eventualmente interviene nel caso di data breach (siano esse presenti nel dark e nel deep web), tentativi di whale-phishing, presenza di vulnerabilità critiche o credenziali e email compromesse.

Un secondo aspetto critico per l'IT manager (rif. Misure minime di sicurezza ICT per le pubbliche amministrazioni) è relativo alla gestione degli asset, al loro aggiornamento e alla presenza di eventuali vulnerabilità che possano essere sfruttate da un potenziale attaccante. Axians risponde a questa esigenza con un servizio di Vulnerability Management gestito dal nostro SOC operativo H24. Attraverso l'utilizzo di soluzioni di ultima generazione e con l'ausilio di professionisti certificati vengono monitorati costantemente gli asset dell'ente, gestito l'inventario, verificate in real-time le vulnerabilità presenti (siano esse relative a mancanti aggiornamenti o, per esempio, certificati in scadenza o scaduti) e se necessario attuate, secondo gli accordi con il cliente, le relative attività di mitigazione o di patch management.

Il modello Axians per la protezione del dato pubblico consente quindi all'ente di focalizzarsi sul miglioramento dei processi e dedicare le sue risorse interne ad attività di evoluzione e miglioramento del proprio sistema informativo, affidando i suoi servizi di cybersecurity all'esperienza di un partner leader del settore.

axians
www.axians.it