L’Identity Governance come difesa dagli insider threat: il caso di Notartel

Author : Redazione

Date : 12 Novembre 2019

Le statistiche evidenziano che a livello mondiale circa il 30% degli incidenti di sicurezza e dei data breach sono attribuibili ad “insider threat”, cioè minacce interne all’organizzazione.

Notartel, una realtà che dal 1997 realizza e gestisce servizi informatici e telematici per i notai italiani, grazie al supporto di **Par-Tec**, software & infrastructure system integrator con 20 anni di esperienza nel mercato delle telco e della finanza on-line, ha implementato una piattaforma per la corretta gestione del ciclo di vita delle identità digitali e il monitoraggio delle attività svolte dagli utenti privilegiati.

Stefano Tufoni, Responsabile IT Operations di **Notartel**, spiega che “*pur non avendo mai fronteggiato situazioni di questo tipo, sappiamo quanto sia importante curare il “fattore umano”, facendo convergere regole, comportamenti e tecnologie. Siamo partiti dalla definizione di ruoli, responsabilità e competenze all’interno dell’organizzazione, evitando di creare degli utenti con privilegi illimitati che possono commettere errori in buona fede o diventare vittime pregiate (in caso di furto d’identità). Il passo successivo è stato tradurre il tutto in un set di policy e automatismi da applicare mediante strumenti ad hoc*”.

Riccardo Fiano, Sales Manager di **Par-Tec**, spiega che “*sul fronte della tecnologia, uno dei momenti chiave del progetto è stata l’adozione delle appliance Safeguard di One Identity utilizzate per monitorare, memorizzare ed analizzare le attività svolte dagli utenti privilegiati. La soluzione è stata poi integrata con un modulo che automatizza ed irrobustisce i processi di autenticazione, introducendo ad esempio l’autenticazione a due fattori ed i workflow autorizzativi*”.

Massimiliano Micucci, Sales Executive di **One Identity**, prosegue dicendo: “*Notartel, come molte altre realtà del mercato telco, ha ben compreso i vantaggi offerti da una piattaforma integrata di questo tipo. Seppur con una scala diversa, anche negli altri mercati riscontriamo la necessità di assegnare ruoli e privilegi, evitare accessi anonimi e non tracciati, comprendere chi ha fatto cosa a seguito di un incidente di sicurezza. Questo è ancora più vero in un’epoca in cui*

una normativa come il GDPR impone modalità e tempistiche precise per la notifica di un data breach”.

Nel corso del **Forum ICT Security 2019**, Riccardo Fiano e Stefano Tufoni hanno illustrato le fasi del processo di adeguamento. La presentazione integrale è ora disponibile sul Centro Risorse del sito Par-Tec.