



Tecnologia - Axitea: l'identity management come fondamento della digital trust

Roma - 20 dic 2021 (Prima Pagina News) Andrea Lambiase, Head of Management Consulting e Data Protection Officer di Axitea, riflette sull'importanza di una strategia avanzata di gestione delle identità in azienda.

Oggi la fiducia è il fattore che determina il successo delle strategie di business e controllo dell'evoluzione tecnologica delle imprese, ma allo stesso tempo la dimensione, il numero e la frequenza delle violazioni dei dati sono talmente rilevanti e diffuse da porre a dura prova l'affidabilità di identità digitali sempre più diffuse. Tuttavia, è possibile adottare un approccio di "sicurezza allargata" per quanto riguarda i domini di dati, internet e IoT, integrata dal punto di vista della disposizione delle funzionalità d'accesso, di autenticazione e "deprovisioning" per l'organizzazione, in modo da poter tenere i sistemi sempre sicuri. A dirlo è Andrea Lambiase, Head of Management Consulting e Data Protection Officer di Axitea. "Qualsiasi transazione commerciale si basa sulla fiducia. Il concetto elaborato dall'economista premio nobel Kenneth Arrow è oggi più vivo che mai, e trova nella nozione di "digital trust" la sua ultima versione e al tempo stesso la sua crisi più profonda", dice. "Mai come oggi la fiducia è così determinante per il successo e lo sviluppo delle strategie di business e di controllo dell'evoluzione tecnologica delle aziende; ma mai come oggi, al contempo, la dimensione, il numero e la frequenza delle violazioni dei dati sono state così rilevanti e diffuse, ponendo a dura prova l'affidabilità di identità digitali sempre più decentralizzate, diffuse e predabili", aggiunge. "Eppure, anche in un contesto così critico, una soluzione è possibile: un approccio di sicurezza allargata, dal punto di vista dei domini di dati, internet e IoT, ed integrata dal punto di vista dell'orchestrazione delle funzionalità di accesso, di autenticazione e di "deprovisioning" per tutta l'organizzazione, al fine di poter mantenere i sistemi sicuri in ogni fase del ciclo di vita dell'utente", evidenzia. E' necessario, dice ancora Lambiase, attivare funzionalità avanzate per quanto riguarda la gestione delle identità e degli accessi: "In un momento in cui le organizzazioni stanno realizzando il potenziale e le capacità del cloud adottando sempre più servizi cloud-based per il proprio IT (in qualunque configurazione e specialmente in un contesto ibrido), la sicurezza dell'identità è stata spesso paradossalmente trascurata, generando un terreno fertile per cyberattacchi esterni, minacce interne e data breach di natura diversa che nel 2020, nella sola Italia, sono stati identificati e affrontati dal Garante per la privacy nell'ordine del migliaio. Ed è proprio in questo nuovo panorama che funzionalità avanzate di gestione dell'identità e degli accessi diventano sempre più urgenti, emergenti e diffusi anche in settori trasversali dell'economia, superando spesso i confini dimensionali a cui approcci più tradizionali e datati e certamente meno "disruptive" ci avevano abituato". "In altri termini, si parla di sistemi di Identity Access Management,



piattaforme con cui diventa possibile decidere quali utenti abbiano accesso a quali dati, con che tempistiche e per quali ragioni specifiche, con l'obiettivo di identificare un utente, autenticarlo e autorizzarlo all'accesso secondo il profilo e ruolo di una sua identità digitale che deve essere mantenuta, modificata e monitorata in ogni momento del ciclo di vita del procedimento di accesso. Ma non solo: i requisiti e le sfide di una gestione allargata, multi source / domain (IT, IoT) e di vasta scala (Internet-driven) hanno oggi dato vita a veri e propri sistemi di Identity Governance and Administration, che permettono di definire e attivare policy e funzionalità IAM in ottica compliance, riuscendo nell'arduo compito di gestire in maniera automatica tutte le attività relative alla creazione, disabilitazione, modifica degli accessi e dei loro profili, per ciascuna persona all'interno dell'organizzazione, con riferimento tanto ai dipendenti quanto a parti esterne". Per quanto riguarda il futuro dell'Identity Management, conclude Lambiase, "Quello che emerge oggi è uno scenario evolutivo e proattivo di revisione del processo di gestione dell'accesso, realizzato attraverso approcci e metodologie che privilegiano attività di assessment organizzativo e di rimodulazione dei profili utenti, abilitato dal potenziamento di funzionalità di sistemi già presenti in azienda o dall'introduzione di soluzioni innovative con funzionalità native orientate all'automazione. Per tutti, questa nuova convergenza tra dati, accesso e sicurezza come piattaforma irrinunciabile per lo sviluppo ed il controllo, rappresenta una ulteriore e significativa occasione per una reingegnerizzazione più profonda ed estesa dei servizi IT e delle logiche di sicurezza. In quest'ottica, la parola d'ordine sembra essere una sola: rendersi affidabili diffidando di tutti".

di Giuliano Risi Lunedì 20 Dicembre 2021