Zero Trust per tutti, Mainframe incluso



Abstract:

La sicurezza moderna impone scelte architetturali che possano reggere agli attacchi più persistenti e sofisticati. Zero-Trust è diventata la parola d'ordine soprattutto quando si opera su sistemi aperti ed eterogenei dove i confini operativi diventano sempre meno nitidi mettendo a dura prova i reparti di sicurezza sia logica che fisica di ogni infrastruttura IT. Una parola d'ordine che si trasforma in una strategia che deve essere applicata in ogni contesto, incluso quei mondi tradizionali dove il mainframe agisce da cuore pulsante per il proprio business

E Cloud fù!

Già, pare proprio che tutto il mondo digitale guardi con un certo interesse alle continue evoluzioni in quest'area. E pensare che l'idea del cloud risale a quando il mainframe IBM ha cominciato a fare la voce grossa sul mercato dell'Information Technology. Parliamo degli anni '60 quando l'informatico statunitense John McCarthy introdusse il concetto di "utilità pubblica" dell'IT, primo vero embrione del cloud. La stessa IBM in quegli anni (nel 1964 circa) sfornava il suo scintillante System/360 che dava il via ad un percorso importante per tutte quelle aziende che si attrezzavano di informatica, fino ad arrivare al giorno d'oggi dove il mainframe è diventato System Z e continua a viaggiare a "testa alta" in mezzo alle "nuvole".

Ricordo come gli uffici aziendali traboccavano di terminali 3270 con cui si instaurava un rapporto di fiducia, come

fossero veri e propri compagni della giornata lavorativa. Ora non è più così. Il mondo è cambiato ma nonostante tutto il mainframe è ancora lì al centro di molte realtà aziendali. Non a caso le più importanti aziende mondiali custodiscono i loro dati su questa piattaforma che conferisce i più alti livelli di sicurezza, affidabilità e resilienza ancor oggi ineguagliati. Ma anche il vecchio e caro mainframe ha dovuto cambiare, ha dovuto modernizzarsi riposizionandosi sul mercato e cercando di ricoprire ancora il ruolo di attore principale per quel nuovo mondo definito come Hybrid-Cloud.

Un nuovo mondo dove gli utenti accedono al mainframe tramite laptop, tablet o via smartphone. Si accede spesso da remoto, con connessioni private (VPN) oppure utilizzando direttamente delle API (Application Program Interface) veicolo fondamentale per ogni architettura Hybrid-Cloud. Basta fare l'esempio del gateway IBM z/OS Connect, che indirizza buona parte della trasformazione digitale in ottica Hybrid-Cloud.

E per quanto riguarda la sicurezza?

Generalmente l'immagine fossilizzata negli occhi di molti riporta al concetto del castello accerchiato da mura invalicabili. Il mainframe era posizionato lì, costituiva il centro del castello, dove le aziende custodivano e proteggevano tutte le loro preziose risorse. Un castello fondato su un disegno progettuale che ancora oggi regge agli urti tecnologici, adeguandosi e modellandosi alla continua trasformazione a cui tutti noi siamo sottoposti.

Ma fuori dalle mura del castello vi erano numerose richieste di accesso per poter usufruire dei servizi messi a disposizione dalla piattaforma. I flussi in ingresso venivano regolamentati con protocolli di comunicazione, inizialmente proprietari (SNA) per poi aprirsi al tcp/ip, che conferivano certezza e sicurezza in quanto consentivano di identificare e verificare la presenza di malintenzionati che cercavano di entrare nel castello, mentre in fase di uscita occorreva

controllare che nessun oggetto prezioso fosse sottratto dal castello. Tutto questo aveva certamente un senso dal momento che si riteneva che “i cattivi” si trovassero solo all’esterno.

Nel mentre, però, il mondo cambiava e tutto ciò evidenziava forti limitazioni soprattutto per ciò che riguarda la fruibilità della merce più preziosa: il dato. La necessità di superare questa limitazione ha fatto si che i muri fossero abbattuti, o perlomeno abbassati, e che i confini diventassero sempre meno definiti e gradualmente sostituiti dal concetto di perimetro in cui però le minacce diventavano sempre più numerose rispetto al passato.

Basta guardare oggi nel Dark Web dove è presente un volume impressionante di dati personali di cui, la maggior parte, è stata sottratta proprio dall’interno di questo perimetro. E subito viene in mente uno dei pericoli più temuti, l’attacco ransomware che ha l’obiettivo di esfiltrare i dati, corrompendo i loro backup e poi crittografandoli per richiederne riscatto. Ma anche il phishing continua a fare la sua parte. Le aziende sono ben consapevoli che il personale, indipendentemente dalla formazione ricevuta, possa fare click su link sospetti oppure inserire dati personali in “forms” inopportuni.

Questo per dire come, all’interno del perimetro o delle vecchia mura del castello, esista il pericolo costituito dal personale a volte deluso e scontento, a volte non considerato e che potrebbe sottrarre o corrompere dati importanti. A volte succede per errore o per negligenza, come il caso in cui si pensa di avere diritto a una copia dei dati di cui si è stati artefici della creazione. Sembrerebbe naturale chiedersi che cosa ci sia di sbagliato se quei dati dovessero risultare utili per un prossimo impiego. Se vogliamo, è un pò come portarsi con sè il proprio portfolio di clienti affezionati quando si cambia azienda di lavoro.

Ma accanto a questi casi si verificano sempre più forme intenzionali di sottrazione di dati. Indice che le mura del castello o che il perimetro disegnato non risulta più efficiente o perlomeno non è più significativo, in quanto quasi la metà dei cattivi, si trova già al suo interno. E' infatti abbastanza comune, navigando in internet, imbattersi in tabelle e grafici che mostrano studi di "Cost of a Data Breach" dove si rileva che circa il 52% delle violazioni è originato dall'esterno, ma il 48% è perpetrato dall'interno!

In che modo ? Il metodo più efficace di tutti risulta sempre l'attacco alle identità. Ad esempio, ancora oggi in molte aziende si fa uso della semplice autenticazione basata sulla sola password, e carpire una password con le tecnologie odierne non è più così difficile come lo poteva essere negli anni passati. Quindi, riassumendo, abbiamo personale con ruoli di fiducia che risulta demotivato, scontento e che lavora anche da remoto utilizzando diversi dispositivi per l'accesso ai dati. Ora, in queste condizioni, c'è realmente da fidarsi ? La risposta la danno i massimi esperti del settore: no, non bisogna fidarsi di nessuno,

Zero-Trust

Secondo Gartner, non dobbiamo fidarci di nessuno che tenti di accedere ai sistemi e ai dati, né di alcun dispositivo che può essere utilizzato per il loro accesso, né di alcuna applicazione. Sono le basi per un'architettura "Zero Trust".

Come reazione assistiamo ad una corsa affannosa verso la crittografia dei dati, memorizzati su supporti fisici (At-Rest), oltre a tutti i dati inviati sulla rete (In-Fly) che devono essere crittografati per fermare possibili attacchi come il famoso Man-in-the-Middle.

Secondo l'architettura "Zero-Trust", le persone devono eseguire sempre la propria autenticazione per superare i controlli di accesso, con una valutazione continua della

fiducia, che si basa su chi sei, dove sei e cosa stai facendo e con l'eventuale identificazione di ogni anomalia comportamentale. Fino ad arrivare ai controlli adattivi, cioè quei controlli sensibili al contesto in cui si agisce, in modo da tarare il livello di fiducia contro ogni possibile rischio.

Il NIST (National Institute of Standards and Technology), fornisce l'indicazione di come l'accesso adattivo risulti una forma di controllo caratterizzata da una politica di autorizzazione che tiene conto delle necessità operative, del rischio e dell'euristica.

Ed è sempre il NIST che traccia le linee guida per una "Zero Trust Architecture". La sua pubblicazione documenta la storia di Zero Trust, le sue basi, i componenti logici e gli scenari di implementazione con casi utente.

Seguendo questa strategia la tecnologia interviene in aiuto fornendo l'autenticazione a più fattori (MFA), soluzione subito adottata da diverse organizzazioni ed aziende per l'accesso sicuro ai sistemi, dispositivi e dati presenti sulle piattaforme più comuni.

Già, ma al buon vecchio mainframe non ci pensa più nessuno ?

Con una imponente gestione di dati memorizzati e così tante transazioni in esecuzione su di esso al minuto, per non pensare alle sue integrazioni con dispositivi mobili ed interazioni con i mondi cloud, è lecito chiedersi se abbia senso adoperarsi per renderlo davvero il più sicuro possibile, oppure no.

Magari ingenuamente pensiamo che attuando la MFA a livello perimetrale o dipartimentale risulti sufficiente per assicurare l'accesso ai dati che risiedono sul mainframe. E tutto ciò che abbiamo detto sugli attacchi interni ? Forse vale la pena riconsiderare la situazione. Ancora oggi sono molte le aziende che non considerano l'attuazione della multi-factor-authentication sui sistemi mainframe, spesso "core" del

loro business, eppure zMFA esiste da tempo e funziona egregiamente proprio secondo la logica “Zero-Trust”.

Una logica pronta per essere applicata nell’architettura del mainframe che risulta già ben posizionato secondo i più noti modelli di accesso RBAC (Role Based Access Control) e MAC (Mandatory Access Control). Ora, con Zero-Trust, è possibile fare in modo che gli utenti autorizzati possano accedere ad una risorsa o applicazione mediante i privilegi sufficienti per svolgere il proprio lavoro, niente di più. Tutto ciò deve avvenire senza alcun rischio che le persone abbiano un livello di privilegio troppo elevato vista anche la possibilità di essere associati a diversi ruoli operativi.

Allora si che risulterebbe possibile rendere la vita difficile ad ogni hacker di questo tempo. Occorre una scelta forte e decisa come “Zero Trust”, scelta da considerare seriamente se si vuol rendere il nostro castello, il mainframe, ancora il posto più sicuro per i propri dati.

Articolo a cura di **Luigi Perrone**

https://www.ictsecuritymagazine.com/articoli/zero-trust-per-tutti-mainframe-incluso/