Sicurezza col Mainframe? Una scelta strategica



Siamo nell’era della completa trasformazione, a partire dai cambiamenti climatici alla moneta digitale, senza dimenticare la pandemia che ha indotto un’accelerazione verso il mondo cibernetico, dove non si tocca più nulla di concreto ma sono sufficienti dei click, i riconoscimenti vocali, facciali e comportamentali, vero carburante per la nuova intelligenza artificiale. Nonostante ciò, troviamo ancora i sistemi Mainframe al centro della scena, come a fare eco alla canzone del “Blasco” che ribadisce “Io sono ancora qua, eh …. già”.

Eh già, il tutto è palesemente dimostrato dal fatto che il mainframe continua ad essere la piattaforma capace di macinare grandissime quantità di dati in totale sicurezza in un’epoca dove i dati crescono a dismisura e dove la loro salvaguardia diventa l’obiettivo primario per tutti. Si rimane ancora sbalorditi nel sentire come il nuovo IBM z15 sia capace di gestire ben 19 miliardi di transazioni crittografate al giorno, ad una velocità di circa 220.000 al secondo. Potenze difficili da riscontrare nell’intero panorama dell’Information Technology.

Sono forse questi i motivi per cui i mainframe continuano ad essere costantemente aggiornati e mantenuti da quelle organizzazioni ad alta intensità di informazioni come ad esempio quelle finanziarie?

Per ora non abbiamo una risposta inequivocabile. Ciò che invece risulta evidente in questa trasformazione digitale è la spinta verso una rivalutazione dei propri sistemi mainframe con l’unica prospettiva del contenimento dei costi, a volte ammaliati dalle tecnologie in cloud, spesso perdendo di vista tutti gli altri aspetti che non possono e non devono essere

considerati secondari proprio nell'ottica di riduzione della spesa. Uno su tutti? Il pericolo che ci tormenta tutti i giorni relativo al rischio economico e finanziario in caso di una perdita di dati.

Ma allora cosa fare?

Cosa ha più senso sia dal punto di vista economico che per la sicurezza dei dati? Aggiornare il Mainframe ad una versione più recente dell'hardware esistente o, meglio, sostituirlo passando completamente ad una nuova piattaforma? Navigando nel web è facile imbattersi in studi specialistici che denotano come una leggera maggioranza delle organizzazioni mondiali abbia preferito effettuare l'upgrade piuttosto che il replatforming.

Eppure, sembra spontaneo pensare che i costi dell'hardware nel modernizzare il mainframe risultino più onerosi rispetto al replatforming, in quanto il passaggio ad un sistema distribuito debba, per forza di cose, costare meno rispetto all'acquisto dell'ultimo Z system. E se non fosse proprio così? A far bene i conti, pare che i costi dell'hardware risultino persino equiparabili, almeno nella fascia che va dai 400.000$ ai 2.000.000$. Ma a quanto ammontano i costi del downsizing in termini di software, personale, consulenza e interruzioni varie della disponibilità dei servizi? Il passaggio da una piattaforma all'altra comporta un netto cambiamento di procedure consolidate, funzionali e di routine a favore di uno svecchiamento delle stesse, ma con la grande incognita delle nuove problematiche e conseguenze economiche che questo cambiamento comporta.

E dal punto di vista della sicurezza?

Proviamo a pensare alla semplice installazione di programmi o applicazioni. Un'attività che è all'ordine del giorno per i sistemi distribuiti, persino alla portata di un utente finale se parliamo di sistemi perimetrali. Ed è proprio durante

questa attività che molti malware, ransomware compreso, agiscono travestendosi da app legittime ingannando facilmente gli utenti.

Sul mainframe la maggior parte degli utenti non può installare applicazioni in maniera autonoma! Non è altrettanto possibile leggere email o navigare sul web annullando ogni rischio di clic su link insidiosi o apertura di allegati sospetti. Inoltre, se qualche intruso riuscisse comunque a veicolare un malware, quest'ultimo per poter funzionare su z/OS, dovrebbe essere stato sviluppato appositamente per il sistema operativo z/OS, in quanto la maggior parte dei malware che troviamo nel mondo distribuito non funzionano sul mainframe.

Tutta la strategia di prevenzione che viene orchestrata nel mondo distribuito tramite sistemi di logging, monitoring ed alerting, sul mainframe è già a disposizione, tant'è che se accade qualcosa di sospetto risulta difficile mistificarlo. Il mainframe registra automaticamente ogni singola azione di ogni utente, senza possibilità di nascondere una possibile cancellazione di quel record. Ciò significa che se accade qualcosa di anomalo risulta improbabile non accorgersi tempestivamente, sempre che siano state attivate tutte le soluzioni di sicurezza offerte dal sistema, come l'alerting in real-time, magari integrato con un sistema SIEM.

E cosa dire sullo Zero-Trust? Concetto che è già insito nel Security Server (RACF) che regola la sicurezza sul mainframe. A partire da un'autenticazione a più fattori che abbatte ogni tipo di rischio di uso improprio delle credenziali, fino ad arrivare alla concessione di permessi e privilegi minimi indispensabili. La maggior parte degli utenti ha zero autorizzazioni per modificare qualsiasi cosa sul mainframe, se non appositamente concesse e monitorate. L'ereditarietà dei permessi viene inibita da un'azione di revoca delle ridondanze presenti nel sistema. Ed è sempre il RACF che regola l'accesso anche dai servizi esterni. Tutte le applicazioni di terze parti non hanno accesso al sistema se non appositamente

concesso e controllato. Ciò elimina uno dei percorsi più comuni per gli hacker, che spesso attaccano i sistemi più deboli per ottenere l'accesso instaurando una backdoor che gli consente di arrivare all'obiettivo più prezioso: il dato.

Ed è proprio nel tutelare i dati che il mainframe mette a disposizione una tecnologia di encryption all'avanguardia, di tipo pervasivo, proprio per proteggere il dato in qualsiasi stadio esso si trovi (at-rest, in-fly, in-use). Tecnologia che non richiede investimenti in nuovi server o software aggiuntivi con l'ulteriore costo di gestione e manutenzione. Insomma, di questi tempi dove i nostri preziosi dati sono in balia di attacchi informatici in continuo aumento e dove le spese devono essere oculate, credo sia un grave errore non prendere in considerazione i benefici che può portare la modernizzazione della piattaforma mainframe anche in un contesto hybrid-cloud. Piattaforma che garantisce la massima affidabilità e la massima sicurezza per le persone ed i dati di ogni azienda, con conseguenti risparmi economici. Proprio come il vecchio Vasco che non passa mai di moda "eh già, io sono ancora qua!"

Articolo a cura di **Luigi Perrone**

https://www.ictsecuritymagazine.com/articoli/sicurezza-col-mainframe-una-scelta-strategica/