Impatto della Brexit sulle identità con privilegi

Mentre il Regno Unito e il resto dell'Europa si preparano per la Brexit (l'uscita della Gran Bretagna dall'Unione Europea), gli esperti in protezione delle informazioni si stanno chiedendo quali saranno le conseguenze sui processi di gestione di sicurezza e rischi implementati in passato e cosa fare per adattarli alla nuova realtà. In questo documento vengono analizzati l'impatto della Brexit sul privileged access management e le informazioni che gli esperti di sicurezza devono prendere in considerazione per trovare soluzioni immediate di contenimento dei rischi.

Brexit - Il passo successivo

Il processo ufficiale di abbandono dell'Unione Europea (UE) è iniziato con la notifica formale dell'uscita del Regno Unito (UK, United Kingdom) da parte del Primo Ministro Theresa May. È prevista una finestra di 24 mesi in cui entrambe le parti devono creare un framework in cui collaborare. Tale processo è illustrato nel seguente diagramma.

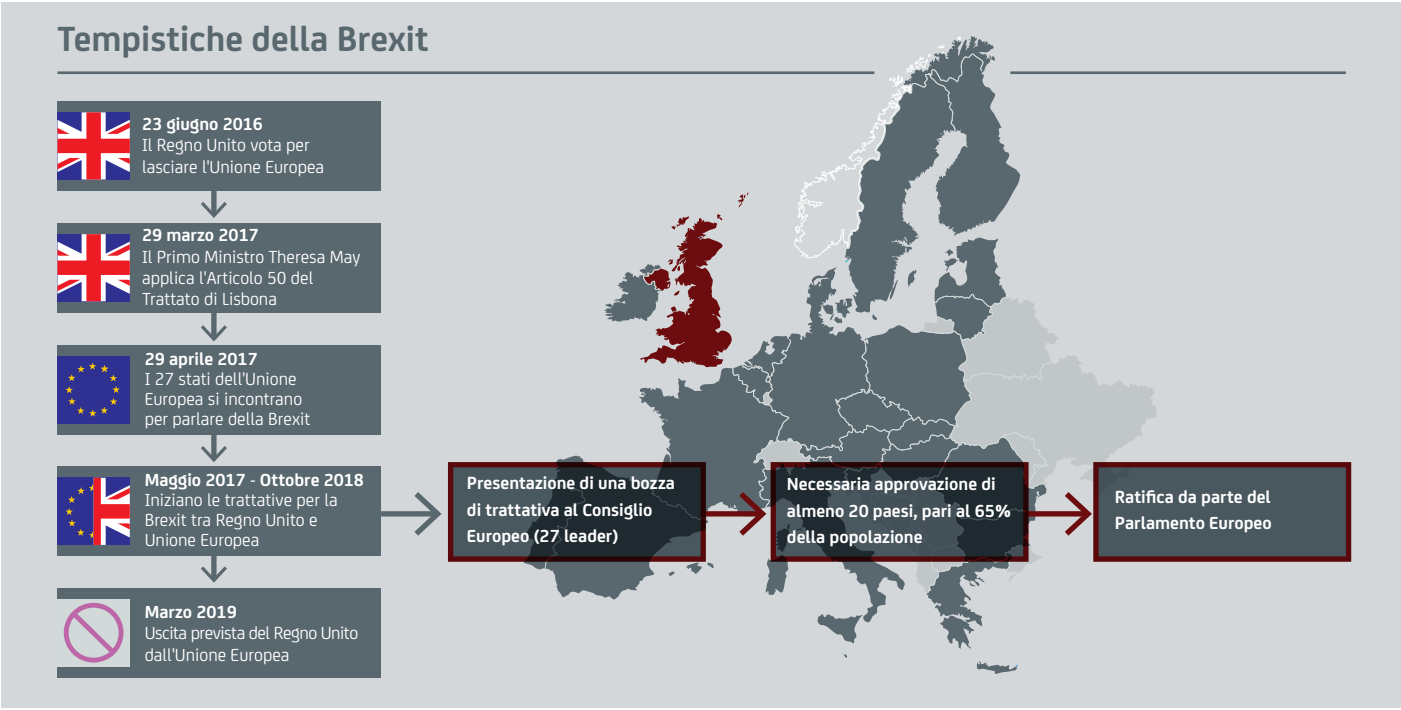

Figura A. Tempistiche della Brexit (per gentile concessione di APA e DW)

Nei prossimi 24 mesi, l'Unione Europea e il Regno Unito devono concordare i termini dell'interazione dopo la separazione. Nel frattempo, da entrambe le parti varie aziende pubbliche e private hanno iniziato a studiare soluzioni per gestire il business in modo più regolare. Questo processo è tuttavia pieno di incognite e rischi, perché tutte la parti coinvolte, direttamente o indirettamente, devono muoversi in un territorio inesplorato. Proprio per questo, occorre un programma attentamente studiato per la gestione del rischio.

Potenziale impatto economico

Sono stati creati vari modelli per illustrare l'impatto macroeconomico della Brexit sul Regno Unito, molti dei quali suggeriscono quanto segue:

- Crollo del PIL a lungo termine
- Drastica riduzione degli investimenti stranieri diretti (FDI, Foreign Direct Investment)
- Rallentamento dell'immigrazione

Nel complesso, ciò significa che molte aziende devono cercare soluzioni per mantenersi competitive e continuare a operare nei rispettivi mercati. Per minimizzare l'impatto sulla gestione del business, le aziende stanno creando un framework per il futuro, spesso prendendo in considerazione lo scenario peggiore. "Ai fini della pianificazione, dobbiamo ipotizzare una Brexit difficoltosa, in cui il Regno Unito perde il suo diritto al passaporto per l'Unione Europea", ha scritto il James Cowles, CEO Europeo di Citigroup in un memo per lo staff. Anche altri istituti finanziari hanno adottato piani simili. Ma gli istituti finanziari non sono entità isolate. È necessario considerare l'impatto della separazione da entrambe le parti. Ad esempio, Vauxhall sta pensando di reperire tutti gli elementi della supply chain per il Regno Unito all'interno del Regno Unito stesso, mentre BMW sta cercando una nuova sede nell'Europa continentale per la sua Mini. Tuttavia, qualunque decisione razionale di business che influisce sulla manodopera, ad esempio una misura per aumentare la produttività nel Regno Unito fino ai livelli degli altri paesi della UE, o introduce cambiamenti nella domanda globale, rischia di essere etichettata come vittima della Brexit.

Impatto sull'occupazione

Uno degli aspetti più preoccupanti è costituito dall'impatto della Brexit sull'occupazione. Varie aziende hanno suggerito lo spostamento dei posti di lavoro oltre confine. Ad esempio Nestlé ha deciso di trasferire la produzione delle barrette al cioccolato Blue Riband dal Regno Unito alla Polonia, e questo potrebbe determinare l'eliminazione di 300 posti di lavoro nel Regno Unito. Questa potrebbe essere una conseguenza dei cambiamenti nelle leggi sull'immigrazione (leggi più severe sui visti o controlli più scrupolosi), delle tariffe commerciali e dell'incertezza. Secondo una delle più importanti agenzie di selezione del personale, nel settore privato britannico le assunzioni sono scese ai livelli minimi degli ultimi tre anni, a causa dell'incertezza generata dalla Brexit. Oltre alle importanti conseguenze sull'economia in generale, questo spostamento dei posti di lavoro costituisce anche una minaccia molto seria per la sicurezza delle informazioni.

Esposizione al rischio

Come appare evidente da quanto abbiamo visto finora, esistono alcuni importanti rischi che le aziende devono gestire nell'ambito della Brexit. Se a questo si aggiungono i cambiamenti tecnologici radicali a cui stiamo assistendo oggi, l'importanza della gestione dei rischi IT assume proporzioni notevoli. Uno degli aspetti più cruciali è costituito dal rischio per la sicurezza delle informazioni.
È ampiamente documentato che i principali rischi per la sicurezza delle informazioni di brand e istituti finanziari sono dovuti allo sfruttamento dell'accesso degli utenti con privilegi. Tali rischi sono amplificati dal fatto che le aziende hanno adottato ambienti virtuali e cloud per l'espansione del business e la digital transformation.

Affrontare i rischi derivanti dal privileged access management

Nel valutare le opzioni disponibili per affrontare le problematiche introdotte dalla Brexit, in particolare lo spostamento dei dipendenti, le aziende devono considerare anche le minacce interne.
Qualunque incertezza, come le potenziali variazioni delle condizioni di assunzione o il trasferimento di responsabilità, può dare luogo a comportamenti imprevedibili del personale interno. Inoltre, offre ai malintenzionati esterni la possibilità di sfruttare potenziali vulnerabilità. Anche il trasferimento delle responsabilità, come il ricorso a un fornitore esterno per determinate funzioni di business, può aumentare l'esposizione, richiedendo una supervisione e livelli di visibilità appropriati. Insieme, tutti questi problemi impongono l'implementazione di una strategia efficace per il contenimento dei rischi dovuti agli accessi con privilegi. Infatti, la protezione dei dati sensibili e della proprietà intellettuale è diventata decisamente più importante.

Considerazioni per il contenimento dei rischi dovuti agli accessi con privilegi

Per contenere i rischi dovuti alla compromissione o all'utilizzo non autorizzato degli accessi con privilegi in questa fase di incertezza, è necessario considerare quanto segue.

1. **Scala:** superficie esposta
    a. Endpoint/device: il problema non è limitato ai dati archiviati on-premise, ma si estende anche agli asset basati su risorse virtuali e cloud
    b. Identità: il problema non è limitato ai soli utenti amministrativi, ma si estende anche agli account e agli script da applicazione ad applicazione

2. **Ambito:** strategia futura
    a. Digital transformation: se è in atto un programma di digital transformation, occorre tenere conto del ruolo svolto dai clienti, fornitori o partner che partecipano all'iniziativa
    b. Programmi per la Internet of Things (IoT): è necessario considerare qualsiasi device che potrebbe avere accesso alle informazioni con privilegi
3. **Automazione:** machine learning e registrazione delle sessioni
    a. Machine learning: occorre utilizzare tecniche di analisi del comportamento degli utenti (UBA, User Behavior Analytics) per rilevare le anomalie, al fine di ridurre il tempo necessario per identificare e limitare l'esposizione
    b. Registrazione delle sessioni: impossibilità di smentita e compliance
4. **Risorse:** budget e talenti
    a. Budget: a causa dell'incertezza geopolitica, è probabile che i budget saranno molto limitati durante la negoziazione della Brexit
    b. Talenti: a causa delle imminenti modifiche alle leggi sull'immigrazione e della migrazione dei talenti, è importante assicurarsi che il deployment non venga ostacolato da una carenza di competenze specifiche

Conclusioni

Il privileged access management, ad esempio tramite le soluzioni di CA Technologies, è importante per assicurare una protezione efficace degli asset critici durante questa fase di cambiamento geopolitico. Anche se si può avere la tentazione di iniziare con le sole funzionalità di base, come il vault delle password, per contenere i rischi è importante valutare il problema in modo olistico. La Brexit prevede tempistiche fisse. Il ritmo delle attività è probabilmente destinato ad aumentare, lasciando agli esperti di sicurezza delle informazioni un tempo brevissimo per reagire. È fondamentale considerare il total cost of ownership (TCO) della soluzione, insieme all'ambito e alla scala del supporto funzionale, prima di imboccare questo percorso. Occorre prevedere eventuali incognite, come la separazione delle mansioni e i problemi relativi alla sovranità dei dati, durante il processo. Infine, è necessario considerare una soluzione che, oltre a fornire scalabilità, portata e automazione, consenta anche di gettare le basi per un privileged access management sicuro, insieme all'analisi basata su machine learning. Questo cambiamento non interessa solo il Regno Unito, ma anche tutti i partner commerciali più importanti di Regno Unito e Unione Europea.

CS200-277092_0617