



CYBERARK®

Implementare il Protocollo dei controlli di sicurezza per i clienti SWIFT con CyberArk



La Società per le Telecomunicazioni Finanziarie Interbancarie Mondiali (SWIFT) fornisce a una ampia comunità di istituti finanziari mondiali la possibilità di scambiare informazioni di contenuto sensibile inerenti alle transazioni finanziarie internazionali. La sua vasta rete - costituita da più di 11 mila clienti in oltre 200 paesi - è diventata nel tempo un obiettivo di alto valore ed è particolarmente vulnerabile agli attacchi degli hacker. Basti pensare alle numerose violazioni della sicurezza ad alto profilo che si sono registrate negli ultimi tempi, tra cui il famigerato **attacco informatico alla Banca Centrale del Bangladesh**. Il cyber-furto di credenziali degli utenti SWIFT, unito all'utilizzo di tecniche di hacking sempre più sofisticate, consente agli hacker di sottrarre milioni di dollari a banche di tutto il mondo.

Per questo proteggere le credenziali dalle insidie dei criminali costituisce un passo fondamentale per prevenire possibili attacchi futuri. A questo scopo il **Customer Security Programme di SWIFT** ha messo a punto un protocollo di sicurezza e definito delle linee guida sulla responsabilità per i clienti SWIFT.

Il protocollo si focalizza in particolare sulla sicurezza degli account privilegiati. Entro il 18 gennaio 2018, le organizzazioni che si appoggiano a SWIFT dovranno dimostrare di aver ottemperato ai controlli obbligatori e a quelli caldeggiati dal protocollo.

Il protocollo di sicurezza SWIFT è costituito da 27 controlli incentrati su tre obiettivi globali, la cui conformità va comprovata entro la scadenza. I clienti CyberArk hanno il vantaggio di poter implementare la gran parte di questi controlli: la società, infatti, permette di ottemperare ai requisiti di sicurezza richiesti in ambiente aziendale, individuando "chi" e "cosa" ha accesso a sistemi e applicazioni di rilievo, concentrandosi allo stesso tempo sulle attività ad alto rischio svolte dagli operatori.

Di seguito i dettagli su come CyberArk è in grado di supportare le società a raggiungere questi obiettivi chiave:

METTERE IN SICUREZZA L'AMBIENTE

I rischi possono provenire sia dall'esterno che dall'interno - da "esterni" con precise finalità dolose o da "interni" distratti e insoddisfatti, causando danni ingenti agli istituti finanziari. In entrambi i casi il punto debole è costituito da una cattiva gestione degli accessi privilegiati. La soluzione **CyberArk Privileged Account Security** abilita servizi di protezione e controllo degli accessi a sistemi critici all'interno dell'ambiente SWIFT locale. Tramite la revoca dei diritti di amministrazione e utilizzando il tool **CyberArk Endpoint Privilege Manager**, è possibile definire le politiche di gestione distribuendo accessi agli utenti "non-admin", variando i diritti in base a necessità specifiche on-demand. Inoltre, le credenziali di accesso degli account privilegiati come password e chiavi SSH (ad esempio per l'accesso a sistemi critici in ambiente UNIX/Linux) vengono protette da strutture di sicurezza integrate e multi-livello.





CONOSCERE E LIMITARE GLI ACCESSI

Il tool **CyberArk Privileged Session Manager** permette di isolare, monitorare, registrare e controllare le sessioni degli utenti privilegiati nei sistemi critici. Il tool funziona come jump server e come punto di controllo degli accessi, consentendo di creare una zona sicura per proteggere il sistema SWIFT locale. Gli addetti alla sicurezza possono monitorare in tempo reale le sessioni degli utenti privilegiati, intercettando le attività sospette mentre vengono svolte e interrompendole tramite controllo remoto per ridurre al minimo ogni potenziale danno. Inoltre, il tool memorizza registri di controllo ricercabili e registrazioni delle sessioni in archivi blindati, a prova di ladro, impedendo così agli utenti privilegiati di cancellare la cronologia delle loro attività. Gli addetti alla sicurezza e al controllo possono accedere alle registrazioni e ai registri per individuare il momento esatto in cui un evento si è verificato, per definirne lo scopo e il livello di gravità.



INDIVIDUARE E RISPONDERE

Individuare e rispondere: le principali prede degli hacker sono utenti affidabili e riconosciuti di cui attaccano e compromettono le credenziali. Individuare i cyber-attacchi è impresa molto ardua. Inoltre molte organizzazioni faticano a rilevare i tentativi di bypassare i controlli di sicurezza da parte di minacce interne ed esterne. Per rispondere a queste sfide, il tool **CyberArk Privileged Threat Analytics** implementa strumenti per l'individuazione di abusi e/o tentativi di attacchi alle credenziali degli utenti privilegiati. L'uso di questo strumento in combinazione alla soluzione **CyberArk Privileged Account Security**, permette di evidenziare le attività anomale e ad alto rischio all'interno dell'ambiente SWIFT locale, generando un registro dettagliato e ricercabile di tutte le attività degli utenti privilegiati.

Per conoscere nel dettaglio le modalità con cui CyberArk può supportare la vostra organizzazione ad ottemperare ai requisiti del protocollo di sicurezza SWIFT entro la scadenza di gennaio 2018, vi invitiamo a:



Scaricare la
presentazione
goo.gl/EHK53x



Seguire il webinar
"Fast Track to SWIFT Compliance"
goo.gl/KvMEyF

CyberArk rappresenta l'unica società che sviluppa sistemi di sicurezza per rimuovere le minacce informatiche più avanzate, ovvero quelle che utilizzano gli accessi privilegiati interni per attaccare il cuore delle società. CyberArk **mette al sicuro** dalle minacce informatiche **prima che i danni diventino irreparabili**, con l'obiettivo di arginare gli attacchi ancor prima che questi blocchino l'azienda.

Le più importanti società al mondo - tra cui il 45% delle società dell'indice Fortune 100 - affidano a CyberArk la protezione di infrastrutture, applicazioni e informazioni di alto profilo. CyberArk è un'organizzazione internazionale con sede a Petach Tikva (Israele) e a Newton, Massachusetts (Stati Uniti), e dispone di una fitta rete di filiali localizzate in America, nei paesi EMEA, in Asia e in Giappone.

**Per informazioni sull'azienda
e sui nostri servizi, visita il sito
www.cyberark.com**



facebook.com/CyberArk



twitter.com/CyberArk



linkedin.com/company-beta/26630

