SSPM: la sicurezza dei SaaS che usi ma non controlli

SSPM è l’acronimo di SaaS Security Posture Management, e nasce da uno spostamento che ha cambiato in silenzio dove vive il rischio. L’attività di un’organizzazione oggi non gira più su server che configura e custodisce, ma su decine, spesso centinaia, di applicazioni in modalità software come servizio: la posta, i documenti, il CRM, le risorse umane, lo sviluppo, la collaborazione. Di queste applicazioni l’organizzazione non possiede l’infrastruttura e non ne scrive il codice. Ne controlla soltanto una cosa, la configurazione, ed è esattamente lì che si è trasferito il problema di sicurezza.

La logica è la stessa che governa il cloud, ma portata un passo più in là. Il fornitore del SaaS si occupa di proteggere la piattaforma e di tenerla aggiornata; al cliente resta la responsabilità di come quella piattaforma è impostata: chi può accedere, cosa è condiviso con l’esterno, quali account hanno privilegi da amministratore, a quali applicazioni di terze parti si è dato il permesso di collegarsi. L’SSPM è la disciplina che verifica, in modo continuo, che la postura di tutto questo parco di applicazioni sia sicura, perché nessun fornitore lo farà al posto del cliente.

La responsabilità che si è spostata

Conviene fissare bene questa divisione, perché è la fonte di gran parte degli incidenti. Nel modello del software come servizio il fornitore garantisce la sicurezza della piattaforma, ma la configurazione del singolo ambiente, il cosiddetto *tenant*, è interamente nelle mani del cliente. È il punto in cui si annidano le esposizioni: una regola di condivisione troppo permissiva che rende un documento

accessibile a chiunque, un controllo amministrativo lasciato aperto, l'autenticazione a più fattori non imposta a tutti. Sono errori di impostazione, non difetti del prodotto, ed è il cliente a doverli trovare.

Il guaio è che la superficie di configurazione è enorme e diversa per ogni applicazione. Ciascuna piattaforma, dalla suite di produttività al CRM, ha centinaia di impostazioni di sicurezza con una propria logica, e quasi nessuna organizzazione le verifica in modo sistematico e ricorrente. La configurazione si fa una volta, all'avvio, e poi si muove da sola: nuovi utenti, nuovi permessi, nuove integrazioni, nuove derive rispetto allo stato sicuro di partenza. Senza un controllo continuo, lo scostamento cresce invisibile, fino al giorno in cui qualcuno si accorge che un dato che doveva restare interno era raggiungibile da fuori.

Il ventre molle: le integrazioni SaaS-to-SaaS

C'è un fronte, in particolare, che sfugge a quasi tutti, ed è quello delle connessioni tra applicazioni. Ogni volta che si collega un'app di terze parti a una piattaforma SaaS, attraverso un consenso OAuth, si concede a quell'app un accesso ai propri dati che è ampio, persistente e raramente rivisto. È, a tutti gli effetti, una identità non umana con permessi spesso eccessivi rispetto a ciò che le serve, concessa con un clic e poi dimenticata. Moltiplicato per le centinaia di integrazioni che un'organizzazione accumula nel tempo, questo intreccio di connessioni da applicazione ad applicazione diventa una rete che nessuno ha mai inventariato.

È un ventre molle pericoloso perché aggira il perimetro. Un attaccante che comprometta un'app di terze parti con un consenso valido raggiunge i dati custoditi nella piattaforma principale senza dover violare nulla del cliente: usa una porta che il cliente stesso ha aperto. Lo ha mostrato in modo

netto la compromissione dell’integrazione Drift di Salesloft, nell’agosto 2025: token OAuth sottratti a quell’app di terze parti hanno dato accesso ai dati Salesforce di oltre settecento organizzazioni, aggirando l’autenticazione, e da lì gli attaccanti hanno cercato credenziali per spostarsi verso altri servizi. È la dimostrazione di come una via legittima, una volta compromessa, diventi un’autostrada. L’SSPM affronta proprio questo, tracciando le applicazioni connesse, valutando gli ambiti e i permessi che hanno ottenuto, e segnalando le integrazioni rischiose o sovradimensionate prima che diventino il percorso di un attacco.

SSPM non è CSPM e non è CASB

Per collocare bene questa disciplina serve distinguerla da altre con cui viene spesso confusa. La gestione della postura degli ambienti cloud, il CSPM, protegge l’infrastruttura su cui si costruisce, le macchine, le reti, gli archivi dei fornitori di servizi infrastrutturali. L’SSPM protegge invece la configurazione delle applicazioni che si consumano già pronte. I due mondi si somigliano nel concetto, postura, scostamento, librerie di regole, ma poggiano su interfacce completamente diverse, al punto che le regole dell’uno non si possono trasferire all’altro: lo spiega bene chi ha mappato chi protegge cosa tra le varie sigle. Il CNAPP, semmai, non è una categoria contrapposta ma la piattaforma più ampia che consolida diverse di queste capacità, il CSPM tra le altre, e che in alcuni casi arriva a inglobare lo stesso SSPM come componente.

Diversa ancora è la funzione di un CASB, che lavora sul traffico: osserva e controlla l’uso delle applicazioni, blocca caricamenti, ispeziona i dati in transito, agendo come un intermediario sul flusso. L’SSPM non sta sul flusso, sta dentro l’applicazione, e governa la configurazione, le identità e gli accessi delle terze parti. Non sono alternative, sono strati complementari: il CASB sorveglia come

gli utenti usano i SaaS, l’SSPM verifica come i SaaS sono impostati. Trattarli come la stessa cosa lascia scoperto proprio il livello, quello della postura, su cui questa disciplina lavora.

Cosa guarda l’SSPM

In concreto, l’SSPM tiene sotto controllo alcune dimensioni ricorrenti su tutto il parco applicativo. Le configurazioni errate, come le condivisioni pubbliche e le impostazioni deboli. Le identità, con gli amministratori dormienti, l’autenticazione a più fattori non imposta, i ruoli sovraprivilegiati. Le applicazioni di terze parti collegate e gli ambiti che hanno ottenuto. E lo scostamento rispetto ai requisiti di conformità. Lo fa attraverso le interfacce delle piattaforme, senza agenti da installare, e soprattutto lo fa in continuazione, perché in un ambiente che cambia ogni giorno una verifica una tantum invecchia nel giro di una settimana.

Perché conta adesso

La spinta che rende il tema urgente è la proliferazione stessa del software come servizio. Le organizzazioni adottano un numero di applicazioni molto superiore a quello che la sicurezza riesce a censire, e una quota consistente è *shadow SaaS*, sottoscritta dai singoli reparti senza passare da nessun controllo centrale. A questo si aggiunge l’arrivo degli assistenti basati sull’intelligenza artificiale dentro le stesse piattaforme, che ottengono accesso ai dati aziendali e allargano ulteriormente la superficie da governare. Il perimetro, in pratica, non è più una rete da difendere, ma un insieme di centinaia di ambienti che qualcuno ha configurato, spesso in fretta, e che da allora vivono di vita propria.

In definitiva, l’SSPM risponde a una domanda che vent’anni fa non aveva senso porsi, quando il software stava sui server di casa: le applicazioni che noleggio ma non gestisco sono

configurate in modo sicuro, e a chi ho dato silenziosamente le chiavi dei miei dati. Più l’attività si sposta nei SaaS, più questi si collegano tra loro e all’intelligenza artificiale, e più la postura di quel parco di applicazioni diventa la vera superficie d’attacco, quella che il cliente possiede per intero e che, paradossalmente, quasi nessuno sorveglia. L’SSPM è il modo per smettere di darla per scontata.

Fonti

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/cyber-security/sspm-saas-security-posture-management/