External Attack Surface Management, la nuova frontiera della cybersecurity aziendale. Cosa dice 7Layers?

Il campo in evoluzione dell'EASM – *External attack surface management* – può senz'altro ritenersi la "prima linea" nella strategia difensiva di un'organizzazione, andando ad applicare uno *shift left che,* in sicurezza informatica, significa anticipare le attività di sicurezza per affrontarle durante le prime fasi del ciclo di sviluppo del software.

Se infatti il "classico" *Attack Surface Management* (ASM) comprende le attività di monitoraggio, rilevamento e analisi delle vulnerabilità di sicurezza, nonché dei potenziali vettori che vanno a costituire la cosiddetta superficie d'attacco, l'EASM anticipa tali azioni, ossia anticipa il momento di rilevazione di possibili *debolezze* sfruttabili da un soggetto malevolo in quello che viene indicata come "superficie di attacco digitale".

Come funzionano gli strumenti EASM

Con il continuo aumento della superficie digitale di attacco di una azienda (sistemi Cloud dove sono presenti VPDC, l'adozione di *serverless application*, il lavoro *smart* e *remoto*, etc), si rende sempre più necessario far evolvere le strategie di difesa adottate al fine di comprendere questa mutevole situazione.

L'*External Attack Surface Management* è stato *ideato* per fornire un livello di protezione più efficace (*shift left*) a tutti gli *asset* IT che sono esposti, a vario titolo, su

Internet: alcuni esempi sono i servizi esposti a livello infrastrutturale, i siti web, i servizi acquisiti da soggetti terzi e ogni altro *entry point* che un attaccante potrebbe sfruttare per acquisire l'accesso all'infrastruttura interna o sfruttare tale asset per attaccare un ulteriore vittima.

L'attuale panorama delle soluzioni EASM prevede la presenza di sistemi che combinano ricerche e analisi automatizzate della superficie di attacco di un target con specifiche metodologie di valutazione del rischio, fornendo una visione più ampia della reale *superficie di attacco*.

La componente automatizza ha lo scopo di identificare gli *entry point* del potenziale target attraverso la verifica delle *digital footprint* di questo: ogni elemento che concorre a definire la presenza digitale di una azienda è potenzialmente un asset di interesse per un attaccante.

La seconda componente, ossia l'analisi del rischio di quanto esposto, ha lo scopo di classificare e prioritizzare le *debolezze esterne* rilevate al fine di pianificare le azioni mitigazione del rischio necessarie e rilevate dalla componente automatica.

Sicurezza integrata grazie all'EASM: la proposta di 7Layers

L'approccio proposto da **7Layers** nell'usare i sistemi EASM ha come scopo quello di fornire una visione sempre più approfondita del rischio associato agli asset aziendali, partendo dalla componente esterna fino a quelle interne, vero *cuore* dell'azienda e grazie alle quali è condotto il relativo business aziendale.

Grazie ad un punto di vista esterno all'organizzazione, tale soluzione permette di identificare quelle debolezze, intese non solo come vulnerabilità o errori di configurazione ma anche come fragilità organizzative, che possono essere

trasformate in pericolose *leve* a favore del *threat actor* di turno: l'attuale panorama della Cyber Security vede una evoluzione dei modelli di servizio degli attaccanti, ad esempio al Cybercrime-as-a-Service (CaaS) o Ransomware-as-a-Service (RaaS), tale per cui non è più possibile considerare un singolo *threat actor* ma una moltitudine di questi.

Servizi Avanzati dell'EASM

- **Analisi Dettagliata dell'Esposizione ai Rischi Cyber**: Oltre alla semplice identificazione degli asset, l'EASM offre un'analisi dettagliata del rischio di esposizione di ciascun asset, considerando non solo le vulnerabilità note ma anche le configurazioni non sicure e le prassi di gestione degli asset che possono aumentare il rischio di attacchi.
- **Identificazione di Asset Sconosciuti o Dimenticati**: Uno dei principali vantaggi dell'EASM è la capacità di scoprire asset che l'organizzazione non sapeva di avere o aveva dimenticato, inclusi sottodomini, servizi cloud e API esposte, riducendo il rischio di attacchi mirati a risorse non monitorate.
- **Correlazione di Dati e Intelligence sulle Minacce:** Integrando dati di intelligence sulle minacce, l'EASM permette di correlare le informazioni sulle vulnerabilità con attacchi noti e tattiche, tecniche e procedure (TTP) degli aggressori, migliorando la capacità di prevedere e prevenire attacchi.

Benefici Integrati dell'Utilizzo dell'EASM

- **Allineamento con Framework di Sicurezza**: L'adozione di un approccio EASM aiuta le organizzazioni a allinearsi meglio con i framework di sicurezza internazionali come NIST e ISO/IEC 27001, fornendo una struttura per la

gestione proattiva dei rischi e migliorando la postura di sicurezza complessiva.

- **Miglioramento della Risposta agli Incidenti**: Con una conoscenza approfondita dell'external attack surface e una valutazione continua dei rischi, le organizzazioni possono rispondere più rapidamente e efficacemente agli incidenti di sicurezza, riducendo i potenziali danni.
- **Ottimizzazione del ROI in Sicurezza**: Investire in EASM consente alle organizzazioni di ottimizzare il ritorno sull'investimento (ROI) in sicurezza, concentrando le risorse su minacce e vulnerabilità che presentano i maggiori rischi per l'azienda.
- **Partnership e Collaborazione**: Implementando l'EASM, le organizzazioni possono anche beneficiare di una maggiore collaborazione sia internamente tra i team IT e di sicurezza, sia esternamente con partner e fornitori di servizi di sicurezza, condividendo informazioni e best practices per una difesa più efficace.

Il costante monitoraggio dell'intera superficie di attacco dell'organizzazione può fare davvero la differenza, anticipando la rilevazione di debolezze e facilitando i decisori nella definizione e attuazione di strategie di sicurezza al passo con il contesto di riferimento e garantendo, così, alle aziende una gestione integrata e proattiva del rischio informatico.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/external-attack-surface-management-la-nuova-frontiera-della-cybersecurity-aziendale-cosa-dice-7layers/