L’evoluzione del Vulnerability Assessment nell’Era Moderna della Cybersecurity. Abbiamo incontrato 7Layers



Fin dai tempi antichi, al fine di poter evolvere e migliorarsi, è necessario *conoscere se stessi* e tale prassi è applicabile anche al settore della sicurezza informatica: conoscere e gestire le vulnerabilità di sicurezza informatica rappresenta una sfida cruciale per le organizzazioni oggi e se già da tempo le attività di *Vulnerability Assessment* sono incluse nel macrocosmo della cybersecurity, oggi con la rapida evoluzione del panorama delle minacce informatiche le azioni non solo di *Vulnerabiliy Assessment* (VA) ma anche di *Penetration Test* (PT) risultano fondamentali per poter identificare, classificare e valutare correttamente le vulnerabilità dei sistemi in uso dall’azienda ottenendo anche una visione complessiva e dinamica delle potenziali superfici d’attacco.

Cosa sono il Vulnerability Assessment e il Penetration Test e le loro evoluzioni?

Il VA/PT, nella sua accezione più ampia, è un complesso di attività e processi che mirano a identificare, analizzare e classificare le vulnerabilità presenti nei sistemi informatici di un’organizzazione, in un processo continuo di analisi che ha come *scope* (ambito) differenti aree:

- ***Physical***: Concentrato sulla sicurezza fisica degli ambienti.

- ***Network-Based***: Rivolto alle vulnerabilità della rete.
- ***Application-Based***: Rivolto alle applicazioni software.
- ***API-Based***: Focalizzato sulle interfacce di programmazione delle applicazioni.
- ***Host-Based***: Riguarda i singoli dispositivi all'interno della rete.

Per poter ottenere, quindi, la piena visibilità di *tutti* i punti deboli dell'infrastruttura che un attaccante potrebbe voler sfruttare, non si tratta di svolgere una sola e singola attività di analisi su uno specifico ambito, ma di svolgere una azione periodica e trasversale su tutti gli ambiti sopra indicati, attraverso un lavoro costante.

Un recente progresso in questo campo consiste nel **Risk-Based Vulnerability Management (RBVM)**, un approccio alla gestione delle vulnerabilità che va oltre la semplice identificazione e classificazione della vulnerabilità: il RBVM ha come elemento cardine la quantificazione del rischio di una vulnerabilità in relazione al reale rischio che questa costituisce per l'organizzazione.

A differenza dei tradizionali metodi di gestione delle vulnerabilità, che si basano sulla sola attribuzione di un *punteggio* di rischio dipendente dalla vulnerabilità senza contesto, l'RBVM utilizza metriche specifiche di contesto, come ad esempio il CVSS scores nei suo parametri completi, analizza l'attività dell'attaccante e la criticità dell'asset e adotta strumenti come il Vulnerability Prioritization Tool (VPT) per prioritizzare le vulnerabilità. L'obiettivo è concentrare gli sforzi di mitigazione e *remediation* sulle vulnerabilità con il più alto potenziale di danno per l'organizzazione: per poter ottenere questo risultato, tale approccio richiede l'integrazione di *threat intelligence*, l'analisi del contesto aziendale e le valutazioni tecniche allo scopo di produrre una roadmap di risposta efficace e tempestiva.

La gestione degli incidenti informatici, stante la metodologia consolidata, prevede diverse fasi:

- identificazione;
- analisi;
- valutazione;
- mitigazione e *reporting*.

Il primo punto, l'identificazione, ha come elemento cardine proprio l'attività di VA/PT, grazie alla quale è possibile rilevare, analizzare e valutare le minacce *cyber* conseguenti, permettendo ai team di sicurezza di prendere decisioni consapevoli tramite i dati acquisiti e consentendo una risposta rapida, scalabile e adattabile a fronte di un attacco.

Una ulteriore ricaduta dell'attività di VA/PT è l'acquisizione di *insights* sui sistemi aziendali, informazioni cruciali per l'analisi della conformità ai protocolli/framework normativi, estendo la mera verifica della sicurezza all'aderenza ai regolamentazioni in vigore.

L'importanza dell'Attack Surface Management

L'Attack Surface Management (ASM) è cruciale nell'era digitale avanzata data la complessa tessitura di componenti fisici e digitali nelle organizzazioni: con l'esplosione di dispositivi IoT e l'adozione pervasiva del cloud, la superficie d'attacco è aumentata esponenzialmente.

Nel 2022, Gartner identifica l'espansione della superficie di attacco come una priorità assoluta rispetto alla gestione della sicurezza: ciò pone sotto osservazione il limite dell'approccio EASM (External Attack Surface Management), che pur essendo essenziale, offre solo una visione parziale, limitata alle minacce esterne. Al contrario l'ASM (Attack Surface Management), con il suo approccio globale che include

anche l’Attack Surface Assessment (ASA) e il Vulnerability Assessment e Penetratione Test, mira ad una protezione completa sotto i vari punti di vista.

L’ASM (*Attack Surface Management*) comprende ogni processo funzionale al monitoraggio costante e dinamico di tutte le potenziali debolezze sfruttabili per un attacco, al fine di garantire la difesa dalle minacce esterne senza tuttavia trascurare le possibili fonti di rischio interne, come ad esempio la presenza di dispositivi obsoleti, una scarsa protezione degli *endpoint*, una debolezza nella catena di fornitura o tentativi di *social engineering* mirati ai dipendenti meno preparati e più facilmente aggirabili.

Sul fronte delle tecnologie impiegate, questa esigenza si traduce nella crescente automazione delle varie attività di analisi del traffico di rete e di *anomaly detection* nonché, in caso di eventuali attacchi, dell’attuazione delle *remediation* necessarie e l’acquisizione dei dati derivanti dal *reporting* secondo il paradigma della *lesson learned*.

Un valido programma di ASM deve altresì comprendere la riduzione ai minimi termini, ove possibile, dei potenziali punti di accesso ai sistemi aziendali tramite il ricorso alla valutazione dei rischi annessi e deve prevedere l’analisi e l’applicazione del concetto di *network segmentation*, unitamente al continuo aggiornamento di tutte le risorse umane o tecnologiche coinvolte.

Il futuro dell’ASM: Vulnerability Assessment-as-a-service

Al fine di fronteggiare validamente il rischio cyber, oggi le organizzazioni devono imparare a gestire l’intero *vulnerability life cycle* in maniera coerente con le priorità aziendali.

Ciò è particolarmente urgente per le numerose realtà che negli

ultimi anni hanno optato per un ricorso stabile al lavoro ibrido: infrastrutture diffuse e reti a cui il personale accede da remoto hanno infatti ulteriormente sfumato i confini fisici e dilatato il perimetro digitale dell'azienda, rendendo meno semplice l'applicazione di uniformi politiche di *patching* sui dispositivi o la piena implementazione del paradigma *Zero Trust* nella gestione degli accessi.

La ricerca, l'esame e la valutazione di tutte le potenziali vulnerabilità possibili, presenti sui sistemi aziendali, risulta per buona parte delle organizzazioni un compito gravoso se svolto con le risorse interne, motivo per cui il trend sempre più consolidato è quello del ricorso, da parte delle organizzazioni, di servizi di Vulnerability-as-a-Service (VaaS) in *outsourcing*: se le attività tecnologiche e le analisi dal punto di vista di un attaccante sono svolte da soggetti terzi, l'organizzazione mantiene la gestione dei flussi di *Digital Risk Protection Services* (DRPS), *Cyber asset attack surface management* (CAASM) ed *External attack surface management* (EASM) entro un unico processo di *Cybersecurity Validation* che garantisca – in attuazione del principio noto come *Continuous Threat Exposure Management* (CTEM) – una gestione della sicurezza dinamica e integrata, in grado di contenere e anticipare l'evoluzione vertiginosa delle minacce informatiche.

Durante il nostro incontro con la Business Unit di sicurezza offensiva di 7Layers, è emersa una considerazione cruciale: in un'epoca in cui le minacce informatiche sono in costante evoluzione, è fondamentale avere una chiara comprensione del proprio panorama di vulnerabilità e adottare un approccio proattivo alla loro gestione per garantire la sicurezza di ogni organizzazione.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/levoluzione-del-vulnerability-assessment-nellera-moderna-della-cybersecurity-abbiamo-incontrato-7layers/