Il Vulnerability Management a Processo

Creare un processo di Vulnerability Management senza supportarlo equivale a non averlo affatto.
Usare un tool che non considera il processo può illudere di essere sicuri.

Le ragioni che possono spingere le aziende a prendere in seria considerazione la tematica del **Vulnerability Management** sono molteplici: dagli obblighi contrattuali (v. dominio #6 dello standard PCI DSS *"Develop and maintain secure systems and application"*) alle policy dettate dalla propria parent company, senza dimenticare la necessità di ridurre il rischio di data breach, per contenere eventuali danni d'immagine e possibili sanzioni dovute al GDPR. Non bisogna infine trascurare il **fattore psicologico**: in questo senso possono giocare un ruolo rilevante gli attacchi, tentati o riusciti, nei confronti della propria azienda o di realtà dello stesso settore, così come un'accresciuta consapevolezza del rischio, reale o anche solo percepito, in merito a un possibile attacco.

Indipendentemente dalle motivazioni alla base, le aziende che necessitano di gestire le vulnerabilità IT possono andare incontro a numerose difficoltà, diverse tra loro solo in apparenza, e a risultati spesso non soddisfacenti.

Nella maggior parte dei casi, il fattore debilitante è la **mancanza di cultura aziendale** in termini di Information Security che, in combinazione con uno scarso commitment da parte del top management, porta a sottovalutare la tematica e a limitare fortemente il budget a disposizione, l'avvio dei progetti e, di conseguenza, i risultati ottenibili. L'efficacia delle attività già in corso può essere minacciata da conflitti di competenza tra sicurezza e reparti IT, che

vogliono evitare impatti sulla normale operatività.

In altre situazioni, invece, si notano aziende sprovviste di reparti dedicati alla sicurezza, ma che dispongono di reparti IT discretamente predisposti e sensibili ad alcuni temi di Information Security. In questi casi vi sono tentativi di aggiornare i sistemi e gli apparati, di intervenire sulle configurazioni, di gestire l'obsolescenza e altre attività che molto spesso si traducono in semplici **azioni destrutturate e poco organizzate**, quasi di "volontariato", per correre al riparo da potenziali attacchi (dimenticando o ignorando, tra le altre cose, la parte di Application Security). Una prassi comune in questo tipo di scenario consiste nel lanciare una scansione generica, con un tool già a disposizione, su un perimetro parziale o non ben definito, per poi intervenire tecnicamente secondo tempistiche fortemente legate alle urgenze di business e alla casualità. Nemmeno questo è un approccio corretto, in quanto rischia di essere poco continuativo e stabile.

In entrambi i casi, i **problemi** alla radice sono simili: mancanza di un approccio basato sul rischio, di analisi preventive (si dovrebbe parlare anche di threat modelling), di gestione degli asset, ma soprattutto l'incapacità di trovare soluzioni che soddisfino le reali esigenze e di individuare corrette strategie di gestione. Il risultato? Una confusione diffusa che genera senso di smarrimento e distoglie l'attenzione dai problemi reali.

Una volta conseguita la consapevolezza sul tema del Vulnerability Management, è fondamentale che questa si traduca nel commitment necessario per proseguire con le fasi successive. In questo senso, la consapevolezza del rischio è, al pari di un budget adeguato, assolutamente propedeutica alle azioni da intraprendere – in primo luogo, la scelta di professionisti accreditati e con comprovata esperienza sul campo.

A valle di un primo assessment sullo stato dell'arte, si dovrebbe quindi procedere con la creazione, formalizzazione e messa in opera di un **processo** che, benché spesso venga visto soltanto come un adempimento normativo, un documento "da avere da qualche parte" atto a definire "chi fa cosa" o, peggio, una vera e propria scocciatura, è in realtà la giusta base di partenza per organizzarsi adeguatamente e giustificare le relative necessità di staffing, definendo ruoli e responsabilità, attività, tempistiche e flussi di comunicazione. In realtà, la definizione del processo può essere relativamente semplice, mentre la sua **applicazione** risulta essere la parte più complessa; basti pensare alla predisposizione di un ambiente di test in cui verificare le patch prima della messa in produzione, così come a garantire che il processo stesso tenga sempre conto del rapporto costi/benefici.

Essendo questo processo verosimilmente scritto a più mani, il risultato può essere scadente a prescindere da altri fattori. Uno dei problemi più gravi che si possono riscontrare nel neonato processo di Vulnerability Management è la **carenza di armonia** con i processi già esistenti, come il processo di Patch Management (con il quale ha diversi punti di contatto) e quello di Incident Management. Per far sì che questo non accada, occorre miscelare le best practice di settore, le competenze specialistiche e il contesto aziendale, non solo dal punto di vista organizzativo, ma anche considerando le possibilità economiche. Questo garantisce un processo formale, completo e su misura.

Una volta creato (o corretto) il processo di Vulnerability Management, è tuttavia necessario applicarlo e supportarlo con **risorse adeguate**. Affinché funzioni, occorre verificare la predisposizione ad interventi tempestivi mediante l'allocazione di figure tecniche di Security a presidio degli asset tecnologici. Occorrono anche figure gestionali in grado di facilitare il processo, interfacciandosi ad esempio con le

altre funzioni aziendali per contrastare ritardi e segnalare criticità, sulla falsa riga di quanto avviene quotidianamente nell'ambito di un classico project management. In certi contesti, questo tipo di figura può coincidere con il profilo del Vulnerability Analyst, che, in estrema sintesi, è uno specialista che si occupa di analizzare e segnalare le vulnerabilità, per poi produrre la reportistica per i Security Manager di riferimento. Non può mancare ovviamente un incaricato al monitoraggio dell'intero processo che, in ambienti strutturati, è spesso collocato nella funzione del CISO.

Sono altrettanto necessari **strumenti avanzati** di Vulnerability Management a supporto dell'omonimo processo che, se dotati delle giuste caratteristiche, possono fare la differenza nel passaggio da semplici attività passive di Vulnerability Scanning (anch'esse da identificare, valutare, programmare ed eseguire secondo regole specifiche) al più efficace, efficiente e proattivo Vulnerability Management, di cui le scansioni rappresentano solo una fase. In realtà strutturate, infatti, non è più sufficiente l'utilizzo di un semplice scanner, ma è consigliabile l'utilizzo di uno strumento che sia compatibile con i principali scanner (di rete ed applicativi), centralizzando la gestione degli output che ne derivano per ottenere un totale controllo del perimetro e per un monitoraggio più efficace dei progressi.

Supportare il Vulnerability Management dal punto di vista del tool significa anche facilitare – o persino automatizzare – certi tipi di valutazioni del rischio associato ad ogni istanza di vulnerabilità, tenendo traccia in maniera strutturata di tutte le informazioni relative a remediation, mitigation e accettazione del rischio. Sarebbe auspicabile avere a disposizione anche feature che consentano la gestione delle priorità, la pianificazione di tutte le attività e la produzione di reportistica di sintesi. I principali benefici ottenibili con questo approccio sono l'**ottimizzazione**

dell’operatività e il supporto alle decisioni, che portano ad un notevole risparmio in termini di risorse e ad una maggiore efficacia del processo. Non può nemmeno essere trascurata la necessità dei clienti di adattare il modello prestabilito alle proprie logiche di gestione, senza che queste generino conflitti o loop inaspettati una volta a regime.

Bl4ckswan lavora da anni a supporto di aziende di primaria importanza per inserire e mettere in opera tutte queste caratteristiche in *J4rvis*, una piattaforma che si propone come soluzione “vendor neutral” a supporto del processo di Vulnerability Management.

Articolo a cura di **Mattia Fierro**



https://www.ictsecuritymagazine.com/articoli/il-vulnerability-management-a-processo/