Pillole di Sicurezza

Monitoraggio della sicurezza dei sistemi informativi

Data pubblicazione: 27 maggio 2015

Controllo del livello di sicurezza dei sistemi informativi di un'organizzazione attraverso il monitoraggio continuo degli eventi e la correlazione con servizi di intelligence

Nel panorama di gestione del business si assiste ad una rapidissima evoluzione nelle architetture dei sistemi ICT a supporto: basti pensare all'evoluzione verso la virtualizzazione, i sistemi cloud e l'integrazione nel sistema informativo di dispositivi mobili; anche le reti sono state progressivamente aperte verso l'esterno in modo da consentire collegamenti verso clienti, partner e fornitori.
Allo stesso tempo diverse organizzazioni hanno deciso di dedicarsi in modo prevalente al loro core business esternalizzando di fatto la gestione dei sistemi informativi attraverso contratti di outsourcing.
Mentre questo ha comportato sicuramente una ottimizzazione dei costi di gestione, ha comportato d'altro canto la perdita della conoscenza sulla mappatura del rischio relativo agli asset informatici aziendali ma soprattutto la consapevolezza se questi possano essere o meno stati oggetto di tentativi di attacco.
Il documento, che prende spunto da progetti realizzati presso alcuni clienti, illustra in modo generale i passi necessari per riprendere il controllo del rischio attraverso il monitoraggio continuo della sicurezza dei sistemi informativi.

Il punto di partenza è sicuramente rappresentato dall'analisi e dal trattamento del rischio effettuati secondo standard riconosciuti: il censimento e la classificazione degli asset, sono informazioni che dovrebbero essere desunte dalla documentazione inerente le attività svolte in tal senso.
La classificazione degli asset informatici, effettata in base a parametri quali il livello di sensibilità od il grado di riservatezza dei dati trattati oppure al ruolo di business è fondamentale, in quanto ai fini del monitoraggio del livello di sicurezza un sistema dispiegato in ambiente di sviluppo segregato è sicuramente meno critico rispetto ad un sistema esposto su Internet. Secondo una logica analoga un sistema che è già stato oggetto di tentativi di attacco, specie se riuscito, dovrà essere sicuramente rappresentato attraverso un livello di rischio incrementato.

Nel corso degli ultimi anni alcune autorevoli organizzazioni internazionali (SANS Institute e NIST) da sempre coinvolte nella definizione di strategie volte al miglioramento del livello di sicurezza hanno proposto delle linee guida, risultato dell'indicazione condivisa da parte degli esperti del settore, che si pongono l'obiettivo di migliorare la sicurezza dei sistemi informativi attraverso un'azione di monitoraggio continuo.
Tali linee guida, individuate attraverso la pubblicazione avvenuta a fine 2011 del documento: Special Publication 800-137 – "Information Security Continuous Monitoring for Federal information Systems and Organizations", dettagliano le esigenze ed i requisiti di monitoraggio continuo (ISCM - Information Security Continuous Monitoring)

Nei sistemi informativi installati presso un'organizzazione moderna, contraddistinti da una discreta eterogeneità, dalla distribuzione geografica e dalla presenza di vari attori, è impensabile immaginare di gestire un incidente di sicurezza informatica affidandosi solo all'analisi dei log conservati localmente su di un sistema sia per la difficoltà di accesso ad informazioni correlabili ad attività ostili,

quali i tentativi di accesso in contemporanea ad altri sistemi, sia per la concreta possibilità che avvenga la sovrascrittura o la cancellazione delle informazioni.
Un aiuto può essere fornito dalla tecnologia che consente di trasferire tali informazioni (file di log ed eventi di sicurezza) su una piattaforma dedicata la quale può essere rappresentata nella sua accezione più semplice da un log server dedicato oppure una piattaforma di log management che, oltre a fornire in modo nativo funzionalità a garanzia dell'immutabilità dei dati registrati, consente di velocizzare le operazioni di analisi dei log oltre a consentire un'archiviazione a lungo termine delle informazioni.
In questo modo sarà possibile effettuare delle ricerche di file di log a ritroso per periodi abbastanza lunghi (generalmente si prevedono periodi di ritenzione di un anno per conformità normativa oppure per periodi più lunghi in caso di applicazioni particolarmente critiche).

Data la rilevanza delle informazioni è di fondamentale importanza che le fonti di log siano correttamente configurate a livello di sistema abilitando la registrazione degli eventi fondamentali ai fini della sicurezza, quali ad esempio l'esecuzione di uno shutdown oppure di un riavvio del server, la modifica delle policy di sicurezza e così via. Occorre assicurare che oltre alla scrittura in locale i log vengano inviati al sistema centralizzato mediante i protocolli standard dedicati (syslog, syslog-NG) oppure mediante i meccanismi di trasferimento messi a disposizione dalle piattaforme di log management (connettori, protocolli scp, ftps ecc).
Da segnalare che i file di log sono generalmente in formato testo standard, mentre ad esempio gli eventi generati dagli ambienti Microsoft sono in formato proprietario e quindi necessitano di una opportuna traduzione, che viene generalmente attuata mediante agent specifici oppure da connettori, per essere gestiti dalle piattaforme standard di log management.
E' importante verificare che anche gli eventi generati dalle applicazioni generino dei file di log, possibilmente in conformità ad un formato standard quale potrebbe essere quello CEF (Common Event Format), promosso da uno dei leader nel mercato delle soluzioni di log management; tale formato prevede l'adozione di un numero elevato di campi e consente di arricchire, dopo la scrittura, l'informazione ricevuta dal file di log con altre generate dalla piattaforma di gestione.

Un passo successivo rispetto alle fasi di raccolta, normalizzazione, indicizzazione ed archiviazione dei file di log e degli eventi è rappresentato dalla possibilità offerta dalle soluzioni SIEM (Security Information & Event Management) di poterli correlare, caratteristica che consente di aggregare e contestualizzare meglio le informazioni, in modo da facilitare le attività di analisi. In questo caso è possibile integrare e correlare ai file di log anche le informazioni registrate dalle sonde presenti sulla rete, quali i cosiddetti flow, oppure le informazioni inerenti la topologia e le configurazioni della rete, la dislocazione degli asset nelle sedi, gli amministratori di sistema coinvolti, il grado di criticità ecc.

E' necessario attribuire agli oggetti da monitorare la corretta attenzione in quanto non tutti gli elementi sono caratterizzati dallo stesso profilo di rischio: una maggiore criticità dovrà essere attribuita ad esempio agli elementi che trattano informazioni di carattere riservato o sensibile, ai dispositivi esposti verso Internet oppure che consentono un accesso dall'esterno, servizi rivolti al pubblico od ai partner, servizi amministrabili da remoto, oppure apparati che svolgono compiti di controllo della sicurezza (firewall, IPS, anti malware, IAM).

Occorrerà pertanto configurare opportunamente gli attributi di tali asset all'interno della piattaforma SIEM in modo tale che queste informazioni vengano presentate con maggiore risalto

rispetto, per esempio, a quelle relative ad un server interno contraddistinto da un basso livello di criticità.

In generale è possibile gestire la priorità degli eventi registrati nei log associando un livello di severità che può essere considerato sinonimo della valutazione della rilevanza: le piattaforme SIEM consentono generalmente di mediare tale attributo con altre informazioni quali ad esempio se si tratti di un nuovo evento generato oppure ricorrente, la provenienza dell'evento da un asset sconosciuto, oppure l'azione indirizzata verso un sistema su cui attività di assessment svolti in precedenza abbiano individuato delle vulnerabilità importanti. Questa caratteristica consente di ottenere in modo automatizzato una classificazione di maggior dettaglio rispetto ai sistemi tradizionali.

Quanto descritto sinora rappresenta indubbiamente un notevole vantaggio in termini di riduzione, grazie all'automazione delle attività, del lavoro necessario all'elaborazione e presentazione al team di Security Operations delle informazioni da analizzare.
Queste misure tecnologiche non avranno la necessaria portata se non accompagnate dalle corrispondenti misure organizzative che, a prescindere dalla necessaria formazione del personale ed alla costituzione di un team operativo preposto alla gestione delle informazioni disciplinino in modo formale le attività di gestione degli incidenti di sicurezza informatica all'interno dell'organizzazione.
E' quindi importante rivedere le policy e procedure relative al processo di gestione degli incidenti di sicurezza informatica, tenendo conto del coinvolgimento del team operativo preposto alla gestione che potrà dare un importante supporto tecnico attraverso le attività di analisi delle minacce.

Secondo i presupposti sopra descritti, applicando un processo di continuo raffinamento delle informazioni sulle attività ostili ottenute dalla piattaforma SIEM, sarà possibile selezionare in base a precise regole (ad esempio eventi provenienti da netblock esteri con cui l'organizzazione non intrattiene rapporti di business, segnalazioni di malware provenienti da IPS validate in sede di analisi, traffico anomalo in uscita verso server che operano attività di Command & Control, attività sospette in orario extra lavorativo) gli estremi per l'apertura di case investigativi su cui impiegare le necessarie risorse ai fini di un'analisi approfondita.

Al termine dell'indagine, che in funzione della gravità attribuita alla minaccia potrà coinvolgere risorse tecniche e manageriali interne od esterne, si procederà all'adozione delle opportune contromisure ed alla redazione della reportistica relativa alla chiusura dell'incidente.

Nell'ottica del processo di miglioramento continuo (in osservanza ai principi della Lesson Learned) si provvederà eventualmente alla modifica delle configurazioni oppure all'adeguamento dei meccanismi di alerting onde poter affrontare in modo adeguato l'eventuale ripresentarsi di minacce analoghe.

Un investimento così importante in termini di risorse tecnologiche ed organizzative contraddistinto da obiettivi sfidanti deve essere opportunamente monitorato, attraverso la definizione di opportuni KPI (Key Performance Indicators) sia ai fini di misurare l'efficienza nella sua gestione sia per valutare in modo oggettivo la sua utilità nel contrasto alle minacce.

E' quindi opportuno adottare delle metriche, da tarare in funzione dello scenario di adozione, che si riferiscono a tre distinti settori:

- Ambiente operativo (numero di eventi giornalieri raccolti ecc.)
- Criticità (eventi a criticità alta ecc.)
- Gestione (numero di case aperti ecc.)

Le indicazioni fornite dalle misure periodiche dei KPI saranno utili per valutare se le risorse messe in campo siano sufficienti nelle attività di analisi oltre a dare indicazioni utili sull'evoluzione e sul trattamento delle minacce.

Sino a questo punto è stato indirizzato il problema delle minacce rilevabili dall'interno della rete attraverso le informazioni desunte dai dispositivi atti al monitoraggio ed alla gestione della sicurezza; questo pone però il problema di come applicare dei principi di "sicurezza preventiva" anche per quanto concerne le minacce potenziali esterne al perimetro che non sono ancora state riscontrate all'interno. Seguendo i principi di uniformità nelle attività di monitoraggio e di correlazione dei fenomeni occorrerà fare in modo che tali informazioni possano essere riportate all'interno dell'organizzazione in modo che possano essere gestite efficacemente dall'unico punto centralizzato responsabile del controllo, rappresentato dal Security Operations Center.

Un aiuto in tal senso può venire dal supporto offerto dalle applicazioni e dai servizi attivi nel mercato dell'intelligence, sia di tipo Open che Closed Source, che attraverso la rete, raccolgono, verificano ed analizzano le informazioni sull'insorgenza di nuovi attacchi, sulle azioni dei gruppi di attacco, sullo scambio di informazioni sui siti Social Media, sulla diffusione di nuove vulnerabilità, su eventuali mutamenti sociopolitici oppure attività ostili mirate ad attaccare l'organizzazione.

Una volta integrate le segnalazioni provenienti sia dall'ambiente interno che da quello esterno occorrerà fare molta attenzione nella corretta valutazione nel contesto delle condizioni di normalità, delle segnalazioni di attività ostili e nella attenta discriminazione dei falsi positivi.
Questo potrà avvenire sia sulla base dell'esperienza pregressa nel contesto di analisi che in base all'impiego di risorse in possesso dei necessari skills specialistici; a questo punto si potrà modellare una baseline sul normale comportamento dell'infrastruttura ICT dell'organizzazione da cui partire per valutare eventuali attività da considerare anomale che potrebbero essere preludere a tentativi di attacco.

Come abbiamo visto nel panorama sempre più complesso di dispiegamento delle nuove infrastrutture ICT è di fondamentale importanza mantenere il governo del livello di rischio associato agli asset informatici; un valido ausilio alle tecniche tradizionali può essere rappresentato dalle soluzioni tecnologiche che, opportunamente configurate e gestite, possono abilitare un livello di consapevolezza eccellente sulle possibili minacce e possono essere un valido supporto nelle azioni volte alla mitigazione dei rischi dell'organizzazione.

Roberto Obialero

Roberto Obialero. Esperto di sicurezza informatica, gestisce il Centro di Competenza IT Security nel Gruppo Finmatica, il cui core business è focalizzato nello sviluppo di soluzioni software nei mercati della Pubblica Amministrazione e della Sanità. A fine 2014 ha intrapreso la carriera di freelance avviando ulteriori collaborazioni con importanti società di consulenza e system integrator nel settore del mercato privato.

Può vantare un'esperienza trentennale nel campo ICT in ruoli principalmente tecnici e di sviluppo business in collaborazione con società nazionali ed internazionali di diverse dimensioni. Da 15 anni opera nel campo della sicurezza informatica occupandosi di progettazione di reti sicure, protezione delle informazioni, analisi e gestione del rischio, business continuity, vulnerability assessment, digital forensics, analisi e gestione di incidenti informatici supportate da apparecchiature SIEM.