Individuare gli utenti malintenzionati con l’User Behavior Analytics

I controlli di sicurezza convenzionali non sono efficaci contro alcuni tipi di minacce, e precisamente nei confronti del comportamento di alcuni utenti. Le anomalie nel comportamento degli utenti possono essere individuate soltanto con un approccio che prevede l’utilizzo dei big data e di algoritmi di machine learning.

L’**User Behavior Analytics** (UBA) può definire, se ben progettato, un modello di comportamento tipico di gruppi di utenti.

Principalmente il bersaglio di attacchi del genere sono i dati non strutturati (ad esempio email, pagine web etc.) poiché non sono facilmente controllabili. La media, tra la compromissione di dati e la sua individuazione, è di 146 giorni (fonte: FireEye), e di questo problema l’User Behavior Analytics può rappresentare una soluzione. Soluzione che è poco utilizzata nonostante l’evidenza: l’anello debole è rappresentato dal fattore umano. La maggior parte dei fondi destinati alla sicurezza è ancora impiegata in software tradizionali.

Cos’è l’User Behavior Analytics

Alla base dell’User Behavior Analytics c’è la distinzione tra tutto ciò che sembra *normale* attività dell’utente e quello che sembra non comune. Non a caso si è usato il termine *sembra* perché fin qui si tratta solo di sospetto comportamento non conforme; poi tocca all’apposito team investigare su quell’utente e su quel comportamento specifico.

Ricapitolando, l’UBA si basa sulla capacità di analizzare grandi quantità di dati, creare modelli e di identificare

comportamenti non simili a quelli previsti.

User Behavior Analytics in dettaglio

L'User Behavior Analytics raccoglie dati, sia strutturati che non strutturati, da diversi punti dell'intera infrastruttura. Da questi dati definisce cosa rappresenta un comportamento normale tenendo conto dei diversi contesti. Dopodiché continua a raccogliere dati cercando comportamenti non conformi a quanto definito in precedenza. I modelli di comportamento definiti, ovviamente, si adattano a nuove situazioni e nuovi ambienti previsti nell'infrastruttura.

Come dicevamo prima un'anomalia non è considerata ancora un rischio per la sicurezza ma solo un sospetto. Va dunque valutato l'impatto di tale comportamento. A tale scopo si può usare la classica equazione (**Figura 1**):



Rischio = Probabilità x Impatto

Dove, in questo caso, *probabilità* indica che il comportamento dell'utente è da ritenersi anomalo mentre *impatto* indica l'effetto e la criticità dell'eventuale accesso alle informazioni in esame.

Come tutti i sistemi basati sulla raccolta di dati si possono individuare per l'User Behavior Analytics tre elementi:

- *Data Analytics*: vengono raccolti i dati da più fonti.
- *Integrazione dei dati*: vengono integrati diversi tipi di dati disponibili e creati dei profili, per uno o più individui, sulla base di questi. Identificando i modelli di comportamenti leciti risulta poi immediato identificare le eventuali anomalie. Tali dati opportunamente trattati sono inviati ad un esistente sistema di sicurezza che si occupa della loro gestione.
- *Presentazione e Visualizzazione*: infine i dati raccolti

e trattati vengono presentati a diversi attori che si occuperanno delle azioni successive.

A cosa serve

L’importanza di uno strumento come l’User Behavior Analytics sta nel fatto che esso tiene conto di dati molto disomogenei come ad esempio la provenienza geografica dei dati, informazioni sugli utenti provenienti dall’infrastruttura di rete (accessi, permessi, etc.), dati sugli utenti provenienti dalle risorse umane, dati provenienti dai sistemi di sicurezza, etc.

Sono valutate anche informazioni che generalmente vengono ignorate dai tradizionali sistemi di sicurezza. Inoltre vengono presi in considerazione sia dati passati che dati attuali in modo da avere un quadro esaustivo della situazione.

Il fattore chiave degli strumenti dei sistemi di UBA è il tempo; attraverso delle operazioni di machine learning svolgono compiti in maniera molto rapida prendendo in considerazione anche più fonti e maggiori dettagli. In questo modo è possibile individuare comportamenti non conformi pressoché in tempo reale; ed è proprio questa caratteristica che ne fa uno strumento indispensabile in ogni organizzazione che si occupa della sicurezza in maniera proattiva.

L’User Behavior Analytics risulta utile anche durante la fase di **valutazione dei rischi** dove le regole precedentemente create possono essere utilizzate per identificare dei potenziali rischi di un’organizzazione legati al comportamento dei singoli utenti. Poiché comprendendo come gli utenti agiscono e isolando un comportamento lecito è possibile individuare gli utenti che potrebbero portare ad un problema di sicurezza.

Individuazione e protezione

Come detto, l'User Behavior Analytics si occupa della raccolta, dell'analisi e della gestione dei dati utenti, tutte operazioni noiose che vengono svolte da chi gestisce la sicurezza ed essendo ripetitive rischiano di generare errori. Permette, ad esempio, di determinare se un account è stato compromesso e se il traffico generato da questo account è lecito oppure necessita di maggiori investigazioni.

La piattaforma che si occupa dell'UBA può eseguire sia azioni indirette per un'ulteriore analisi (come ad esempio l'invio di email e alert vari, l'aggiornamento di dashboard etc.) sia azioni dirette (come ad esempio l'aggiornamento delle regole di un firewall o di un IPS, la disattivazione di un account etc.).

Mentre la maggior parte dei dati non è significativa, bastano poche informazioni che combinate tra loro contribuiscono ad identificare una minaccia. Qui sta la capacità nell'identificare un comportamento potenzialmente malevolo partendo da informazioni apparentemente insignificanti e non correlate. Comportamento non identificabile in breve tempo se non utilizzando appositi algoritmi per l'analisi dei dati. Inoltre bisogna considerare la natura di alcuni attacchi che prevedono un'escalation di privilegi, quindi *niente è come sembra*.

Consigli per l'implementazione

Ecco infine alcuni consigli utili in fase di implementazione di una soluzione che prevede un sistema di UBA:

- vanno raccolte tutte le informazioni possibili anche se appaiono insignificanti;
- va usato un tool "serio" di machine learning in modo da ridurre al minimo i falsi positivi;
- quando si scrivono nuove regole vanno prese in

considerazione sia le minacce interne sia quelle esterne;
- e le regole vanno sempre aggiornate in modo da tenere in considerazione i nuovi attacchi;
- non bisogna considerare nessun account innocuo (anche i più insignificanti dal punto di vista dei permessi);
- dopo aver implementato la soluzione UBA è necessario definire delle regole di base che all'inizio hanno il compito di definire cosa viene trattato come comportamento lecito;
- dopo l'implementazione e la definizione del comportamento di base è necessario un periodo di test utile per affinare le regole e adattare la soluzione all'ambiente.

Conclusioni

L'User Behavior Analytics si occupa quindi di collezionare, correlare e analizzare sia fonti interne sia fonti esterne come ad esempio informazioni di terze parti su possibili minacce al fine di creare modelli attendibili di comportamento.

Non solo gli algoritmi utilizzati nell'User Behavior Analytics permettono di creare modelli comportamentali riducendo al minimo la possibilità di falsi positivi ma permettono anche di valutare i possibili rischi e i processi di sicurezza in generale alla luce dei dati raccolti.

A cura di: **Gianluigi Spagnuolo**

Si interessa di sicurezza informatica, reti di sensori e ingegneria del sotware.

Attualmente si occupa pricipalmente dell'analisi dei dati.

Collabora con diverse riviste del settore scrivendo di programmazione e sicurezza

https://www.ictsecuritymagazine.com/articoli/individuare-gli-utenti-malintenzionati-con-luser-behavior-analytics/