Traffico di rete nella risposta agli incidenti: Implementazioni e Tecnologie

Introduzione

L'analisi del traffico o del flusso di dati è uno dei compiti più importanti da eseguire durante un'indagine interna al fine di confermare o negare l'esistenza di un incidente di sicurezza. Qualora un ambiente abbia preliminarmente previsto una buona infrastruttura preposta alla raccolta e all'analisi del traffico di rete, in caso di incidente il *team* dedicato alla sua gestione dovrebbe infatti essere in grado di raccogliere rapidamente informazioni quali registri di flusso, *endpoint* di comunicazione interni, componentistica malevola utilizzata nell'attacco, canali di esfiltrazione e così via

Al fine di sintetizzare quanto questa fonte di informazioni sia di vitale importanza in tale tipologia di indagini, è possibile elencare una serie di situazioni per le quali i dati di rete (oltre la seguente analisi e reportistica) risultano essenziali:

1. *Estrarre indicatori ed eventuali evidenze di compromissione*
2. *Confrontare i dati con sorgenti aperte e/o chiuse*
3. *Identificare le risorse coinvolte e movimentazioni laterali*
4. *Indicare lo scopo dell'intrusione*
5. *Costruire una "timeline" degli eventi*
6. *Indicare il vettore del'intrusione*

Quanto detto risulta ancora più importante se si considera che in molte situazioni potremmo trovarci nella necessità di acquisire dettagli da comunicazioni destinate a servizi

interni che potrebbero non essere in grado di mostrare l'intero *payload* della richiesta (si pensi, ad esempio, ai servizi web nell'uso dei metodi HTTP POST e PUT).

In questo caso, pur avendo a disposizione *log* locali provenienti da host compromessi, non saremo generalmente in grado di vedere quale sia stato l'intero contenuto della richiesta originale. Questo è solo un esempio di come è essenziale implementare una buona strategia di acquisizione del traffico di rete per supportare il team di gestione degli incidenti.

Al fine di elencare quali potrebbero essere le tecnologie e le attività dedite all'acquisizione ed al monitoraggio di tale flusso di informazioni, è necessario elencare alcune grandi categorie di elementi in cui queste potrebbero ricadere:

1. *Collezionamente basato sul "full packet logging" sulla base di eventi di*
2. *Collezionamente basato sul "full packet logging"come condizione*
3. *Collezionamento basato sul "full packet logging" in base a criteri specifici (allorchè, per esempio, il flusso vada ad interessare una DMZ o particolari nodi di rete).*
4. *Collezionamento basato sul*

Ciascuna di queste implementazioni ha i suoi punti di forza e di debolezza, strettamente correlati allo spazio di *storage* disponibile, alle policy di ritenzione dei dati, oltre che alle fasi antecedenti e successive di un incidente di sicurezza.

Per ragioni legate al *main topic* di questo elaborato, non verranno approfonditi nel dettaglio tutte le possibili implementazioni di tali tecnologie, ma, in linea generale, esistono due grandi modalità principali che è possibile utilizzare per eseguire una raccolta dei dati di traffico: analisi del flusso (*NetFlow*) e analisi dei pacchetti .

Sistemi “NetFlow”

Ogni “*flusso di dati*” risulta caratterizzato da una serie specifica di identificatori.

Di solito questi identificatori sono *IP di origine*, *IP di destinazione*, *porta di origine*, *porta di destinazione*, *protocollo* e tutti i *metadati* che definiscono quelli che vengono comunemente chiamati “*canali di traffico*“.

Qualora anche solo uno di questi identificatori vada a subire delle modifiche durante una sessione di comunicazione, un nuovo flusso di traffico viene generato. Per una singola connessione client-server, possiamo avere flussi di traffico multipli poiché il *client* molto spesso va a creare connessioni multiple da una porta sorgente diversa per ogni singola sessione di comunicazione.

I dispositivi di rete moderni come *router* o *switch* eventualmente coinvolti nel canale di comunicazione generato da un *host* interno da/veso internet, possono generare flussi di dati (in genere *NetFlow* v.5) sulla base delle specifiche del traffico che si trovano a gestire.

E’ bene chiarire che i dati così ricavati ed inviati al collector *NetFlow* sono dati “*statistici*” sul traffico in transito e non risultano copie di pacchetti come possiamo osservare per le implementazioni basate su porte di SPAN e in generale nelle tecnologie DPI.

Inoltre, i dati *NetFlow* sono spesso campionati per ridurre i requisiti di archiviazione. Una ipotetica implementazione di una soluzione di raccolta e analisi dati di tipologia *NetFlow* può essere rappresentata nella Figura 1:



Figura 1

Analisi del NetFlow nella gestione degli incidenti

Soluzioni dedite all'analisi del *NetFlow* vengono spesso utilizzate dagli *incident responders* ed in generale dagli specialisti di sicurezza come risorsa utile al rilevamento di anomalie e di comportamenti classificabili come "*anomali*" rispetto ad una *baseline* di utilizzo *pre-osservata*.

L'analisi delle anomalie, indifferentemente dal fatto che sia focalizzata ad una particolare indagine o che sia eseguita come controllo generico, viene utilizzata al fine di rilevare particolarità nel traffico di rete che vadano a discostarsi dai normali modelli di comportamento previsti.

Sulla base di quanto appena affermato ed in considerazione delle sei fasi della gestione degli incidenti (preparazione, identificazione, contenimento, eradicazione, recupero, apprendimento), l'implementazione e l'analisi del traffico di rete risulta molto utile nella prima e nella seconda di queste.

Tali pratiche infatti possono essere utilizzate come ausilio all'identificazione ed alla categorizzazione di eventi sospetti e potrebbe fornire informazioni molto utili per rintracciare e contenere eventuali azioni dannose oltre che agevolare, in qualche caso, le pratiche di attribuzione.

Nella pratica, risultano inoltre molto utili al fine di provare o smentire azioni mirate all'esfiltrazione di dati durante l'investigazione di incidenti sia accertati che sospetti. La *Figura 2* mostra un grafico derivato da una reale attività di risposta ad un incidente con il quale è stato possibile individuare una attività di *data exfiltration* mediante *cover channel*:



Figura 2

La linea blu rappresenta la *baseline* del comportamento per quanto concerne il normale traffico in uscita. La linea rossa è un derivata dall'analisi dei metadati del traffico in uscita dopo l'installazione, in uno dei sistemi interni, di un *malware* progettato per lo spionaggio industriale non precedentemente rilevato.

Rispetto ad una *baseline* inferiore a 1 GB di traffico in medio, c'è un picco di quasi 14 GB nel periodo di tempo estratto, a dimostrazione di una sorta di attività anomala.

Riassumendo come l'analisi del flusso di rete tramite *NetFlow* possa essere utile nel rilevare comportamenti anomali nelle attività di risposta agli incidenti, può essere sufficiente pensare alle capacità che questa pratica offre in termini di "*visione complessiva*" di ciò che è accaduto o che sta accadendo.

I *team* dediti alla risposta di incidenti informatici infatti, hanno spesso necessità di trovare delle risposte molto rapidamente. Per tale motivo, in molti casi, questi non necessitano, almeno nelle prime fasi del ciclo IR, di una visione troppo dettagliata degli ambienti in cui si trovano ad operare.

Implementare sistemi e tecnologie dedite alla raccolta e all'analisi del traffico NetFlow, risulta nei fatti una soluzione davvero efficace se il nostro scopo risulta quello di possedere una capacità di visione e controllo a "*largo spettro*" del nostro ambiente.

Sistemi "*Full Packets Log*"

Le attività di estrazione ed analisi dei flussi di rete basati su tecnologie DPI o più genericamente su tecnologie "*full packet log*" del flusso dati in transito sono solitamente implementate al fine di arrivare a possedere la capacità di approfondire nel dettaglio singoli eventi occorsi all'interno

dell’ambiente in questione.

Un aspetto di estrema importanza di questa pratica è quello di collezionare evidenze riguardo attività ostili in modo da supportare sia le attività di investigazione interne che esterne, essere di ausilio ad eventuali indagini penali da parte degli organi competenti, oltre che di acquisire, in dettaglio, indicatori di compromissione utili a valutare il grado di estensione della minaccia, nonchè eseguire pratiche di “*threat hunting*” sulla base di quanto osservato nel dettaglio (per esempio diffondendo nella rete *agents* che vadano alla ricerca di specifici *payload* malevoli estratti in precedenza).

Tale tipologia di analisi infatti consente di avere un tale dettaglio di informazioni che in molti casi permette di ricomporre ed identificare quelli che sono stati, per esempio, i *tool* utilizzati nelle prime fasi di intrusione, quali tecniche o componentistiche malevole sono state utilizzate per raggiungere un certo grado di privilegi all’interno dei sistemi colpiti o per archiviare l’esigenza di un accesso continuato al network in esame (c.d. *persistenza*).

Inoltre, c’è anche da dire che implementare tali tecnologie permette una c.d. analisi retrospettiva di quanto transitato all’interno dell’ambiente, per esempio nel confronto fra un flusso dati non recente con indicatori noti solo all’atto dell’analisi.

In tali casi, per esempio, è possibile avere evidenze di attività ostili occorse in passato per le quali oramai i *tool* utilizzati sono stati cancellati o per le quali non ci sono evidenze dirette nel presente.

Ovviamente, in considerazione di quanto appena enunciato, l’implementazione di tali tecnologie potrebbe risultare, ad una prima e veloce analisi, sempre la soluzione migliore da possedere al fine di riuscire ad avere buone capacità di

risposta ed analisi.

In effetti, sotto l'ottica di un professionista di settore, tali capacità rappresentano il meglio di quanto si possa desiderare. Tuttavia, nelle prime fasi di risposta ad un incidente, un così approfondito livello di dettaglio potrebbe addirittura sovraccaricare il gruppo di analisi di una tale quantità di informazioni tale da dover considerare il rischio di perdersi fra l'esclusione di falsi positivi nonchè nell'esame di eventi totalmente estranei alla specifica missione.

Oltremodo, l'inclusione di metodologie FPC/DPI per la raccolta e l'analisi del traffico non può fare a meno di considerare la sempre parziale capacità di copertura dell'ambiente da controllare nonchè i requisiti di spazio necessari per l'archiviazione.

All'interno di ambienti molto estesi e distribuiti infatti risulta quantomeno difficile posizionare centinaia di sistemi c.d. "*packets sniffers*" (TAP o periferiche per la cattura dei pacchetti) oltre al fatto che un progetto con tali requisisti potrebbe raggiungere costi davvero gravosi.

Come accennato in precedenza, nel caso di una intrusione sospetta o accertata, agli analisti viene solitamente chiesto di muoversi molto rapidamente al fine di trovare risposte rapide su quanto accaduto, e molto difficilmente avranno il tempo e le capacità (in termini di numero di elementi) per muoversi all'interno di vari *terabytes* e *terabytes* di log, oltre al fatto che è impensabile approcciare la missione partendo dall'analisi delle singole sottoreti o sistemi.

La via migliore e maggiormente rapida per capire quanto accaduto, è muoversi avendo a disposizione qualcosa che permetta di avere una visione più ampia della rete, e solo in un secondo momento approfondire nel dettaglio quanto trovato di interesse.

Un caso a metà: “*Full Packets Log*” su eventi di sicurezza

Come la stessa parola suggerisce, una piattaforma di tipo “full packet log” basata su eventi permette di registrare il completo traffico di sessione relativo ad un probabile (o presunto, in considerazione dei falsi positivi) evento di sicurezza.

Le periferiche di rete che consentono una tale tipologia di approccio nel controllo del traffico sono molto spesso basate su firme (*signatures*) ed una delle sue maggiori implementazioni nel settore è sicuramente SNORT.

L’approfondimento dello specifico funzionamento delle periferiche di tipo IDS/IPS è fuori lo scopo di questo elaborato, tuttavia, è possibile chiarire che, come anticipato, la loro logica spesso è basata sul riconoscimento di *pattern* specifici, solitamente mantenuti in costante aggiornamento, che si devono verificare all’interno del flusso dati in esame affinchè un evento possa essere sollevato.

Semplificando molto l’intero ciclo di *detection* di una eventuale intrusione mediante tali sensori, un *evento* potrebbe essere classificato come qualcosa di possibile interesse per l’analista.

Tali tecnologie hanno solitamente lo svantaggio di dover essere mantenute in costante aggiornamento. La loro efficacia inoltre si basa sul riconoscimento di qualcosa già classificato come malevolo dalla comunità di sicurezza. Le firme su cui tali apparati basano la loro efficacia infatti, fanno parte di un set di regole per il riconoscimento di *payload* ostili che potrebbero essere evase e/o illuse (eh già, pensi che sia aria quella che respiri ora? cit. *Morpheus*).

Infine, il *tuning* di tali apparati è essenziale. Sensori non ben configurati potrebbero portare alla mancata *detection* di

un reale incidente o sovraccaricare il gruppo di analisti con una tale mole di informazioni da rendere difficile il concentrarsi nella discriminazione di un reale evento di sicurezza.

Tuttavia, questi restano dispositivi molto utili e dalla reale importanza nell'analisi degli incidenti di sicurezza. Un dispositivo ben configurato e mantenuto è in grado, molto spesso, di indirizzare nella giusta via una eventuale analisi e di accorciare di molto i tempi di risposta e contenimento della minaccia.

Solitamente tali sensori sono posizionati all'ingresso di reti sensibili e sono, in genere, in grado di riconoscere molto efficacemente minacce dalla diffusione massiva e generalista. La loro capacità di risposta si abbassa inesorabilmente nel confronto con attacchi mirati, in risposta a minacce persistenti avanzate (APT) o *malware* particolarmente furtivi.

Poco utile, infine, ricordare che qualora un flusso in transito, seppur realmente malevolo, non venga classificato dal sensore come tale, non ci saranno i dettagli (e dunque il "*full packet log*") di quanto accaduto.

Implementazione di un sistema "*Full Packet Log*"

Allorchè un *Security Architect* si trovi davanti la necessità di soddisfare dei requisiti (solitamente abbastanza stringenti in termini di *bugdet*) nell'implementazione di architetture di rete che consentano l'acquisizione dell'interno flusso dati, egli problabilmente dovrà considerare alcune variabili che andranno ad influire sul piano delle capacità operative nell'ottica di soddisfare determinati requisiti di prestazione.

Le maggiori questioni a cui trovare risposta in tali tipologie

di progetto sono solitamente legate alle direttive del cliente, alla natura ed alla sensibilità dei sistemi da proteggere, nonchè al già citato *budget* a disposizione.

Solitamente, esse sono le seguenti:

- *Dove, fisicamente, tale sistema dovrebbe essere posizionato?*
- *Quali sono i servizi, le sottoreti ed i sistemi da controllare?*
- *Quali sono le aree, i sistemi ed i servizi critici per il business in questione?*
- *Quali sono le richieste per la ritenzione dei dati?*
- *Quali sono i requisiti di ridondanza dell'infrastruttura?*
- *E' necessario orientare l'applicazione verso sistemi commerciali o open?*

Come è facile immaginare, non esiste una risposta omni-comprensiva a tali questioni.

Ovviamente è necessario tener conto delle influenze dell'organizzazione riguardo le sue inclinazioni sull'hardware, sul software, le capacità operative attese etc. etc., ma, in linea generale, un tale sistema di controllo è sempre posizionato fra un servizio / rete "fidato/a", ed un servizio / rete "non fidato/a".

Un tale scenario potrebbe essere rappresentato da un segmento di rete interno (LAN) che sarà la nostra "*zona fidata*", ed Internet, che rappresenta la zona "*non fidata*".

Solitamente, un' architettura di rete che vada ad implementare un sistema per la raccolta completa del traffico di rete in grado di ben supportare le attività di risposta agli incidenti, è simile a quelle rappresentata nella Figura 3:

Figura 3

Posizionando il sensore prima del NAT di rete permetterà ad un eventuale CERT/SOC di identificare immediatamente eventuali sistemi compromessi all'interno del network in esame e di passare da subito alle fasi di "*remediation*".

Al contrario, un posizionamento del sensore dopo il NAT, costringerà gli specialisti ad eseguire analisi approfondite sull'intera sottorete prima di poter identificare con certezza gli host coivolti dall'infezione prima di passare alle successive fasi di contenimento e bonifica.

Una immagine rappresentativa è quella mostrata nella Figura 4:



Figura 4

Parlando in via generale, è bene ricordare che il posizionamento delle sonde nella fase progettuale di tale tipologia di sistemi risulta di estrema importanza. Da questi dipende l'intera capacità ed efficacia dell'infrastruttura di monitoraggio posta in essere

Tale concetto, inoltre, si applica all'interno panorama delle tecnologie per la raccolta di dati e metadati del traffico in transito, siano esse FPC / DPI e/o NetFlow.

Conclusioni

Come visto, l'analisi e le informazioni provenienti da apparati in grado di supportare protocolli e standard per la raccolta del traffico in transito svolgono un ruolo cruciale nelle attività di risposta agli incidenti. Le aziende e le organizzazioni che vogliano implementare un buon ambiente di controllo in grado di supportare efficacemente un processo di indagine interna in risposta ad eventi di sicurezza, dovrebbero necessariamente pensare a tecnologie in grado di fornire sia una visione ad alto livello dell'intera infrastruttura, sia una visione nel dettaglio per quanto di

interesse.

Poichè, come analizzato, le soluzioni progettate per la raccolta totale del traffico di rete non si rivelano totalmente appropriate nel lungo periodo in considerazione dei requisiti di calcolo e di conservazione dei dati, il protocollo *NetFlow* potrebbe essere utilizzato come risorsa utile al rilevamento di eventuali anomalie non previste.

Tecnologie di tipo FPC/DPI di contro, fornendo una visione maggiormente dettagliata di quanto accaduto, potrebbero essere utilizzate, su richiesta, a supporto di analisi specifiche che vadano a considerare un limitato numero di settori, servizi o sottoreti.

In una situazione ottimale, un'organizzazione o un'azienda dovrebbe infatti essere in grado di supportare un team di risposta agli incidenti includendo la capacità potenziale di effettuare una raccolta FPC/DPI (almeno per le aree critiche per il *business*) all'interno del proprio piano di risposta agli incidenti.

Oltre quanto affermato, una buona progettualità nelle architetture di rete e nel posizionamento di sistemi e tecnologie dedite alla raccolta ed all'analisi del traffico, rimane essenziale per una accurata ricostruzione dei fatti.

Bibliografia

- *Network Security with Netflow and IPFIX: Big Data Analytics for Information Security by Omar Santos – Ciscopress*
- *CCNA Cyber Ops SECOPS 210-255 Official Cert Guide by Omar Santos – Ciscopress*
- *The Tao of Network Security Monitoring: Beyond Intrusion Detection by Richard Bejtlich – Tenable Network Security*
- *Security Monitoring: Proven methods for Incident*

Detection on Enterprise Networks by Chris Fry, Martin Nystrom – 0'Reilly

- *Crafting the InfoSec Playbook: Security Monitoring and Incident Response Master Plan by Jeff Bollinger – O'Reilly*

Articolo a cura di **Emanuele De Lucia**

L'articolo Traffico di rete nella risposta agli incidenti: Implementazioni e Tecnologie proviene da ICT Security Magazine.

https://www.ictsecuritymagazine.com/articoli/traffico-di-rete-nella-risposta-agli-incidenti-implementazioni-e-tecnologie/