Milano, 24 gennaio 2017

LO STATO DELL'ARTE DELLE INVESTIGAZIONI DIGITALI E DELLA CYBER THREAT INTELLIGENCE

Le attività di Cyberspionaggio preoccupano, come conseguenza dei fatti recenti riportati dalla cronaca dei giornali, e le aziende italiane ripensano la propria capacità di difesa e intelligence: ne abbiamo parlato con ***Gerardo Costabile****, Esperto di Cybersecurity, Intelligence e Digital forensics, Professore di Sicurezza Aziendale all'Università Telematica San Raffaele di Roma, Presidente IISFA (International Information Systems Forensics Association).*

TIG. Qual sono oggi i principali trend della Cyber intelligence e della Digital forensic che si osservano oggi?

Gerardo Costabile. L'argomento tecnico che Aziende e Istituzioni dovranno affrontare nel 2017 sarà l'implementazione di un **maturity model della Cyber threat intelligence** a supporto delle attività di prevenzione e *detection*; l'Incident response e la Digital forensic servono in una **fase successiva,** ma possono essere "guidate" da una buona attività di Cyber intelligence. Non a caso di parla in gergo di **"Cyber Threat Hunting"**. La Cyber threat intelligence è un concetto che innanzi tutto va correttamente inquadrato dal punto di vista terminologico: ci sono varie interpretazioni a seconda dell'interlocutore. A titolo esemplificativo ci sono topic di cyber intelligence per la sicurezza nazionale, per il monitoraggio di informazioni in rete o sui social network, sul deep web e sul dark web, con un approccio per "semantica" multilingua, dove OSINT e HUMINT possono trovare un punto di sintesi. Un altro discorso ancora è l'intelligence per prevenire le frodi, verificare se ci sono **campagne di phishing** che stanno attaccando i servizi bancari, o se c'è vendita di credenziali e carte di credito nell'underground del black market (oggi si direbbe nel **dark web**). Avere prima queste informazioni permette di prevenire gli usi illeciti, a tutela di clienti, dipendenti, cittadini.

Una definizione più specifica di Cyber threat intelligence potrebbe essere questa: **disporre di un "knowledge" basato su evidenze tecniche** (ad esempio dati, meccanismi, modalità, IoC, etc) in ordine a minacce emergenti o attuali alla cybersecurity dei propri asset. Prendiamo il caso del malware presumibilmente utilizzato dai fratelli Occhionero. Al di là delle informazioni giornalistiche è fondamentale, per un Security manager, **avere informazioni tecniche adeguate per fare un'analisi operativa nella propria infrastruttura, per comprendere se si è stati sotto attacco o meno.** Una buona Cyber threat intelligence mi può servire per fare questi "*controlli del giorno dopo*" o, meglio ancora, *"del giorno prima"*. Avere gli indirizzi IP dei server americani a cui il malware inviava i dati "spiati" mi consente di metterli in blacklist; comprendere tecnicamente il funzionamento di un trojan di cyberspionaggio mi consente di andare oltre ai normali antimalware, lavorando su indicatori di compromissione più "complessi", oltre che mediante "behavior analytics". In ogni caso questa materia andrebbe affrontata sia con approccio tattico sia con approccio più strategico.

TIG. Quale è la situazione dell'Italia su questi temi?

Gerardo Costabile. L'Italia è un po' indietro: quello che servirebbe è **fare in modo che il SOC aziendale sia più *intelligence-driven*.** La parte di monitoraggio e detection deve essere "guidata" da un patrimonio informativo e da una capacità di analisi che si è sviluppata nel

tempo, tecnica e meno tecnica, esterna ed interna. In ambito internazionale, in un ipotetico Maturity model, si parla difatti di *"cyber threat fusion".*
In generale, in ambito di contrasto al c.d. "rischio cyber", si osservano a livello internazionale 3 possibili approcci (anche sovrapponibili):

1) **Guidato da ipotesi**: in base alla conoscenza delle vulnerabilità *et similia*, si fanno delle ipotesi sulla possibilità di essere potenzialmente attaccati/attaccabili.
2) **Basato su Indicatori di Compromissione (IoC)**: gli IoC sono informazioni tecniche che un SOC può subito applicare per verificare se è avvenuta una compromissione, se è presente un malware sui sistemi. Comprendono anche delle regole sulle attività da svolgere in caso di compromissione, rendendo quindi tutto il processo di Incident Management molto più efficiente.
3) **Basato su analisi comportamentali (behavior analytics) e su dati statistici/Machine learning**: in caso di anomalie rispetto a comportamenti (Anomaly detection), osservate su reti o sistemi, scattano in automatico degli alert da gestire.

In Italia abbiamo un mercato a macchia di leopardo e – purtroppo – **si sottovaluta il ruolo degli analisti rispetto all'acquisto di piattaforme**. Inoltre, personalmente sono abbastanza scettico su un approccio tecnico di tipo statistico senza aver fatto un percorso basato su regole e indicatori, con la speranza di "saltare" più velocemente il gap tecnico. Si rischia di avere una mole enorme di falsi positivi e di non avere le corrette competenze per la gestione di questi processi.

TIG. Il modello preferibile per queste attività è in house o in outsourcing?

Gerardo Costabile. Dal punto di vista tecnologico può essere in house oppure in outsourcing, dipende sostanzialmente dal modello generale di gestione delle infrastrutture ICT scelto dalla singola realtà. Se ad esempio una grande banca avesse scelto un modello di gestione interno, è probabile che avrà anche la Cyber threat intelligence al proprio interno: invece un istituto più piccolo - per snellire le operazioni - potrebbe avere scelto un modello tecnologico in outsourcing (e quindi anche la security). C'è poi anche una **scelta ibrida**: c'è chi fa gestire alcuni processi o un primo livello di alert all'esterno, per poi "prendere in carico" il processo in caso di classificazione ad un certo livello di incidente o, analogamente, si può decidere di dare all'esterno solo notte e week end, per mere motivazioni aziendali sulla turnistica.

TIG. Cosa ci possiamo aspettare per il 2017 sul fronte dell'utilizzo di soluzioni di Cyber threat intelligence?

Gerardo Costabile. Oggi il principale limite dell'attuale (e pressochè timido) approccio alla Cyber threat intelligence è il fatto che **queste analisi sono ancora sconnesse agli aspetti di risposta in caso di incidente**. Si ottengono delle informazioni ma sono scollegate tra loro, c'è una manualità eccessiva e numerosi automatismi ancora da creare. La connessione diretta tra le informazioni, il contesto, le regole di contrasto tecnologico sono ancora tutte da creare; chi ha cominciato a lavorare con questo obiettivo, deve ancora ottimizzare il tutto,

chi invece è più indietro dovrà colmare il gap. Oggi il problema di chi gestisce le infrastrutture (pensiamo ad esempio a un centralino telefonico di una filiale bancaria o di una grande azienda, che può essere attaccato come testa di ponte per ulteriori intrusioni) deve essere in grado di capire se la minaccia è applicabile al suo contesto. Come è configurato l'apparato? Esiste una black list? Quali sono le vulnerabilità? **La mancanza di competenze interne può essere un grave problema**; analogamente è fondamentale una conoscenza interna delle proprie infrastrutture oltre che una capacità di connettere quello che è il contesto interno con le minacce esterne (come già accennato, questo processo potremo chiamarlo "Cyber threat fusion").

TIG. Con riferimento invece alle attività di Digital forensics, cosa dovrebbero fare le aziende per poter rispondere in modo efficace in caso di incidenti cyber?

Gerardo Costabile. Oggi si osserva una forte debolezza delle aziende sul fronte della Digital forensics. Ci sono anche diverse prospettive del problema: da un lato abbiamo il contrasto alle frodi interne, la **risposta a comportamenti fraudolenti dei dipendenti**, che oggi avvengono anche sfruttando le tecnologie. Pensiamo al caso di un dipendente che si crea una busta paga in più, o al furto di *know how* ed invio dei dati alla concorrenza. Tutto questo lascia (o può lasciare) delle **tracce** che possono essere considerate a supporto delle classiche attività investigative sull'infedeltà aziendale, ma per avere processi solidi ci vogliono competenze, esperienza e strumentazione adeguata allo stato dell'arte. In questi casi, comunque, è abbastanza facile appoggiarsi a consulenti esterni, **sperando che non si siano maneggiate in modo scorretto le informazioni prima dell'intervento** di un esperto.
Dall'altro lato – invece - abbiamo le attività di *digital forensics* legate alla cybersecurity o al cyber crime (ad esempio per capire come è avvenuto un attacco cyber o le attività di cyber spionaggio dall'esterno). In questo caso, servono delle competenze ancora più specialistiche ed è necessario a mio avviso avere al proprio interno almeno una persona che faccia da *trait d'union*, che sia in grado di gestire una serie di aspetti abilitanti le successive indagini informatiche. Meglio ancora se si decide di **far evolvere un SOC in un CSIRT**, con le **competenze interne sia di *incident response* che di *digital forensics***. Pensiamo ad esempio ad un attacco informatico al sito web dell'azienda: il responsabile della tecnologia ha una sola priorità, rimettere tutto in funzione il prima possibile, per una corretta business continuity. Invece chi è esperto di digital forensics sa che intervenendo subito in modo non corretto si **rischia di cancellare delle tracce** che - analizzate - potrebbero aiutare a capire l'attacco e a risalire alla sua fonte. Una persona interna (in taluni contesti può andare bene anche una persona dell'area Legale con competenze di cybersecurity) deve essere in grado di individuare il giusto *trade-off* tra esigenze diverse ed applicare (o far applicare) la giusta accortezza nella fase di *triage*, *first response* e di *post incidente*, perché tutto quello che viene fatto in questa fase avrà delle conseguenze dopo.

A cura di:
Elena Vaciago, The Innovation Group