Insider Threat: tipologie di minacce e contromisure

Author : Mattia Siciliano

Date : 28 novembre 2018

Ormai negli ultimi 5 anni riscontriamo un'evoluzione del mercato della Cybersecurity da parte delle organizzazioni pubbliche e private che sempre più spesso ricorrono ad un adeguamento delle tecnologie e dei programmi legati alla gestione del rischio Cyber.

Solo nel 2018 abbiamo dato seguito all'attuazione di due importanti direttive europee: la Direttiva 2016/679 (GDPR) per la protezione della privacy e la Direttiva (UE) 2016/1148 (NIS – Network and Information Security) per la gestione degli incidenti di sicurezza informatica e relativa comunicazione verso terzi.

Molto spesso però si dimentica che la parte più importante del rischio Cyber è legata e generata dai *dipendenti dove gli strumenti attuali non riescono sempre ad essere efficaci*; pertanto risulta importante pensare ed attuare un approccio innovativo di gestione del rischio Cyber, che contempli sia gli aspetti tecnologici sia l'"human factor" [1].

L'elemento più ricorrente legato al rischio cyber e che sempre più spesso viene citato da report internazionali come Verizon, è il Data Breach, ovvero la fuga di dati, in cui l'elemento minaccia definito come Insider Threat rappresenta uno dei fattori principali.

In questo ultimo anno, nel mondo si sono registrati oltre ***53.000 incidenti e 2.216 data breach confermati di cui circa il 30% sono legati alla minaccia Insider Threat;*** *di questi****,*** *il 28% ha coinvolto attori interni alle organizzazioni, mentre il restante 2% ha coinvolto fornitori/partner*. Quasi la metà (48%) dei Data Breach è relativa ad attività di hacking di cui le principali motivazioni sono di tipo finanziario (76%); si riscontra altresì un aumento dei Data Breach in ambito Sanitario e PMI[2].

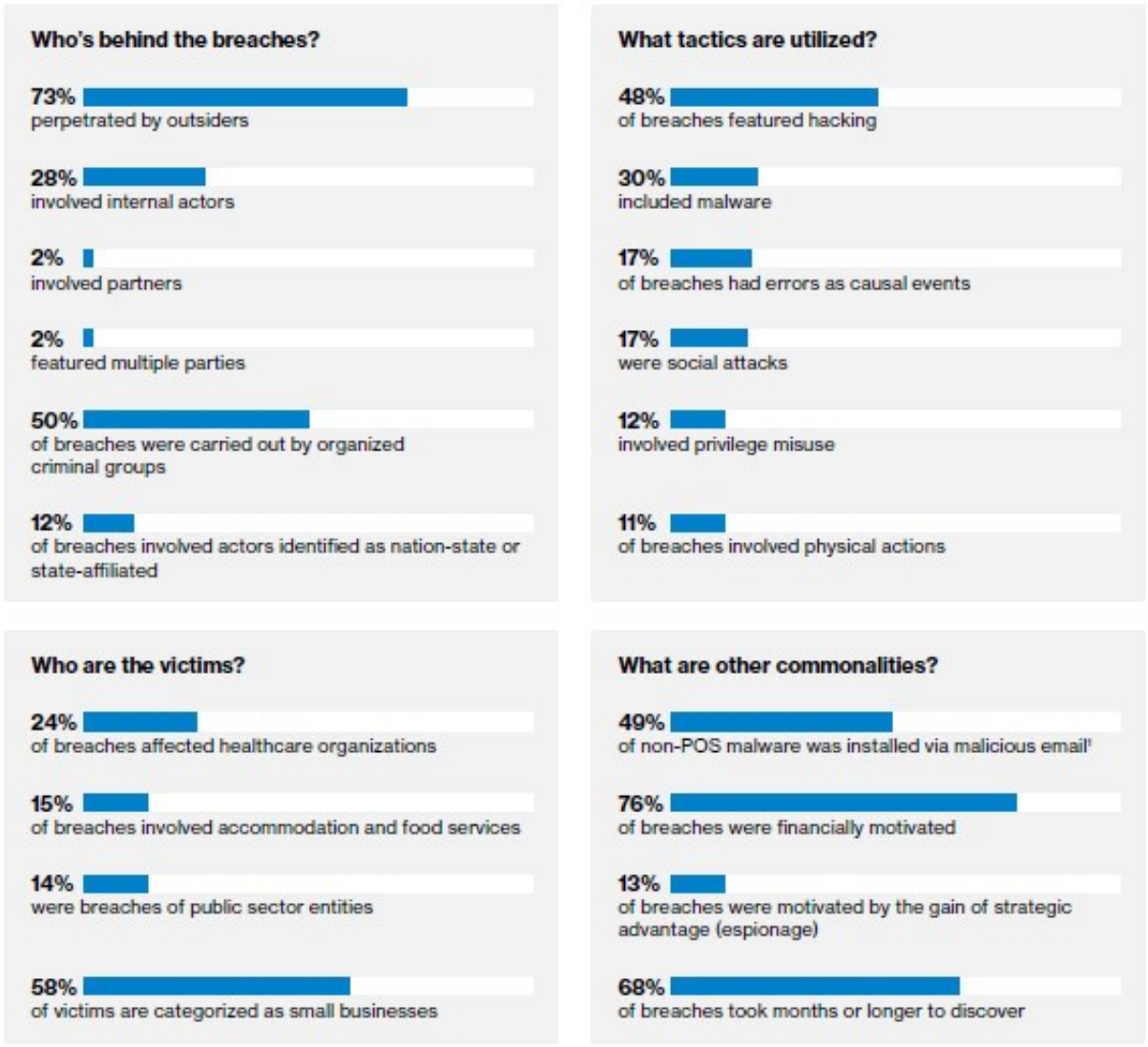

Figura 1 - Summary of findings from DBIR 2018

Le aziende e i responsabili della cybersecurity, stanno quindi iniziando a valutare e prevenire eventuali minacce da Insider.

Ma che cosa si intende per Insider Threat? Insider Threat è una minaccia dannosa per un'organizzazione che proviene da persone interne all'organizzazione, come dipendenti, ex dipendenti, appaltatori o soci in affari, che dispongono di informazioni interne relative alle pratiche di sicurezza dell'organizzazione, ai dati e ai sistemi informatici.

La minaccia può comportare la frode, il furto di informazioni riservate o di valore commerciale, il furto di proprietà intellettuale o il sabotaggio di sistemi informatici[3].

La minaccia di utilizzo e/o vendita di informazioni privilegiate da parte dei propri dipendenti

(fornitori e/o venditori) è uno dei maggiori problemi irrisolti in materia di sicurezza informatica. Le aziende sono certamente consapevoli del problema, ma raramente dedicano le risorse o l'attenzione esecutiva necessaria per risolverlo.

La maggior parte dei programmi di prevenzione sono insufficienti e si concentrano esclusivamente sul monitoraggio dei comportamenti senza prendere in considerazione le norme culturali e di privacy[4].

L' Insider può appartenere a quattro categorie:

- **Pedine (Pawns)**. Questi sono i dipendenti che vengono manipolati da qualcun altro, di solito un hacker esterno, al fine di farsi aiutare a commettere il crimine. *Esempio: un dipendente diventa bersaglio di un attacco di spear phishing e scarica inconsapevolmente un malware sul desktop consentendo all'hacker di infiltrarsi nell'organizzazione*.
- **Persona Incompetente (Goofs)**. Si tratta di dipendenti non intenzionalmente maliziosi o che deliberatamente danneggiano i propri datori di lavoro. Sono spesso soggetti che agiscono per ignoranza o anche per dolo, credendo di poter aggirare le politiche di sicurezza. *Esempio: un dipendente ignora le procedure e le soluzioni di sicurezza interne per la trasmissione di informazioni confidenziali (server dedicati, aree cloud aziendali, etc) ed invia le informazioni tramite la posta aziendale non crittografata o peggio ancora su un CD, USD drive*. Tali azioni sempre più spesso rappresentano una minaccia per i datori di lavoro. Gartner indica che circa il 90% degli incidenti interni è causato da personale incompetente.
- **Collaboratori (Collaborators).** Si tratta di addetti ai lavori che collaborano consapevolmente con un altro soggetto, di solito esterno all'azienda, al fine di perpetrare un crimine contro il proprio datore di lavoro. Sono pienamente consapevoli delle loro azioni e del loro ruolo nel crimine. Spesso vendono attivamente i propri servizi ai criminali che incontrano su forum di social media e sul deep web.
- **Lupi solitari (Lone wolves).** Questi attori agiscono da soli, senza alcun collaboratore esterno che li manipoli e sono soggetti che pur avendo bassi privilegi, accedono ad informazioni privilegiate/sensibili. Peccato che le organizzazioni spesso si preoccupino più degli utenti con privilegi elevati come amministratori del database o amministratori di sistema, che dei lupi solitari.

Rispetto alle categorie di cui sopra, i controlli disponibili e le tecnologie emergenti nel mercato, sono limitate rispetto alle azioni del malintenzionato coinvolto in attività non autorizzata.

La figura seguente mostra come l'uso della tecnologie (in verde) e l'approccio da seguire (in blu) cambia rispetto al tipo di Insider, da cui l'organizzazione deve proteggersi.

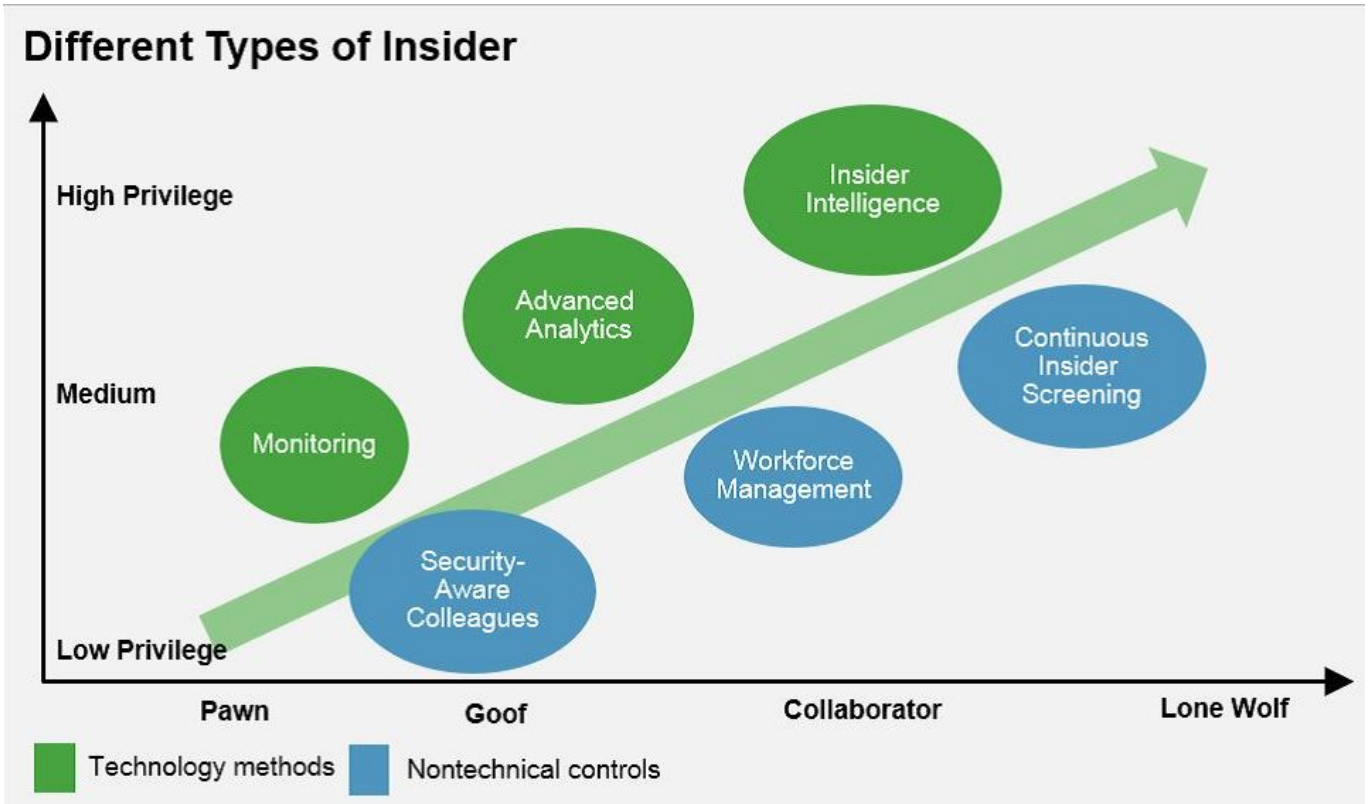

Figura 2 - Different types of Insider - Gartner source

I manager di cybersecurity sempre di più devono adottare un approccio innovativo e proattivo sulla base di tre elementi:

- **La microsegmentazione**, consente all'organizzazione di identificare le aree ad alto rischio adottando un approccio mirato di monitoraggio e attenuazione delle minacce. In tal senso si identificano i gruppi di dipendenti in grado di provocare un elevato danno all'Azienda e si sviluppano interventi mirati per limitarne il rischio.
- **Il cambiamento culturale**, permette di identificare in anticipo eventi di rischio dannosi o azioni negligenti da parte dei dipendenti, ponendo l'azienda in una fase preventiva anziché reattiva. Ciò è possibile se i dipendenti si sentono coinvolti nel processo di "Cyber-Hygiene" di cui i dirigenti aziendali sono i primi promotori e sostenitori.
- **La tecnologia**, che consente all'organizzazione di identificare e interrompere le attività da parte degli Insider, molto prima nel ciclo di vita della minaccia stessa.

Tutti gli elementi dipendono molto dalla strategia aziendale, dal livello di consapevolezza dell'azienda rispetto alle minacce Cyber e dalle azioni intraprese delle diverse funzioni aziendali (es. Direzione Generale, CIO, Compliance, CFO, HR, Legale, etc).

Per quanto riguarda la tecnologia, esistono ad oggi 3 soluzioni avanzate di rilevamento delle minacce interne "Insider Threat", come alternative ai tradizionali sistemi di prevenzione e perdita di dati (DLP - Data Loss Prevention):

1. Analisi del comportamento degli utenti e delle entità (UEBA);
2. Monitoraggio del dipendente (o di qualsiasi utente) - utilizzando un endpoint, un'applicazione di monitoraggio basata su agenti;
3. Audit e protezione incentrati sui dati (DCAP – Data Centric Audit and Protection).

Le soluzioni UEBA analizzano il comportamento degli utenti, i loro gruppi di appartenenza e le entità coinvolte nella comunicazione tra utenti stessi, utilizzano tecniche analitiche avanzate al fine di rilevare transazioni e comportamenti anomali. La maggior parte di queste soluzioni è in grado di rilevare prontamente accessi anomali e/o comunicazioni anomale, ed applicare i modelli di apprendimento automatico (Machine Learning) grazie anche all'utilizzo di fonti di cyber threat intelligence esterna (Feed).

Invece strumenti di monitoraggio basati su agenti, offrono una visibilità più completa dell'attività dell'utente sulla sua postazione di lavoro rispetto a minacce Cyber o comportamenti dannosi verso l'organizzazione. La maggior parte di queste soluzione è in grado di effettuare una registrazione video di eventi di sicurezza degni di nota, come per esempio un accesso ad un aree riservata o l'avvio di un processo anomalo sulla postazione di lavoro (es. Malware, Trojan, etc).

Infine le soluzioni DCAP, si concentrano tradizionalmente sull'accesso privilegiato ai dati memorizzati nei file, come ad esempio sistemi di gestione di database relazionali (RDBMS), big data, database NoSQL o cloud pubblici. Le tecnologie DCAP sono in grado di rilevare potenziali attività dannose o accidentali prima che ci sia una violazione. Gli Alert e le azioni possono essere prioritizzate in base alla classificazione o alla sensibilità dei set di dati a cui si accede.

Per concludere, ad avviso di chi scrive, questo approccio ha però un limite rappresentato dalla privacy, che dipende principalmente dalla cultura aziendale e dalla presenza dell'azienda in particolari geografie (es. EU, USA, CINA, etc). Alcune cose si possono fare ma è importante stare attenti ai processi ed alla trasparenza e correttezza verso i dipendenti, che devono essere consapevoli sia dei comportamenti non ammessi ma anche delle modalità di controllo e delle tecnologie sottostanti.

Al momento , il consiglio più importante resta quello di adottare, il prima possibile politiche di microsegmentazione e programmi di formazione sui temi Cyber, anche attraverso simulazioni avanzate di attacco o di gestione della crisi, mentre per quanto riguarda gli aspetti tecnologici limitarsi alla verifica di comunicazioni anomale tra entità (UEBA) e controllo delle postazioni di lavoro attraverso soluzioni di EDP – End Point Protection, limitandosi al monitoraggio di accessi anomali ai dati "sensibili" aziendali (es. patrimonio informativo aziendale, dati di R&D, conti correnti dei clienti, etc) e non ai dati personali dei dipendenti.

Note

- [1] Il fattore umano nella cybersecurity: Phishing, Social Engineering e Mind Hacking - Gerardo Costabile e Ilenia Mercuri Luglio 2018
- [2] DBIR – Data Breach Investigation Report – Verizon 2018
- [3] Fonte wikipedia

- [4] Insider threat: The human element of cyber risk – McKinsey Settembre 2018

Articolo a cura di **Mattia Siciliano**