

Offensive Security (OffSec), 7Layers e la difesa attiva attraverso l'Adversary Emulation

Se è vero che l'attacco è la miglior difesa, è altrettanto vero che mettersi nei panni di un potenziale attaccante resta il modo migliore per prevenire e contrastare ogni sua mossa: è proprio questo il principio alla base dell'*Offensive Security* (anche nota come OffSec).

Cos'è l'offensive security?

Nata intorno agli anni '90 nella galassia dell'*Ethical Hacking*, l'OffSec rappresenta da sempre una risorsa imprescindibile a tutela di infrastrutture e sistemi informatici.

All'interno del mondo aziendale è stata per lungo tempo appannaggio esclusivo dei *Red Team* – impegnati soprattutto in attività di *Penetration Testing*, *Attack Simulation*, *Cyber Threat Intelligence* – lasciando ai cosiddetti *Blue Team* le azioni di *Defensive Security*, in cui rientra il monitoraggio delle reti insieme ai vari tipi di *Vulnerability/Risk Assessment*.

Tuttavia Nicola Santoro, Regional Sales Manager di 7Layers, ci tiene a sottolineare che “tali distinzioni appaiono da tempo superate in favore di un approccio integrato che vede le due “squadre” in costante interazione, a testimonianza dell'evoluzione verso una gestione condivisa delle minacce informatiche. Ciò è all'origine di quanto oggi noto come *Purple Team*, dove le informazioni raccolte mediante attività offensive sono utilizzate per potenziare (con esercitazioni o

simulazioni mirate) quelle difensive, così riducendo sia i tempi di risposta che i margini d'incertezza circa i possibili effetti di un attacco".

Dal Counter-Attack/Active Hacking Back alla gestione della Cyber Kill Chain: evoluzione delle strategie difensive

Mutuato dal gergo militare, il termine *counter-attack* indica ogni azione reattiva messa in campo per contrastare un'offensiva nemica.

Nell'ambito cyber, le attività tese a rallentare o contrastare gli incidenti informatici adottando la prospettiva degli attaccanti sono note come *Hacking Back*. Sebbene la legittimità di queste tattiche sotto il profilo etico-legale sia oggetto di dibattito ("*Examining cyber counter attacks from an ethical perspective*"), tale approccio risulta vincente ove si converta nell'anticipazione delle legittime azioni difensive a protezione di reti, applicazioni e infrastrutture aziendali.

L'utilità dell'OffSec risulta particolarmente evidente nei casi in cui le conseguenze di un attacco si concretizzano in modo pressoché istantaneo. Ad esempio attendere il verificarsi di un *data breach* per correre ai ripari spesso significa accettare la distruzione o diffusione di informazioni aziendali, con gli inevitabili danni economici e reputazionali che ne scaturiscono; ecco perché gli interventi *threat-focused* restano centrali per ottimizzare gli sforzi dei vari team di sicurezza verso la presa in carico dell'intera "catena di attacco".

Cos'è la Cyber Kill Chain?

La definizione della Cyber Kill Chain si deve alla società Lockheed-Martin, operante nell'industria della difesa statunitense, con la realizzazione del framework

sull'*Intrusion Kill Chains*.

Questo modello – che può essere impiegato anche per scopi offensivi – elenca le 7 fasi in cui sono soliti articolarsi gli attacchi informatici, ponendosi come strumento utile nelle strategie di cyber security e permettendo di irrobustire le azioni di difesa.

Le 7 fasi della *Cyber Kill Chain* sono:

1. *Reconnaissance*
2. *Weaponization*
3. *Delivery*
4. *Exploitation*
5. *Installation*
6. *Command and Control*
7. *Actions on Objectives*.



Fonte: COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION, A “Kill Chain” Analysis of the 2013 Target Data Breach

Nel tentativo di superare taluni limiti e migliorarne l'efficacia, il concetto di *Cyber Kill Chain* si è evoluto negli anni grazie all'apporto delle società di sicurezza informatica, che ne hanno realizzato diverse varianti utili a moderare i rischi e ostacolare le azioni degli attaccanti.

Adversary Emulation / MITRE ATT&CK

Partendo dalla consapevolezza di dover anticipare sempre più il fronte della cyber difesa, oggi esistono numerosi strumenti mirati a tale obiettivo.

Tra questi il noto MITRE ATT&CK®: quadro di riferimento globale e gratuito, massicciamente adottato sia da soggetti privati sia da realtà istituzionali o governative, per prevenire le più comuni tipologie di attacchi nei vari domini digitali attraverso l'impiego di “*adversary tactics and techniques*”.

Il framework MITRE include infatti tra le risorse anche processi di *Adversary Emulation and Simulation*, rispettivamente dedicati a imitare (*Emulation*) e riprodurre (*Simulation*) le potenziali attività condotte da uno specifico *threat actor*, al fine di osservarne gli effetti e potenziare l'assetto difensivo di un'organizzazione rispetto alle minacce note.

VA e PT, Vulnerability Assessment e Penetration Test (VAPT)

Come già osservato rispetto alla convergenza tra differenti team di sicurezza, il cambio di prospettiva in atto trova ulteriore conferma nella diffusione del VAPT, che integra le operazioni di *Vulnerability Assessment* con un tipico processo di OffSec quale il *Penetration Testing*.

Poiché tramite VA si espongono le vulnerabilità insite nei processi organizzativi, mentre mediante PT si valida il reale rischio di una vulnerabilità sfruttandola per superare il livello superficiale della stessa, è intuitivo come fondere i due tipi di test consenta di compiere un passo in più rispetto ai controlli di sicurezza tradizionali, garantendo un importante vantaggio strategico rispetto ad avversari esterni ma anche ad eventuali *Insider Threats*.

L'ormai consolidato impiego di strumenti "ibridi" a cavallo tra sicurezza offensiva e difensiva certifica un definitivo cambio di visione nella cybersecurity: non più parcellizzata o suddivisa in base all'obiettivo da difendere ma al contrario concepita – *by design* – per essere trasversale, olistica, proattiva e quindi maggiormente efficace nella difesa degli asset aziendali.

A cura della Redazione

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/notizie/offensive-security>

-offsec-7layers-e-la-difesa-attiva-attraverso-ladversary-emulation/