Gruppo Daman

Deception: non solo inganno

Strategie moderne di cyber security per una difesa attiva e preventiva - È ormai chiaro che le strategie di attacco adottate dal cyber crime continueranno a evolversi e ad aumentare ogni anno. Questo trend rende sempre più vulnerabile il perimetro di difesa di qualsiasi organizzazione.

Tra le tante criticità che espongono le organizzazioni a un rischio sempre maggiore, non si può non tenere conto della difficoltà crescente di riuscire a controllare e a proteggere un perimetro che cresce continuamente. Ma paradossalmente tra le criticità vi è anche l'incremento delle soluzioni di sicurezza e la conseguente sovraesposizione dei team di sicurezza a eventi e allarmi da gestire.

Basare unicamente la difesa informatica su tecnologie specializzate nell'individuare la presenza di un problema e nella continua ricerca di attività malevoli in un oceano di attività lecite, rischia di diventare inefficace e di aggravare nel tempo anche l'impatto sulle performance dei sistemi, sul traffico di dati e sulle risorse coinvolte.

Soluzioni innovative in grado di contrastare il cyber crime - Adottare una difesa attiva e preventiva in grado di attirare, rilevare e difendere l'organizzazione da malware e intrusi, che possono muoversi lateralmente all'interno della rete, può quindi risultare una scelta fondamentale e strategica.

È per questa ragione che le soluzioni di Deception, o cyber-inganno, stanno rapidamente emergendo sul palcoscenico della sicurezza informatica come scelta funzionale per una difesa attiva.

La Deception attira il nemico e lo sradica dalle sue posizioni difensive posizionandolo in una modalità di attacco controllata dal difensore. In questo senso la Deception non è più solo uno strumento difensivo, ma si rivela una vera e propria strategia. Questa strategia ha tanto più successo se la piattaforma abilitante è agentless, e se è basata su una tecnologia virtualizzata per un rapido deploy che evita l'adozione di hardware, solitamente costoso. Le strategie di Deception sono senza dubbio di grande efficacia se applicate da sole, ma risultano ancora più determinanti se combinate con altre piattaforme di sicurezza. Eliminando i falsi positivi e migliorando la qualità degli allarmi, possono scatenare azioni quali l'invio dell'evento a un sistema SIEM o SOAR, fornire informazioni utili alla creazione di regole firewall e altro ancora.

Un metodo di rilevamento rivoluzionario estremamente accurato e di ampia copertura - La soluzione di Deception IllusionBLACK è il risultato di un'attenta selezione effettuata dagli specialisti di Gruppo Daman. La soluzione garantisce al 100% la certezza dell'attacco in corso, consentendone la tempestiva segnalazione e analisi. Eliminando l'inutile dispendio di tempo per l'analisi di falsi positivi, riduce i tempi necessari all'individuazione della minaccia già presente all'interno dell'organizzazione.

IllusionBLACK è di facile implementazione, grazie alla sua installazione rapida e a basso impatto operativo, non genera alcun ulteriore aggravio sulle prestazioni della rete o degli endpoint e non richiede l'utilizzo di licenze software aggiuntive per creare le esche utilizzate.

Gruppo Daman
Passione e innovazione