Capgemini Italia Red Teaming

Capgemini

Red Teaming

Il ruolo del Red Teaming nelle attività di *Security Assessment*

Migliorare la sicurezza fingendosi un attaccante

Il Red Teaming rappresenta un approccio innovativo per testare e migliorare la resilienza informatica delle organizzazioni. Simulando attacchi informatici mirati e realistici, i Red Team coinvolgono l'organizzazione a 360°, e permettono di individuare vulnerabilità in ambiti che i tradizionali processi di security assessment come Vulnerability Assessment e Penetration Test non valutano. I Red Teaming, infatti, riguardano non solo aspetti tecnologici delle organizzazioni, ma anche persone e processi, e permettono quindi di individuare vulnerabilità in ambito digitale, fisico e sociale, offrendo una panoramica completa dei rischi e suggerendo contromisure mirate e personalizzate. Questo approccio consente alle organizzazioni di ottenere una reale valutazione del rischio a cui sono esposte e di valutare e migliorare le capacità del "Blue Team", ovvero valutare le proprie misure di sicurezza e di risposta agli incidenti, migliorandone sensibilmente la preparazione.

La storia del Red Teaming: dalla strategia militare alla Cybersecurity

L'origine delle Red Teaming Operations risale al 19° secolo, quando esercitazioni simili venivano utilizzate nei contesti militari per preparare le truppe agli imprevisti dei conflitti. Questo metodo consentiva di simulare conflitti e testare strategie.

Durante la Guerra Fredda, il termine "Red Team" venne adottato dagli Stati Uniti per indicare unità militari addestrate a comportarsi come forze nemiche, simulando tecniche e tattiche sovietiche.

In tempi moderni, il Red Teaming si è adattato alle esigenze del mondo della sicurezza informatica, diventando uno strumento essenziale per rispondere alle minacce cyber sempre più complesse e sofisticate.

There are two types of companies: those that have been hacked, and those who don't know they have been hacked.

John T. Chambers
Ex CEO & Chairman @ CISCO

$4.45M

Costo globale medio di un data breach nel 2023

Fonte: IBM Cost of a Data Breach Report 2023

Gli elementi fondamentali del Red Teaming per la sicurezza aziendale

Un'efficace strategia di Red Teaming prevede l'uso di diversi strumenti e metodologie per mettere alla prova le difese aziendali.

Le principali attività che vengono effettuate sono le seguenti.

1. Threat Intelligence

Il primo passo per costruire una strategia di attacco efficace e realistica è la raccolta di informazioni accurate sui possibili attori malevoli che potrebbero attaccare l'organizzazione e sulle principali minacce a cui l'organizzazione è esposta. Capgemini utilizza una vasta gamma di fonti, anche attraverso attività di Open Source Intelligence (OSINT), ed analizzando il Deep e il Dark Web, per monitorare i movimenti e le tendenze dei cyber-criminali, studiare il loro comportamento ed emulare i loro attacchi.

2. Red Teaming

Durante questa attività, il Red Team simula attacchi reali, adottando le tattiche, le tecniche e le procedure (TTP) che un reale attaccante potrebbe impiegare. L'obiettivo è esplorare percorsi di attacco all'interno dell'organizzazione ed identificare vulnerabilità in applicazioni, sistemi, processi aziendali e nei comportamenti del personale. In questo modo si analizza e si comprende a fondo cosa potrebbe accadere nel caso in cui l'organizzazione subisse un attacco da parte di un *threat actor* avanzato. Di conseguenza, al termine dell'attività si attua un processo di *lesson learned* per valutare le vulnerabilità presenti ed eventuali errori commessi, e migliorare sensibilmente il livello di sicurezza rispetto a questo tipo di minacce.

3. Purple Teaming

Questo approccio combina le forze di attacco del Red Team e le capacità difensive del Blue Team. Durante le esercitazioni di Purple Teaming, il Red Teaming lavora a stretto contatto con il team difensivo dell'azienda (ad esempio, con il team del SOC), il quale verifica in tempo reale se le tecniche utilizzate dagli attaccanti vengono rilevate e gestite correttamente. Questo approccio permette di comprendere ancora più da vicino le mosse di un possibile attaccante, e di conseguenza permette al Blue Team di imparare rapidamente come difendersi al meglio.

Pensare come l’avversario

Le fasi di un’esercitazione di Red Teaming: come funziona nella pratica

Un esercizio di Red Teaming si sviluppa attraverso fasi ben definite, attraverso le quali l’attacco viene organizzato, preparato, eseguito e concluso.

1. Preparazione

In questa fase preliminare, i responsabili aziendali definiscono insieme al Red Team gli obiettivi, la finestra temporale ed il perimetro dell’esercizio. Viene stabilito il livello di coinvolgimento dei team interni, come il Security Operations Center (SOC), per decidere se i responsabili della sicurezza verranno informati della simulazione. Vengono concordate le tecniche permesse agli attaccanti (ad esempio, si decide se consentire attività di *phishing* e *social engineering* mirate ai dipendenti). Vengono anche definiti eventuali asset da escludere dall’esercitazione. Infine, vengono identificati i *crown jewels*, obiettivi ultimi che gli operatori dovranno raggiungere. Ad esempio, essi possono essere rappresentati da una serie di documenti confidenziali, l’accesso ad un server critico o l’ottenimento di determinati privilegi di dominio.

2. Ricognizione

Il Red Team raccoglie informazioni dettagliate sull’organizzazione target, eseguendo una fase di ricognizione per comprendere al meglio la struttura dell’azienda e per raccogliere quante più informazioni possibili utili all’esecuzione dell’esercizio. Questa fase di intelligence include la ricerca di informazioni pubbliche (OSINT), l’esecuzione di scansioni di rete verso i sistemi dell’azienda e la valutazione dei comportamenti dei dipendenti sui social media per individuare potenziali punti di attacco.

3. Sviluppo e test degli scenari di attacco

Gli esperti del Red Team sviluppano scenari di attacco realistici basati sulle informazioni raccolte e su quanto concordato in fase di preparazione. Gli scenari sono progettati per testare le difese aziendali da diverse prospettive, inclusi lo sfruttamento di vulnerabilità nei sistemi informatici, la compromissione di sistemi di accesso fisico e persino attacchi di social engineering che mirano a sfruttare errori umani.

4. Simulazione dell’attacco

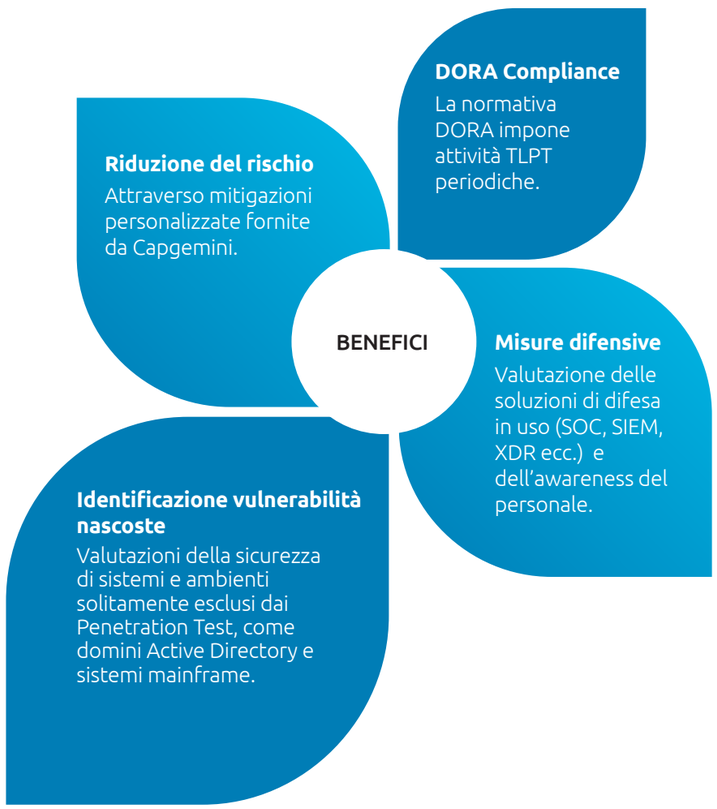
In questa fase il Red Team esegue l’attacco simulato. Gli specialisti possono adottare diverse tattiche, come il tentativo di accedere ai locali aziendali per testare la sicurezza fisica, l’uso di phishing per indurre i dipendenti a rivelare informazioni sensibili, o il tentativo di sfruttare vulnerabilità nei sistemi per muoversi lateralmente e raggiungere altri sistemi. Durante queste attività, gli specialisti di Capgemini pongono la massima attenzione ad essere il meno rumorosi possibile per non essere rilevati, proprio come un reale attaccante farebbe.

5. Valutazione dei risultati e report finale

Al termine della simulazione, il Red Team prepara un rapporto dettagliato che documenta il percorso dell’attacco e descrive le vulnerabilità rilevate. Il rapporto include raccomandazioni su misure correttive e miglioramenti per i sistemi e per le strategie di difesa. Le osservazioni riguardano aspetti tecnologici, processi e persone, con l’obiettivo di rafforzare la resilienza complessiva dell’organizzazione. Viene inoltre calcolato l’impatto potenziale di un attacco riuscito sugli asset critici aziendali.

Benefici di un Red Teaming

Il valore di un approccio proattivo alla sicurezza



Threat Led Penetration Test (TLPT)

Un’ulteriore declinazione del Red Teaming è data dai Threat-Led Penetration Test (TLPT), ed in particolare da quelli regolamentati dal framework TIBER-EU. Sebbene la definizione “Penetration Test” possa essere fuorviante, si tratta a tutti gli effetti della declinazione più completa ed efficace del Red Teaming. Infatti, il TLPT ha come obiettivo principale quello della simulazione di un attacco da parte di un avversario reale, e richiede un’importante fase di threat intelligence preliminare proprio per poter provvedere a questa disposizione.

Queste esercitazioni, offerte da Capgemini ed adottate da molte autorità finanziarie internazionali, permettono alle aziende di confrontarsi con attacchi mirati e avanzati. Utilizzando la combinazione di threat intelligence e red teaming, i TLPT forniscono una valutazione completa di misure e capacità di difesa dell’organizzazione.

L’approccio di Capgemini

Grazie alle numerose esperienze guadagnate nel corso degli anni, e grazie a professionisti esperti ed in possesso delle migliori certificazioni del settore, Capgemini ha sviluppato un approccio strutturato e completo grazie al quale è possibile offrire soluzioni personalizzate di Red Teaming e TLPT per ogni contesto aziendale. Un team multidisciplinare, comprendente analisti di intelligence ed esperti penetration tester, è pronto a supportare le organizzazioni nel loro percorso di miglioramento della sicurezza. Al termine delle attività di assessment, attraverso sessioni formative, gli esperti di Capgemini guideranno le aziende nella comprensione delle proprie debolezze e nell’applicazione delle migliori mitigazioni possibili.

About Capgemini

Capgemini is a global business and technology transformation partner, helping organizations to accelerate their dual transition to a digital and sustainable world, while creating tangible impact for enterprises and society. It is a responsible and diverse group of 340,000 team members in more than 50 countries. With its strong over 55-year heritage, Capgemini is trusted by its clients to unlock the value of technology to address the entire breadth of their business needs. It delivers end-to-end services and solutions leveraging strengths from strategy and design to engineering, all fueled by its market leading capabilities in AI, cloud and data, combined with its deep industry expertise and partner ecosystem. The Group reported 2023 global revenues of €22.5 billion.

www.capgemini.com

Capgemini

Get the future you want