Comprendere gli attacchi informatici

La Cyber Kill Chain è uno strumento eccellente per capire in che modo le organizzazioni possono aumentare notevolmente la possibilità di difendere il loro ambiente

"Cyber Kill Chain" è l'espressione usata per indicare il modello del ciclo di vita di un attacco informatico. Il nome è l'adattamento al campo della cyber security del concetto di Kill Chain utilizzato in ambito militare per indicare un modello a fasi utile a identificare i vari passaggi necessari all'esecuzione di un attacco.

In ambito informatico, è uno strumento eccellente per capire in che modo le organizzazioni possono aumentare notevolmente la possibilità di difendere il loro ambiente rilevando e bloccando le minacce in ogni fase del ciclo di vita dell'attacco: ci insegna quindi che, mentre gli avversari devono completare tutte le fasi affinché l'attacco vada a buon fine, noi (i difensori) dobbiamo "solo" fermare e spezzare la catena in qualsiasi fase del processo. Ma come fare?

Le fasi della Cyber Kill Chain

La Cyber Kill Chain afferma che, per compiere i loro misfatti, gli attaccanti devono sempre seguire sei passaggi fondamentali. Vi è una Cyber Kill Chain esterna ed una interna: la prima porta alla violazione del perimetro di rete aziendale, la seconda è costituita dalle azioni per ottenere l'accesso all'endpoint preso di mira. La combinazione della Cyber Kill Chain esterna e interna nel settore è definita **Cyber Kill Chain estesa**.

Uno degli obiettivi è quello di disporre di meccanismi di difesa efficienti della Cyber Kill Chain estesa per **rallentare**

gli attaccanti, far sì che la prosecuzione dell'attacco diventi sempre più costosa e rendere il più difficile possibile il passaggio a ciascuna fase successiva. Se gli attaccanti non riescono a raggiungere il loro obiettivo in modo conveniente, dirigeranno i loro sforzi altrove.

La strategia di sicurezza di un'organizzazione deve quindi tenere conto di come viene eseguito un attacco, all'esterno e soprattutto dall'interno, poiché gli attaccanti, una volta entrati nella rete, hanno accesso agli endpoint e alle loro risorse.

L'approccio tradizionale alla sicurezza dovrebbe essere esteso con metodi basati sulla comprensione della Cyber Kill Chain, fornendo tecnologie che siano in grado di impedire agli attaccanti di accedere agli endpoint e anche di bloccarli in ogni possibile fase della Cyber Kill Chain interna.

Nella guida realizzata da WatchGuard, dal titolo "**Comprendere gli attacchi informatici**", si spiega come la soluzione di endpoint security Adaptive Defense 360 (AD360) garantisce che l'esecuzione della Cyber Kill Chain venga sempre interrotta, lasciando a mani vuote gli autori degli attacchi.

AD360 aiuta i team di sicurezza a progettare una strategia di sicurezza allineata alla Cyber Kill Chain estesa senza necessità di aumentare il personale grazie al rilevamento e alla risposta intelligente degli endpoint (EDR). Nella guida viene illustrato come AD360 interviene in ognuna delle sei fasi della kill chain in un attacco ransomware e in che modo può prevenire e bloccare gli attacchi in corso prima che causino danni.

Per saperne di più, la guida "Comprendere gli attacchi informatici" è disponibile a questo link:

https://www.watchguard.com/it/wgrd-resource-center/ebook/under

standing-cyber-attacks

https://www.ictsecuritymagazine.com/notizie/comprendere-gli-attacchi-informatici/