HYPERsafe

In periodi come quelli attuali in cui gli attacchi e le minacce informatiche diventano sempre più insidiose, ci sono dei servizi essenziali che le aziende, gli enti e le pubbliche amministrazioni devono tenere in seria considerazione per proteggersi da attacchi e intrusioni che possono risultare devastanti.

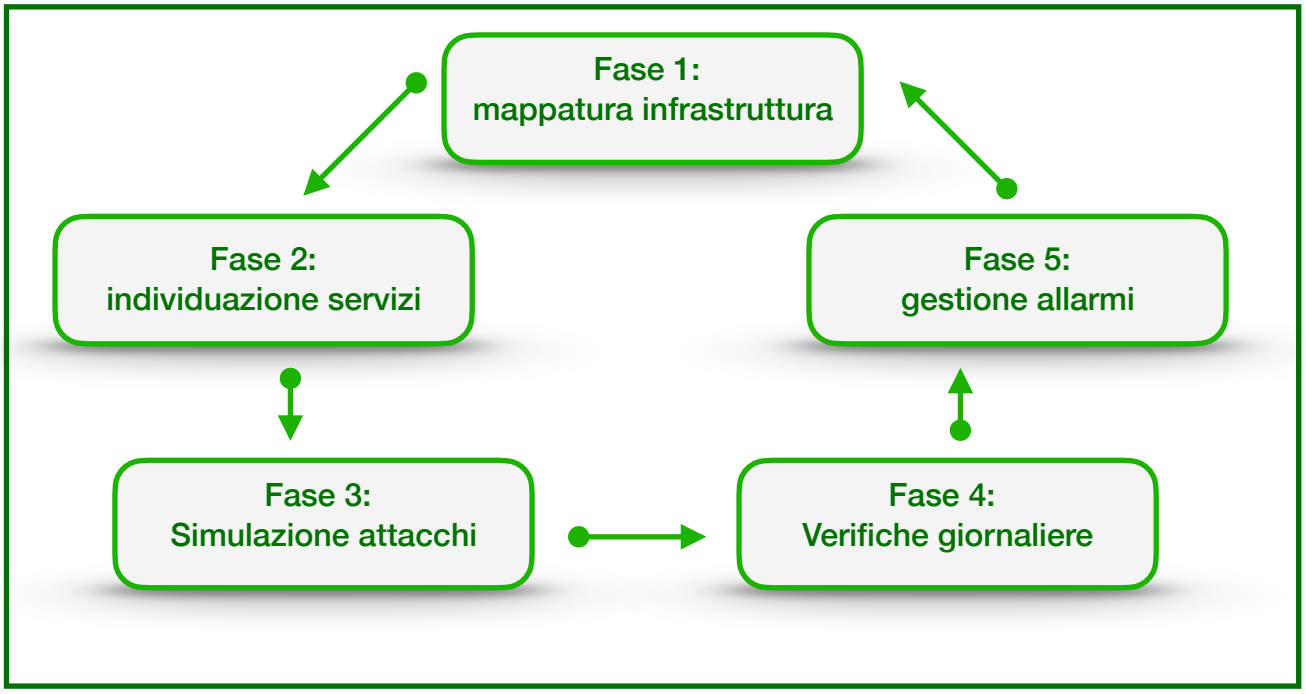
HyperGrid propone **HyperSAFE**, un Managed Security Service (MSS) che sfrutta le tecnologie più aggiornate per la protezione della rete. I cosi detti “Servizi di Sicurezza Gestiti” vengono comunemente dati in affidamento a provider esterni specializzati in questo settore, situazione che genera un grande vantaggio per gli uffici IT facendo in modo che gli amministratori di sistema possano gestire i loro compiti primari senza doversi occupare della sicurezza delle informazioni eliminando le limitazioni delle risorse sia a livello hardware che di personale. Sarà infatti il provider a occuparsi della sicurezza di rete bloccando malware e virus, furto dei dati ed eseguendo esaustive verifiche sull’infrastruttura.

HyperSAFE è un sistema progettato per rendere impenetrabili le reti e i sistemi informatici. Il team di esperti dell’azienda è in grado di gestire l’infrastruttura con soluzioni che monitorano le risorse di rete in modo da bloccare i tentativi di manomissione e le intrusioni. Tutti gli strumenti e le tecnologie usati nel servizio sono costantemente aggiornati sia lato software, sia hardware: per esempio, per la gestione dei firewall e l’analisi delle vulnerabilità vengono impiegati i database **Cisco Talos** che sono una vera garanzia di sicurezza. Questi database vengono creati utilizzando set di telemetria basati su miliardi di dati e comprendono milioni di campioni di malware e analisi delle intrusioni in modo da garantire la massima efficacia. Le funzioni di un servizio di sicurezza come **HyperSAFE** possono includere svariati compiti che comprendono il monitoraggio e la gestione H24 dei sistemi di rilevamento delle intrusioni e dei firewall, la supervisione e la gestione delle patch software (ed eventuali update hardware sui dispositivi obsoleti), l'esecuzione di valutazioni di sicurezza e la risposta immediata agli allarmi e alle emergenze. **HyperGrid** ha strutturato il servizio **HyperSAFE** dopo un attento studio relativo ai metodi utilizzati dai cybercriminali e l’analisi supportata dal team di esperti consente di adattare con la massima reattività le contromisure impiegate per la difesa in modo da fornire ai clienti la migliore sicurezza possibile anche anticipando i tentativi di manomissione. Alcune delle verifiche possono essere eseguite in remoto o in modalità automatica, ma ovviamente è di fondamentale importanza l’esecuzione dei controlli sul campo in modo da valutare l’effettiva conformità delle misure di protezione utilizzate.

LA PROCEDURA IN FASI

Il team di **HyperGrid** analizza ogni tentativo di intrusione nella rete approntando adeguate soluzioni e intervenendo per correggere le configurazioni del sistema. Inoltre, **HyperSAFE** è un servizio elastico, in grado di adattarsi alle necessità di ogni cliente e, proprio per questo motivo, è strutturato in modo da poter scegliere attraverso quali modalità conviene avviare i controlli primari, oltre a gestire la scelta sui tempi e le modalità di monitoraggio. Ogni fase della procedura viene eseguita nel pieno rispetto della normativa Europea (GDPR) e seguire consiste in 5 fasi:

• **Mappa infrastruttura**	• **Verifiche giornaliere**
• **Individuazione dei servizi**	• **Verifiche gestione degli allarmi**
• **Simulazione attacchi**	



Analisi delle fasi che i clienti possono richiede di eseguire nella procedura:

Prima fase - **Mappatura della rete**
Si tratta di una procedura fondamentale che esegue una dettagliata mappa dell'infrastruttura di rete e della sua organizzazione. Il team di **HyperGrid** è in grado di segnalare ed evidenziare gli eventuali punti deboli e indicare la soluzione per porvi rimedio.

Seconda fase - **Individuazione servizi e protocolli**
Viene eseguita l'analisi approfondita dei i protocolli e delle porte attive dell'intera infrastruttura procedendo poi con la loro verifica per individuare e mappare le vulnerabilità. In questo modo è subito possibile evidenziare gli eventuali punti deboli che potrebbero essere usati per attacchi e infiltrazioni.

Terza fase - **Simulazione attacchi**
Non tutti i clienti potrebbero aver bisogno di questa fase che però, rammentiamo, è una delle più importanti e consigliate, in particolare se si tratta di strutture complesse che garantiscono accesso a numerosi utenti. Sull'infrastruttura sono eseguiti dei test di verifica sul tipo di connessione Internet e sui tempi di risposta dei sistemi. Vengono inoltre eseguiti esaustivi test (prove manuali e automatizzate), per analizzare i sistemi di protezione. Al termine dell'analisi i tecnici dell'azienda forniscono un report con l'indicazione dettagliata dei punti critici individuati.

Quarta fase - **Verifiche e sensori**
Gestione delle verifiche giornaliere e installazione dei sensori IDS (Intrusion Detection System) in modo da fare cadere in trappola eventuali cybercriminali che tentano di penetrare le difese. Fra i controlli consigliati ci sono i test di intrusione, test di interruzione di fornitura servizi, test per l'analisi della sicurezza dei siti web, monitoraggio del traffico e attivazione di regole di allarme in funzione della configurazione della rete.

Quinta fase - **gestione degli allarmi**
Individuate eventuali debolezze nella gestione della sicurezza della rete il team di **HyperGrid** suggerisce le configurazioni da adottare e la gestione e il posizionamento degli allarmi.

www.hypergrid.it - info@hypergrid.it - Tel. 0382 528875