HyperCut

La soluzione per il controllo del corretto utilizzo delle risorse di rete

La sicurezza informatica delle reti è gestita mediante un insieme coordinato di servizi e tecnologie. Fra gli elementi più importanti ci sono le soluzioni per il controllo delle risorse dell'infrastruttura come il servizio **HyperCut** che usa Firewall di nuova generazione (sempre aggiornati), software IDPS (intrusion detection and prevention systems) progettati per rilevare e prevenire le eventuali intrusioni e tecnologie SIEM che provvedono al monitoraggio e alla gestione del sistema in tempo reale e alla raccolta dei dati d'uso.

DOPPIA FUNZIONE

HyperCut usa un database centralizzato di tutte le policy di sicurezza attive e permette al SOC (Security Operations Center) **HyperGrid** di gestire e monitorare l'infrastruttura aziendale tramite un'unica interfaccia. Inoltre, grazie al cosi detto Endpoint Security è possibile definire quali software e applicazioni gli utenti possono usare. Il sistema è in grado di verificare da che computer avviene l'accesso, se ci sono software non consentiti o se il sistema è infetto da malware. Se questa situazione si dovesse verificare **HyperCut** bloccherà l'accesso in modo da risolvere la situazione, soluzione utile anche per il personale che accede in smartworking. **HyperCut** è completamente configurabile in base alle esigenze dell'azienda e consente di creare zone con livelli di sicurezza intermedie per la pubblicazione di servizi o per altre esigenze del cliente. Inoltre, è progettato per integrarsi perfettamente con altri servizi proposti da **HyperGrid** come per esempio HyperVPN Plus per l'accesso sicuro all'infrastruttura da una rete di dati criptata con la sicurezza dell'autenticazione a due fattori.

PREVENZIONE DEGLI ATTACCHI INTERNI

Dato l'alto numero di cyber-attacchi provenienti dall'esterno l'attuale tendenza è quella di concentrarsi prevalentemente sui sistemi di sicurezza per contrastarli, ma c'è una situazione più subdola da tenere in considerazione: ovvero le minacce interne, comunemente indicate con il nome di "insider threats". Possono essere situazioni attivate inconsapevolmente, per esempio quando un malware viene scaricato per avere cliccato su un link di un'email di phishing. Ma ci sono minacce più gravi e difficili da individuare che comprendono tipologie di attacco portate a termine per interessi finanziari: furto e vendita dei dati aziendali, frodi con la modifica dei dati finanziari, fino ad arrivare al furto di progetti e segreti commerciali. Si tratta di casi estremi che però risultano più frequenti di quanto si possa immaginare.
Un servizio come **HyperCut** rappresenta una valida soluzione dato che, oltre a monitorare l'infrastruttura, fornisce la possibilità di impostare e modulare l'accesso alle risorse di rete del personale. Grazie a questa soluzione è possibile definire l'accesso solo alle aree di competenza, impostare delle "access list" per ogni singolo utente, consentire la navigazione online o bloccarla e anche attivarla solo in particolari ore del giorno e da determinate postazioni. Inoltre, è possibile creare delle "black list" di connessione per alcuni utenti, in modo da privilegiare la sicurezza dei dati nelle aree che richiedono maggior attenzione.

Per richiedere ulteriori informazioni o un preventivo:

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