

In primo piano

Cyberoam e l'Identity Based Security

Soluzioni proattive per proteggere gli utenti da attacchi mirati, distribuite in Italia da Horus Informatica.



Le appliance UTM Cyberoam

Le violazioni ai dati di alto profilo fanno sempre notizia, mentre gli innumerevoli incidenti riferiti ad aziende meno conosciute rimangono nel silenzio, sebbene abbiano conseguenze altrettanto dannose. I *targeted attacks* non puntano alla rete in generale, sfruttano la parte più vulnerabile di un'infrastruttura di sicurezza, gli utenti, in particolare gli utenti privilegiati, ovvero coloro che hanno accesso a informazioni di un certo valore e a dati sensibili. Fino a qualche anno l'obiettivo degli attacchi era ampio e non focalizzato su 'chi è attaccato' ma sul 'numero delle vittime'. La metodologia di attacco coinvolgeva soprattutto worm di mailing di massa, Trojan inviati a diverse persone, scansioni di massa di varie vulnerabilità della rete/server e così via.

L'utente è il punto di svolta

Ma lo scenario è cambiato: gli attacchi sono studiati per colpire attività e sistemi specifici. È più difficile fermare un attacco mi-

rato, anche perché proviene da soggetti esperti e motivati dal lucro. In tutti gli attacchi mirati il filo conduttore è l'utente. È lui a determinare il successo dell'attacco, diretto o indiretto (ad esempio derivante da un comportamento poco consapevole che permette l'insediamento di codice maligno). Talora è lo stesso utente a comportarsi in modo doloso. Per questo conoscere cosa accade fuori dalla rete è importante quanto avere traccia di cosa accade al suo interno. Solo una soluzione capace di fornire trasparenza su 'chi fa cosa' nella rete, estendendo le funzionalità di sicurezza fino all'utente reale, e non semplicemente agli indirizzi IP delle macchine, può dirsi in grado di sconfinare gli attacchi mirati, ma anche garantire una piena conformità alle normative. La tecnologia identity-based di Cyberoam, distribuita in Italia da Horus Informatica, estende le funzionalità di security al Layer 8, lo *human layer*, del modello OSI. Quella del Layer 8 è una tecnologia unica, in fase di brevetto, che pone la soluzione UTM Cyberoam più vicina all'intelligenza umana. Nel caso di attacchi mirati, è proprio la granularità della soluzione ad avere il ruolo decisivo. Cyberoam raggiunge l'obiettivo legando l'identità degli utenti alla security in tutti i suoi aspetti a partire dall'autenticazione, gli strumenti di implementazione delle policy e il reporting. Una soluzione UTM Identity Based

come Cyberoam non è solo in grado di autenticare gli utenti, ma riesce ad applicare policy personalizzate per utente o gruppo di utenti.

Le ultime novità

Una caratteristica della soluzione è la semplicità: la nuova release Cyberoam UTM Versione X, oltre a beneficiare di un ulteriore potenziamento della soluzione UTM, diventa più efficiente nella gestione via interfaccia utente. Grazie alla nuova release le appliance Cyberoam UTM saranno più veloci nel garantire sicurezza identity-based, più semplici da gestire, avranno tempi di reboot più rapidi e immediato accesso a GUI. La Versione X comprende inoltre l'Extensible Security Architecture (ESA), l'application Layer 7 Management, la connettività 3G/WWAN, il traffico HTTPS/SSL sicuro, l'archiviazione e controllo Instant Messaging, l'interfaccia grafica utente (GUI) di nuova generazione, il supporto IPv6.

www.horus.it

A.C.R.

Horus su 



CODICE VIDEO GG604
www.soietv.it