

KaP, Knowledge and Prevention

Il progetto basato sulla console eTrust Security Command Center

La collaborazione

Nasce nel 2006 l'idea di sviluppare un prototipo di sistema centralizzato e proattivo di gestione della sicurezza It, in grado di prevenire e neutralizzare gli eventi critici legati ad incidenti e attacchi di varia natura, cui sono continuamente esposte le reti aziendali.

Il progetto si concretizza in un modello proprietario di gestione delle informazioni di sicurezza, denominato Knowledge and Prevention (KaP).

KaP ha come cuore nevralgico la console CA eTrust Security Command Center (Sec) e la sua integrazione con il Pna (Parallel Network Auditor), sonda proprietaria di Con.Nexo', società italiana di consulenza e di servizi Ict.

Sfruttando le capacità di raccolta e correlazione di grandi quantità e formati di log offerte da Sec, KaP aggiunge nuovi

modelli di interpretazione dei dati, offrendo discriminanti di alerting, non più solamente it-centriche, ma business-oriented.

La granularità dei moduli di analisi previsti consente, inoltre, una completa visione di ciò che coinvolge le risorse It, aiutando così a migliorare le performance di monitoring, imposte dagli standard internazionali e dalla normativa vigente.

KaP e Cnr

Il progetto KaP, svolto e realizzato nell'infrastruttura del Cnr, Area di Ricerca Roma 2 di Tor Vergata, nasce dalla necessità di individuare una soluzione in grado di gestire e analizzare un elevato numero di eventi e dati generati da un'infrastruttura tecnologica open, caratterizzata da una rete di IP pubblici, con grande capacità trasmissiva (100mb), un'ele-

vata eterogeneità di sistemi operativi ed elementi tecnologici, ed un accesso quasi illimitato a livello utente.

Perché KaP

A parlare del sistema KaP di gestione degli eventi inerenti la sicurezza It è uno dei suoi primi clienti e sostenitori, Gaetano Chionchio, Responsabile del Servizio Reti di Telecomunicazioni del Cnr, che ha fortemente voluto e sostenuto la nascita e lo sviluppo del prototipo, fornendo tutte le indicazioni che solo chi ha a che fare in prima persona con il quotidiano problema della gestione della sicurezza di una infrastruttura di rete complessa, come è quella del Cnr, poteva fornire.

"In un contesto It per definizione 'aperto' come è quello di un centro di ricerca, l'esigenza di avere il controllo delle minacce interne ed esterne in tempo reale è fon-

damentale; inoltre, il nostro compito istituzionale di promuovere la ricerca in ambito It è stato il terreno fertile per la nascita del laboratorio denominato 'Open-Lab', in cui aziende italiane, come Con.Nexo', trovano spazio per lo sviluppo di idee e soluzioni innovative...!"

Il KaP nasce proprio dall'esigenza sempre più diffusa di raggiungere un livello sostenibile di sicurezza, gestendo le diverse tecnologie e tipologie di informazioni, spesso disomogenee, in un sistema globale in cui le minacce (e le tecniche di difesa) sono in continua evoluzione.

La soluzione, tramite la console Sec di CA, offre, infatti, un duplice livello di protezione: la centralizzazione delle informazioni (ottimizzando e migliorando il lavoro degli It manager) e la prevenzione dalle minacce, altrimenti non identificabili in normali tempi di analisi.