Simona Venuti – GARR-CERT

HoneyPot - Cattura e analisi tentativi di intrusione - Netflow-tool

In questa presentazione verranno illustrati i limiti nella gestione della sicurezza dovuto alla presenza di nuove minacce e nuove metodologie di attacchi. Per ottenere un adeguato livello di sicurezza e' necessario un nuovo approccio basato sulla "gestione dell'insicurezza", ossia sistemi di monitoraggio, di early alerting, e di tecniche proattive. Verranno illustrate le tecniche in uso al GARR-CERT per monitoraggio globale a protezione di tutta la rete GARR a livello nazionale, basato sull'analisi di flussi tramite il protocollo NetFlow e il relativo tool di elaborazione.

Verranno presentate tecniche di monitoraggio locale, basate sull'installazione e deployment di HoneyPot per l'analisi della distribuzione di malware e tentativi di intrusione, che possono essere usati dagli APM per monitorare le proprie sedi. Infine verra' presentata una brevissima panoramica sui progetti di ricerca e deployment: early alarm system basati su HoneyPot e studio analisi di metodologie di rilevamento di botnet.