Cento occhi per proteggere le infrastrutture critiche europee

Luca Severini, CEO e fondatore di Epistematica

Dopo lo shock dell'11 Settembre, con la comunicazione al Consiglio e al Parlamento europeo del 20 ottobre 2004[1], anche la Commissione europea varava una serie di iniziative per la lotta contro il terrorismo, finalizzate alla protezione delle infrastrutture critiche.

Consapevole della natura infrastrutturale delle ICT, tra le varie iniziative la Commissione europea varava anche una serie di misure per stimolare la crescita delle competenze nel settore della Cyber Security. Tra queste azioni, hanno rivestito un ruolo molto importante i finanziamenti alla ricerca nell'ambito del 7° Programma Quadro.
A dimostrazione dell'interesse dell'Europa sul tema "sicurezza", nel periodo 2007-2013 sono stati finanziati 528 progetti[2], per un valore di circa 1,4 miliardi di euro. L'ultimo progetto finanziato nell'ambito della call ICT-2013.1.5 - Trustworthy ICT è stato il progetto PANOPTESEC - Dynamic Risk Approaches for Automated Cyber Defence[3]. Un ambizioso progetto che si concluderà entro il 2016.

Il progetto Panoptesec si prefigge lo scopo di realizzare un prototipo "oltre lo stato dell'arte" di un sistema informatico a supporto delle decisioni per la difesa delle infrastrutture ICT definite "critiche". L'obiettivo generale del progetto è quello di fornire capacità di monitoraggio superiori a quelle dei sistemi attualmente disponibili sul mercato.
Ecco perché il nome del progetto contiene il termine "panoptes", un parola che in greco antico significa "che tutto vede". In mitologia era l'epiteto dato al gigante Argo, dotato di cento occhi, ucciso da Ermes per liberare la ninfa Io. Fu Era a prendere gli occhi dalla testa del gigante morto per ornare le piume del pavone, l'animale a lei sacro. Da qui il logo del progetto.

Il sistema Panoptesec è composto da tre sottosistemi: proattivo; reattivo; e di visualizzazione. Quest'ultimo fornisce una console che permette di valutare le debolezze, individuare i potenziali percorsi di attacco, fornire un elenco di azioni di reazione in ordine di priorità, e fornire un mezzo per eseguire queste azioni; il tutto supportato da motori di analisi automatizzata, anche per la misurazione dell'impatto sul business.

---

[1] COMUNICAZIONE DELLA COMMISSIONE AL CONSIGLIO E AL PARLAMENTO EUROPEO - La protezione delle infrastrutture critiche nella lotta contro il terrorismo - http://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52004DC0702&from=IT
[2] Elenco progetti FP7-Security - http://cordis.europa.eu/search/result_it?q=contenttype=%27project%27%20AND%20programme/pga=%27FP7-SECURITY%27&srt=startDate:decreasing
[3] PANOPTESEC - Project reference: 610416 - http://cordis.europa.eu/project/rcn/111202_en.html