

■ *Workshop di Selex Sistemi Integrati a Bacoli*

## La "cyber protection" la nuova frontiera dell'Homeland Security

**S**i è parlato soprattutto di "cyber protection", vale a dire della protezione di infrastrutture informatiche, e del delicato problema della privacy nel workshop internazionale organizzato da Selex Sistemi Integrati, che si è tenuto a Bacoli (Napoli), dal 21 al 25 settembre, dal titolo "The Homeland Security facets: attacks, counter-measures and the private issue". Quattordici ore di lezioni accademiche, più altri interventi più brevi – come ha sottolineato **Marina Grossi**, amministratore delegato della società Finmeccanica – con la partecipazione di illustri docenti e professori universitari, come il preside della Facoltà di ingegneria di Berkeley, in California, **Shankar Sastry**, e il professor **Giorgio Franceschetti**, dell'Università "Federico II" di Napoli, ma anche di rappresentanti delle

BACOLI (NA)

Affrontati due argomenti principali: la protezione di infrastrutture informatiche e il dilemma tra avere le informazioni e nello stesso tempo salvaguardare la privacy

DALL'INVIATO **LUCIA ANGELONI**

istituzioni, come l'onorevole **Filippo Ascierio**, componente della commissione Difesa della Camera, e delle forze armate. Si tratta del secondo workshop organizzato da Selex Sistemi Integrati sull'Homeland security, e nelle intenzioni di Marina Grossi deve diventare un appuntamento annuale, in modo da poter confrontare i risultati del mondo universitario con quello delle azien-

de e creare le basi per lo scambio conoscitivo tra industria e utenti sulle metodologie nell'ingegneria dei grandi sistemi.

Il workshop ha trattato sia il problema della sicurezza delle strutture reali, come ad esempio le reti di distribuzione di energia, che virtuali appunto, perchè il pericolo terroristico adesso può arrivare anche da internet o per quelle infrastrutture guidate, gestite e sviluppate da sistemi informatici. Per questo il prof. Sastry ha sottolineato che occorre ripensare completamente la scienza del computer, per creare un sistema sicuro, in grado di distruggere l'attacco e di individuare sempre da dove arriva, e in grado di operare anche attraverso eventuali intrusioni, creando cioè un sistema "trustworthy", ovvero un sistema che faccia quello che gli viene richiesto nonostante gli attacchi dell'ambiente esterno,

l'utilizzatore e gli errori operativi.

E sul tema della sicurezza informatica anche Selex Sistemi Integrati sembra già ben preparata. «Ascoltando le varie presentazioni abbiamo visto che non c'è una novità enorme che a noi manchi di sapere», ha sottolineato l'ing. **A. Farina**, di Selex Sistemi Integrati. «La tecnologia ci è nota e la stiamo già implementando nei nostri sistemi, ad esempio nel programma Forza NEC, che riguarda la modernizzazione delle Forze Armate italiane, per il quale la società è prime contractor».

Forza NEC, acronimo di Network Enabled Capabilities, è un progetto congiunto Difesa-industria, nato per soddisfare le esigenze del soldato futuro, che nell'era del digitale potrà beneficiare dei vantaggi della rete. I tempi di comunicazione e di acquisizione delle informazioni, che da sempre rappresentano una criticità nella condotta delle operazioni militari, saranno infatti abbattuti grazie alla introduzione di nuove tecnologie informatiche. La filosofia del proget-

to Forza NEC si riassume in sintesi nella possibilità di collegare, in maniera diretta e immediata, ogni singolo soldato con il centro decisionale. Il militare sul terreno potrà così accedere a banche dati come se fosse davanti al proprio Pc, potrà comunicare inviando messaggi facilmente componibili, sarà in grado di vedere di notte come di giorno e di inviare immagini a tutte le unità collegate in rete. Chiaro quindi che un sistema di comunicazione sicura si fa sempre più necessario.

E la società Finmeccanica, incaricata della gestione dei grandi sistemi, ha portato ad esempio il sistema di gestione del G8 dell'Aquila, che ha previsto una progettazione di grandi sistemi che si svolge contemporaneamente sul piano delle opere civili, su quello dei sistemi informativi ed elettronici, ed anche sullo quello della pianificazione operazioni. Per la gestione del G8 era stato ad esempio previsto un Security Operation Center (SOC), cioè un centro di controllo tramite cui era possibile: controllare lo

stato di sicurezza della rete in tempo reale; gestire un Incident Event ed il relativo Incident Response Team (IRT) e controllare la rete di connessione che garantisce la disponibilità delle reti geografiche e locali e la sicurezza degli accessi wireless prevista. In relazione agli obiettivi di progetto, il SOC è stato strutturato ed organizzato per erogare i seguenti servizi di sicurezza: Real Time Device Monitoring: che prevede il monitoring remoto dispositivi di sicurezza (Firewall, IDS, Antivirus, Antispam, Proxy), per il rilevamento di azioni anomale; Policy Management & Enforcement: che prevede la gestione remota di apparati di sicurezza (Firewall, IDS, Antivirus, Antispam, Proxy) e gestione di apparati di rete; Incident Identification, Classification, Notification & Response: che prevede la realizzazione di un IRT capace di svolgere attività di identificazione, classificazione e response ad un determinato attacco informatico; Vulnerability Assessment: Attività di vulnerability assessment e Penetration Test. ●