Intelligence, il top manager dell’Eni all’Unical: “Fondamentale la sicurezza energetica”

Alfio Rapisarda, **responsabile sicurezza del Gruppo Eni**, ha tenuto una lezione al **Master in Intelligence dell’Università della Calabria** diretto da **Mario Caligiuri**. Il dirigente ha esordito raccontando della singolare storia dell’Eni, che da volàno dell’economia nazionale si è trasformata in azienda internazionale in grado di modificare gli equilibri mondiali dell’energia.

La dimensione dell’**Eni** è straordinaria: operazioni in 73 paesi del mondo, più di 33.000 persone che vivono e si muovono nelle più disparate aree operative in terra e in mare. Mutuando dal suo fondatore Enrico Mattei una visione a lungo termine, Eni è una società che pensa già a ciò che ci sarà nel futuro, oltre al petrolio e al gas. In questo senso molto interessante è l’accordo siglato di recente con il Mit di Boston sulla fusione nucleare.

«Bisogna tener presente – ha ribadito Rapisarda – che le variabili geopolitiche sono una componente di rischio da valutare attentamente nell’ambito di una **strategia energetica sia nazionale che internazionale**».

Approfondendo questo aspetto, il top manager ha osservato

come l’economia energetica costituisca una leva importante per la crescita economica e sociale specie per quei Paesi in via di sviluppo e che si trovano ad affrontare complessi scenari geopolitici, dove si registrano tensioni legate a conflitti regionali e minacce terroristiche e criminali. **L’attenzione alla sicurezza è nel DNA di Eni**, che da sempre adotta rigide politiche di security improntate a logiche di prevenzione per misurare, stimare e governare rischi di varia natura: il terrorismo, la pirateria, i sabotaggi, la criminalità, lo spionaggio industriale ed il cyber crime, una nuova forma di minaccia che, per sua natura, è senza confini e quindi ancor più pervasiva e pericolosa. In Italia non c’è ancora una legge che disciplina la security e le regole che ciascuna azienda adotta vengono mutuate dalla safety, in particolare dalla legge sulla sicurezza nei luoghi di lavoro e dai vincoli relativi alla responsabilità amministrativa delle aziende.

«La security Eni – ha spiegato Rapisarda – **monitora ed analizza centinaia di paesi**: l’Africa, sia nella parte settentrionale che ad ovest, dove Eni è la prima compagnia petrolifera, il Sudamerica dove è presente da molti anni, l’Europa, il Medio Oriente e l’Asia centrale.

> *Per ogni Paese Eni ha elaborato una mappa dei rischi e delle minacce, analizzando puntualmente una molteplicità di dati. Gestire il rischio significa anzitutto saperlo valutare*

A tal proposito, è essenziale conoscere il business, valutare il contesto ed avere consapevolezza delle minacce relative all’azienda. Tutto ciò concorre a definire una strategia in grado di mitigare i rischi e ridurli entro i limiti del possibile.
In tale contesto su può parlare di una cosidetta “**intelligence aziendale**“, che secondo Rapisarda è una disciplina

fondamentale per integrare una serie di competenze complesse, dalla sociologia alla psicologia, dalla statistica alla giurisprudenza, dall'economia all'informatica, dalla logistica alle scienze della comunicazione. Ogni piccola parte contribuisce alla comprensione dell'insieme.
Ripercorrendo la nascita della cultura dell'intelligence, Rapisarda ha ricordato ancora la **figura di Mattei** ed il suo ruolo centrale dell'individuare le opportunità di sviluppo industriale nazionale attraverso metodiche analisi sui Paesi, sulle potenzialità e sugli aspetti contrattuali e commerciali in grado di rendere appetibile l'accesso di Eni a mercati che prima le erano preclusi.

Rapisarda ha concluso il suo intervento parlando del rischio attuale della **cybersecurity**, dove c'è ancora poca esperienza, sensibilità e norme. «In un mondo che usa in maniera rilevante internet e che diventerà sempre più "virtuale" la rete sarà sempre più un campo di battaglia.

> *L'aumento esponenziale delle connessioni imporrà di approntare strumenti adeguati per coniugare business e sicurezza non solo nelle aziende ma anche per proteggere la sfera privata.*

La sicurezza informatica è indubbiamente il bisogno emergente. Gli attacchi informatici aumentano anche nel nostro Paese in tutti i settori ed è ancora estremamente difficile disporre di strumenti giuridici in grado di prevenire e tutelare la privacy aziendale e personale».

Anche in questo campo, come in generale sul tema della security è centrale, secondo Rapisarda, il **fattore H**, il fattore umano, che è l'anello debole di ogni sistema di sicurezza. Il manager ha concluso: «Bisogna pensare alla sicurezza prima che serva. La fiducia, il coinvolgimento e la sensibilizzazione di tutti gli operatori dell'azienda sono decisivi per lavorare nell'ambiente più sicuro possibile».