

NEWS  
29/3/2010

## Tlc, fa più paura un terremoto di un attacco informatico

Infrastrutture di trasporti, energia e comunicazione esposte a catastrofi naturali più che a terrorismo. Un black out può mandare in tilt un Paese

ROMA

Fa più paura «un **terremoto** o un'**alluvione**» di «un **cyber attack** per la sicurezza delle **reti critiche**» come le **infrastrutture di trasporti, di energia elettrica**, di telecomunicazioni o **sistemi economico-finanziari e banche**. È più preoccupato dai terremoti che dai cyber terroristi Sandro Bologna dell'Unità Calcolo e Modellistica dell'Enea che all'*Adnkronos* spiega gli scenari «più realistici» di **protezione** contro i **rischi di black out** di elettricità, trasporti o Tlc che potrebbero mandare in **tilt un intero Paese**.



«La protezione delle infrastrutture critiche -afferma Bologna- è un problema che va affrontato anche tenendo conto che i maggiori rischi sono esterni alle strutture stesse e, per la maggior parte, sono rischi derivanti da **catastrofi naturali** piuttosto che da **attacchi informatici**. Basti pensare che a mandare in tilt i bancomat, i check-in di Fiumicino e le banche della Capitale, il 2 gennaio del 2004, fu un allagamento degli impianti di Tor Pagnotta e non un attacco informatico a bloccare la rete Tlc di Roma Sud».

E se gli attacchi informatici evocano maggiori paure e fanno spendere, secondo il recente rapporto commissionato dal McAfee al Csis di Washington,

6,3 mln di dollari al giorno, sono le catastrofi naturali a dover essere ugualmente messe al centro dell'attenzione, secondo l'esperto dell'Enea. «Per realizzare un attacco informatico ad una rete protetta -sottolinea Bologna- è necessario avere altissime competenze ingegneristiche e conoscere dall'interno i potenti sistemi di protezione informatica di queste infrastrutture sensibili». Due fattori chiave, dice Bologna, «non certo facili da trovare sul mercato».

«Inoltre, se guardiamo le statistiche -continua Bologna- i casi di cyber attack nel mondo sono davvero pochi. In 10 anni i maggiori black out sono stati determinati da eventi naturali o errore umano e non da attacchi informatici». Ma come difendere le reti critiche evitando pericolosi black out ad intere popolazioni? «Tra le strategie più accreditate -spiega Bologna- c'è il self healing, l'autoguarigione o autocicatizzazione dei buchi informatici che possono mandare in tilt reti critiche. E la ricerca guarda al mondo biologico per trovare soluzioni. Anche le reti di smart grid possono essere una soluzione». E sono due, inoltre, i punti tecnici rilevati da Bologna per alzare il livello di sicurezza delle reti critiche.

«Innanzitutto -spiega- è necessario diminuire la penetrabilità, la vulnerabilità di queste infrastrutture, poi rendere questi sistemi resilienti, cioè bisogna renderli capaci di erogare comunque il servizio». Quindi infittire la «policy di sicurezza delle aziende sul personale che,

comunque, esiste già» aggiunge ancora l'esperto dell'Unità Calcolo e Modellistica dell'Enea, ribadendo che la vera azione di protezione «deve tenere conto dei fattori esterni dovuti alle catastrofi naturali».

E di sicurezza delle infrastrutture critiche si è parlato oggi al summit tecnico e scientifico promosso a Roma dall'Aiic (Associazione italiana esperti infrastrutture critiche) e dall'Enea sulla fragilità e protezione delle infrastrutture critiche, materia su cui è da poco intervenuta una Direttiva Ue su cui dovrà esprimersi anche il nostro Paese. Molti gli esperti intervenuti all'Enea e rappresentanti del mondo delle università e della ricerca, del Dipartimento della Protezione Civile, di Banca d'Italia, Gse, Cnr, Enav, Jrc-Ispra, Telecom Italia, Booz & Co, **Eustema** e Formit.

Obiettivo dell'incontro è stato mettere in comune le esperienze nate dall'attività quotidiana di gestione di infrastrutture critiche e da studi ed attività di ricerca delle comunità scientifiche per individuare sistemi di protezione. Il summit dell'Enea arriva anche in risposta alla Direttiva Ue che richiede agli stati membri di individuare le European Critical Infrastructure (Eci) nazionali entro il 2011 per una strategia comunitaria di gestione e protezione, visto la stretta implicazione per i diversi Paesi di ogni rete critica. «Mentre negli Usa -spiega Bologna- sono 18 i settori delle reti ritenute infrastrutture critiche, in Europa la Direttiva del dicembre 2008 ha classificato come reti critiche solo quelle dei settori energia e trasporti, e poi forse potrebbero essere inserite le Tlc. Ora i Paesi membri sono chiamati, entro il 2011, a individuare all'interno di questi due settori, le proprie reti critiche».

«Anche l'Italia -prosegue l'esperto dell'Enea- dovrà definire i propri Eci nazionali e dovrà farlo presto visto che siamo in ritardo a causa di un rimbalzo di competenze fra differenti istituzioni. Dovremo quindi fare l'analisi fra le diverse reti energetiche, per esempio la rete Gas o la rete elettrica, ed individuare eventuali altri settori critici come, per esempio, gli impianti da rinnovabili». L'obiettivo europeo di strategia comune ha un senso importante per le diverse popolazioni comunitarie. «Il black out del 2003 -sottolinea Bologna- ci ha infatti insegnato che un'errata manovra compiuta in Svizzera ha tolto la corrente a noi. Quindi serve una linea comune».

Una linea che però «esclude il nucleare che -riferisce Bologna- ha una regolamentazione tutta propria». Ed in questo scenario, conclude Bologna, «l'Enea ha il ruolo di supporto tecnico-scientifico. Stiamo cercando di realizzare laboratori per affrontare il tema della interdipendenza delle reti critiche, ovvero se scatta la rete Tlc come posso gestire la rete elettrica». «Tema -aggiunge- che stiamo affrontando nel nostro laboratorio di modellistica e simulazione dove studiamo il fenomeno di ricaduta a cascata». E sul cyber attack? «Abbiamo un laboratorio che si sta occupando di questo aspetto. Ma -conclude l'esperto dell'Enea- ripeto, attacchi così sono operazioni complesse e se ne contano pochissime nel mondo».