ENEA

nòva 24 24 ORE

30/10/2008

Sicurezza distribuita

Modelli e piattaforme per valutare tutte le criticità del sistema Paese Puntando su sistemi connessi a rete

DI ROBERTO VACCA

I grandi sistemi tecnologici corrono rischi gravi dovuti a disastri naturali, guasti, errori di progetto e di gestione, impatti in cascata di guasti di altri sistemi e azioni violente (terrorismo, vandalismo). Per guardarsi dai terroristi si comincia a fare "data mining": raccolta e registrazione di dati su comportamenti e frequentazioni sospette, su disponibilità di strumenti distruttivi o sostanze venefiche, su messaggi che implichino premeditazioni. Su questa strada si eccede talora, specie in Usa, ove le unioni per le libertà civili protestano che è illegale spiare normali cittadini non sospetti. Pare che in Inghilterra si voglia imporre a chi compra un cellulare la registrazione dei dati del passaporto. È arduo dettare regole sensate per evitare rischi senza scadere nella tirannia. Parallelamente va studiato l'uso di scienza, tecnica, legge e politiche per proteggere sistemi e infrastrutture.

Il tema è stato analizzato da Critiso8, workshop sulla sicurezza delle infrastrutture critiche organizzato a Roma dall'Enea e dall'Aiic-Associazione italiana esperti infrastrutture critiche a metà ottobre con la partecipazione di 150 esperti internazionali.

Massoud Amin, professore dell'Università del Minnesota ha sostenuto che dovremo affidare controllo e supervisione dei grandi sistemi a strutture intelligenti e distribuite. In questo modo cresce la resistenza dei sistemi e anche la loro capacità di auto-rigenerarsi. Continuano a crescere complessità e interdipendenza dei sistemi, come anche le dimensioni e l'interconnettività di web e internet, a loro volta soggetti alle vicende di cavi e connessioni radio. È anche vitale l'efficienza umana degli operatori e degli utenti. Se ne deduce che adeguati modelli matematici di questo universo sono talora impossibili da creare o risulteranno molto vaghi. George Apostolakis dell'Mit ha suggerito di valutare rischi e ottimizzare le decisioni costruendo un albero dei valori. Ogni valore è definito come misura dell'impatto di un evento o di un componente sull'efficienza del sistema e, combinato con una valutazione di rischio, definisce un rango, usato per valutare le decisioni possibili.

Sujeet Shenoi, professore dell'Università di Tulsa, ha sottolineato la necessità di usare pragmaticamente scienza, tecnologie e misure politico-organizzative, oltre agli innumerevoli provvedimenti in corso di implementazione da parte di internet provider, istituzioni, organizzazioni tecniche e scientifiche, aziende e industrie per bloccare virus, malware e attacchi cibernetici vandalici o mirati. La possibilità che terroristi usino le connessioni telematiche per creare danni o panico è sempre più temibile, come dimostra quanto accadde in Lituania l'anno scorso, quando tutti i collegamenti telematici del Paese furono paralizzati per giorni dall'azione di un hacker; o quanto sperimentato dalla Georgia nei giorni del conflitto con la Russia. Andrea Valboni, di Microsoft, ha notato che la vulnerabilità ai virus dei computer in rete sta diminuendo, mentre aumentano i furti di identità e gli attacchi che mirano a causare gravi danni economici. Non esiste una soluzione finale al problema della sicurezza: occorre migliorare le difese mediante metodologia, cooperazione e tecnologie sempre più sofisticate.

Gli atti del workshop includono parecchie decine di lavori originali che descrivono in dettaglio tecniche e procedure di modellistica e di progetto mirate a conseguire maggiore sicurezza delle infrastrutture critiche. Cito fra i tanti interessanti, il notevole lavoro di Eric Luiijf et al. (Tno e Università di Delft). È un'analisi eseguita su una base dati di 2.375 seri incidenti verificatisi in infrastrutture critiche europee, evidenziando le conseguenze che ciascuno ha prodotto a cascata in infrastrutture adiacenti. Ricerche analoghe su sequenze Scada (Supervisory control and data acquisition) andranno fatte con continuità su scala crescente. Menziono, a titolo di esempio, il lavoro di Marco Beccuti (Università del Piemonte Orientale, et al.) su un modello delle interazioni fra un'infrastruttura di informazione (centro di controllo computerizzato) e una elettrica (sottostazione). Un difetto della prima (connessione Lan, firewall, denial of service) menoma o annulla le prestazioni della seconda e, con certi ritardi viceversa.

In una tavola rotonda a conclusione dei lavori è stato sottolineato come analizzare e prevedere i rischi sistemici sia vitale, ma che questa attività non è considerata prioritaria dai decisori privati e pubblici. Dovrebbe essere essenziale effettuare azioni per massimizzare l'impatto di risultati come quelli descritti sull'opinione pubblica e sui centri decisionali. A questo fine, però, occorrerebbe assicurarsi la cooperazione di radio, televisione e giornali, ma i mezzi di comunicazione di massa costituiscono notoriamente un grande sistema largamente degradato, forse irrecuperabile.

Rispetto a un analogo workshop organizzato dall'Enea nel 2006 (Cnipo6), pur rimanendo scarsa la consapevolezza dei decisori italiani il vero passo avanti a livello nazionale sta nel fatto che Enea ha varato

un progetto strategico – «Governo e sicurezza delle reti tecnologiche ed energetiche» – mirato ad affrontare le sfide poste dalla globalizzazione, dalle privatizzazioni delle reti e dalle liberalizzazioni, che incrementano le interdipendenze.

Il progetto sviluppa un sistema di conoscenze, modelli e tecnologie per affrontare il problema della sicurezza delle grandi infrastrutture critiche (specie energetiche) creando piattaforme di simulazione e prova da mettere a disposizione degli operatori. ◆

L'emergenza alla grid

Quattro architetture. Il sistema nordamericano di energia elettrica, chiamato in gergo "the grid", è articolato su quattro architetture di interconnessione all'interno delle quali ci sono centinaia di migliaia di generatori, linee di trasmissione e sottostazioni. Il piano di emergenza tiene conto che l'elettricità fluisce alla velocità della luce ed è antieconomico il suo stoccaggio in grandi quantità, che l'energia viene prodotta nel momento in cui deve essere usata e il sistema deve essere in grado di rispondere rapidamente a richieste o cambiamenti. L'energia elettrica si muove liberamente dai generatori ai consumatori lungo tutti i percorsi di corrente alternata disponibili e la ridondanza della rete garantisce sufficiente resistenza alle sollecitazioni e alle relative variazioni. Il piano di soccorso si basa su dinamiche di bilanciamento delle fonti di alimentazione e di mantenimento di voltaggi e potenze richieste, attuabile tra l'altro mediante un monitoraggio delle linee e degli impianti mirato a garantire condizioni stabili, reindirizzando i flussi ed evitando pericolosi surriscaldamenti. *(dav.m.)*

I punti critici

- Agricoltura e alimentare
- Edifici commerciali
- Industria di base della difesa
- Edifici governativi
- Reattori nucleari
- Trasporti
- Banche e finanza
- Comunicazioni
- Servizi d'emergenza
- Information technology
- Posta e porti
- Acqua
- Industria chimica
- Dighe
- Energia
- Monumenti nazionali
- Sanità pubblica

Strategie d'azione