

SICUREZZA

## La "guerra fredda" informatica costa 6,3 mln di dollari al giorno

**Secondo il rapporto McAfee-Csis a farne le spese sono soprattutto le infrastrutture critiche. Tucci, presidente Aiic: "Le tecnologie migliorano l'erogazione dei servizi ma comportano impreviste vulnerabilità"**

La "guerra fredda informatica" è in atto e ogni giorno presenta complessivamente un "conto" molto salato, stimato in 6,3 milioni di dollari. A farne le spese sono soprattutto le infrastrutture critiche, ossia i sistemi a rete che consentono la normale vita di un Paese, come quelli di trasporto di persone e merci, le reti idriche ed energetiche, telecomunicazioni e dati, sanitarie, economico-finanziarie, le reti di governo, quelle funzionali alla sicurezza nazionale e alla gestione delle emergenze. È quanto emerge dal rapporto "Nel mirino, l'infrastruttura critica nel periodo della guerra informatica", commissionato dalla McAfee al Csis-Center for Strategic and International Studies di Washington, che ha posto in evidenza come il rischio sia in aumento.

"Lo sviluppo, la sicurezza e la stessa qualità della vita nei paesi industrializzati dipendono dal funzionamento continuo e coordinato di un insieme di installazioni che, per la loro importanza e strategicità, sono definite Infrastrutture Critiche - spiega Salvatore Tucci, ordinario alla facoltà di ingegneria dell'Università di Roma Tor Vergata e presidente dell'Aiic - Associazione Italiana Esperti Infrastrutture Critiche -. Per ragioni di natura economica, sociale, politica e tecnologica esse sono diventate sempre più complesse ed interdipendenti. Se ciò ha migliorato la qualità dei servizi erogati contenendo i costi, ha però indotto impreviste vulnerabilità, in concomitanza con situazioni di crisi, eventi eccezionali o atti terroristici. Fragilità connessa alla loro elevata interdipendenza che rischia di indurre un pericoloso 'effetto domino', ripercuotendosi a tutto il sistema".

Intervistati per il rapporto di McAfee, il 54% dei 600 dirigenti responsabili della sicurezza di aziende che, a livello mondiale, forniscono e gestiscono infrastrutture critiche di 14 Paesi, ha ammesso di aver già subito attacchi su larga scala o "infiltrazioni occulte" da parte di gang criminali o di terroristi.

Proprio sulla fragilità e protezione delle infrastrutture critiche, materia su cui da poco intervenuta una Direttiva Ue, il 29 marzo a Roma ci sarà un summit tecnico e scientifico, promosso dall'Aiic e dall'Enea. Tra i partecipanti ci saranno i rappresentanti del mondo delle università e della ricerca, del Dipartimento della Protezione Civile, Banca d'Italia, Gse, Cnr, Enav, Jrc-Ispra, Telecom Italia, Booz & Co, **Eustema** e Formit, che metteranno in comune le esperienze derivanti dall'attività quotidiana di gestione di infrastrutture critiche e da studi ed attività di ricerca delle comunità scientifiche.

L'indagine del Csis per McAfee ha messo in evidenza che, nonostante l'elevazione delle barriere tecnologiche e l'adeguamento delle normative, il 37% degli intervistati ha ammesso che la vulnerabilità è aumentata negli ultimi dodici mesi. Ma addirittura due quinti si attende un incremento degli incidenti di sicurezza.

"Data l'attuale situazione economica, è necessario che le aziende si preparino alla instabilità che gli attacchi informatici sulle infrastrutture critiche potrebbero causare - puntualizza Dave DeWalt, amministratore delegato di McAfee - perché ci sono sistemi dai quali dipendiamo ogni giorno, dal trasporto pubblico all'energia e telecomunicazioni, e un attacco ad uno di questi settori potrebbe provocare sconvolgimenti economici molto estesi, disastri ambientali, perdita di proprietà e persino della vita".

Lo scenario che emerge dal report è allarmante. C'è poca fiducia nel livello di preparazione (soprattutto in Arabia Saudita, India e Messico); c'è la percezione di un aumento dei rischi anche per i tagli alle risorse per la sicurezza imposti dalla recessione (riduzioni rilevanti sono state registrate nell'energia, 27%, e nel gas-petroliero, 31%); e dell'implicazione di istituzioni e Paesi stranieri negli attacchi (tra quelli più colpiti dalle minacce gli Usa e la Cina); si riconosce che le leggi sono ancora inefficaci per la protezione da attacchi (lo crede il 55% degli interpellati, maggior scetticismo in Russia, Messico e Brasile); l'onere maggiore delle aggressioni lo sostengono le compagnie d'assicurazione, ma parte ricade anche su clienti e contribuenti.

L'Italia non brilla per il livello di adozione delle misure di sicurezza per la protezione delle infrastrutture critiche: mentre al primo posto nella corsa c'è la Cina (62%), seguita da Usa (53%) e Inghilterra (51%); nel gruppo di coda, dietro alla Germania, c'è il nostro Paese, seguito da Spagna e India (tutti sotto il 40%).

Tra le fragilità dei sistemi ci sono gli standard di autenticazione, basati ancora sul vecchio sistema "username - password" e, invece, molto poco sulla tecnologia biometrica. E questo facilita gli attacchi che gli hacker compiono sempre di più ai danni dei singoli utenti mediante attacchi di phishing. Altro motivo di allarme è la crescente diffusione del "cloud computing", in base al quale i programmi e le applicazioni non sono più nei pc ma nei server remoti, scelta vista con favore dalle aziende, ma che - secondo gli esperti di sicurezza e protezione delle infrastrutture critiche - crea un nuovo fronte di fragilità dei sistemi.

Un problema che è emerso con frequenza riguarda la risposta dei Governi alle nuove minacce. Esistono modelli comuni, come i team per le emergenze informatiche, i Cert- Computer Emergency Response Team (in Italia è attivo presso l'ex CNIPA, ora DigitPa) per la gestione della reazione agli eventi di sicurezza. Ma la loro efficacia non è omogenea e in molti casi si assiste ad un costante "lavori in corso". Il rapporto McAfee-Csis si conclude con una considerazione-appello: "Se il cyberspazio è il Far West, allora lo sceriffo deve riportare l'ordine". Ossia spetta ai governi intervenire sulla sicurezza delle reti che coinvolgono le infrastrutture critiche, cioè il normale svolgimento della vita di un Paese.