PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 21 - numero 4453 di Martedì 23 aprile 2019

La sicurezza informatica è ormai un problema di dimensione mondiale

Anche le Nazioni Unite hanno compreso che il problema della sicurezza informatica richiede un approccio globale, coordinando le iniziative in tutti paesi del mondo. Ecco una proposta concreta.

Quasi ogni giorno i mezzi di comunicazione di massa ci danno notizia di attacchi informatici, che si verificano in varie parti del mondo. La crescente sensibilità a questi temi ha indotto la UNECE (United Nations Economic Commission for Europe), vale a dire l'organismo nel Nazioni Unite che coordina attività tecniche e commerciali a vario livello, ad avviare uno studio di una politica comune mondiale sulla protezione dei sistemi informativi.

In questo contesto, è stato messo a disposizione un documento di lavoro, sul quale tutti paesi sono chiamati ad esprimere il loro giudizio. Il documento è stato presentato a metà novembre 2018 a Ginevra e verrà riproposto, nella versione definitiva, nel corso del 2019.

Il documento vuole stabilire un approccio coordinato al problema della sicurezza informatica, dando incarico a gruppi di esperti di sviluppare delle regole comuni.

L'obiettivo è quello di promuovere una convergenza delle norme tecniche nazionali od internazionali, attualmente in vigore, o che stanno per essere messe in pratica in questo specifico settore, in modo da mettere a disposizione una politica coordinata di analisi di rischio. Questo approccio riduce le possibili smagliature fra le tecniche di sicurezza utilizzate in vari paesi, incoraggiando un più libero movimento di prodotti e di dati. Inoltre, per attività che coinvolgono vari paesi, viene garantito un approccio relativamente coerente, che minimizza la possibilità che avarie che si verifichino in uno specifico paese possano avere riflessi a cascata su numerosi paesi, collegati attraverso reti informatiche.

Anche se i principi di base della sicurezza informatica sono ben noti, vi sono ancora delle smagliature presenti nell'attività normativa di vari paesi. Ad esempio, anche se sono già disponibili delle valide norme, come la serie IEC 62443 e la serie ISO 27000, sono troppo diverse le modalità applicative nei vari paesi.

Particolare attenzione deve essere poi prestata alle infrastrutture critiche, che in tutti paesi del mondo rappresentano un bersaglio privilegiato degli hackers e hanno quindi bisogno di una strategia di sicurezza particolarmente efficace ed incisiva. Occorre però fare attenzione al fatto che occorre sempre individuare un equilibrio tra l'efficacia della protezione ed il costo di attuazione della protezione stessa.

Inoltre le norme internazionali sono recepite in modo diverso in vari paesi del mondo: ad esempio, in alcuni paesi il rispetto di norme nazionali o internazionali rappresenta un obbligo, mentre in altri paesi rappresenta solo una opportunità. Ecco perché si raccomanda che nei vari paesi del mondo vengano introdotti dei provvedimenti legislativi, che rendano obbligatorio il rispetto di determinate normative, che ormai hanno dimostrato di essere efficienti ed efficaci raggiungere l'obiettivo di proteggere un bersaglio da attacchi informatici.

Infine, occorre convalidare ancora una volta il principio che un sistema informativo può essere composto da parecchi sottosistemi, che possono fare capo a diversi soggetti: in questi casi, è obbligatorio uno stretto coordinamento di tutti i soggetti coinvolti, per raggiungere un livello omogeneo di sicurezza informatica.

In allegato metto a disposizione dei lettori questo documento, che può rappresentare un prezioso strumento per impostare e sviluppare una idonea attività legislativa.

Allegato (pdf)

Adalberto Biasiotti
