PRAGMEMA

Il valutatore economico automatico del rischio *cyber*

Il valutatore economico automatico del rischio *cyber*

Il modello valutativo automatico (*tool*) proposto si basa su un'analisi *ex-ante* di scenari che permette di giungere a una quantificazione dell'esposizione economica conseguente a un potenziale evento cibernetico.

Il modello, recuperando la tradizionale definizione di *cyber risk*, tiene conto:

- dell'impatto economico dell'evento, distinto a seconda del risultato dell'attacco: esfiltrazione, corruzione, distruzione di basi di dati e/o interruzione dell'operatività producono scenari e costi diversi;
- della probabilità di accadimento;
- delle vulnerabilità che affliggono le reti e i sistemi informativi utilizzati nello svolgimento dell'attività.

Utilità

Le tradizionali analisi del *cybersecurity risk* sono limitate a valutazioni *ex-post*, in cui si osservano gli effetti subiti dell'attacco e se ne dà una quantificazione economica successiva, oppure sono consolidate su mere analisi preventive basate su parametri qualitativi (scale di riferimento o punteggi di *rating*) che non forniscono contezza del valore economico e monetario del *cyber risk*

La valutazione svolta *ex-ante* consente una successiva indicazione del rischio assunto quantificato in termini monetari. Il comportamento automatizzato (*tool SIVARI*) risulta inoltre effettivamente conforme:

- al quadro normativo attuale che impone una seria attività di *risk assessment*
- alla consueta attività di pianificazione, programmazione e controllo tipica dell'organizzazione
- all'attività di allocazione delle risorse.

Funzionalità

Il *tool* di valutazione del rischio *cyber* offre le seguenti caratteristiche:

- identificazione degli *asset*, delle minacce e delle vulnerabilità che affliggono la rete e i sistemi informativi
- analisi delle fasi di attacco, tenendo in considerazione la piattaforma ontologica PragmemaPOC
- la valutazione dei costi, diretti e indiretti, a seguito dell'attacco mediante un'analisi per scenari oltre l'anno, ricorrendo alla metodologia del *Present Value*
- la quantificazione della probabilità di successo dell'attacco in base gli attuali modelli esistenti (ACT - *Attack countermeasure tree*, FTA - *Fault trees analysis*, raccomandazioni ENISA…)
- la quantificazione del rischio mediante combinazione delle variabili precedenti: probabilità, vulnerabilità e impatto
- l'identificazione delle misure di trattamento del rischio, a seconda dei risultati dell'attività valutativa
- la valutazione *ex-post* dell'efficacia degli interventi (analisi ROSI e VAN).

Casi di utilizzo

Il meccanismo di valutazione può essere implementato in tutte le organizzazioni pubbliche e private che in base al contesto dell'attività svolta e della dimensione devono effettuare una valutazione del rischio cibernetico al fine di impostare le contromisure necessarie (logiche, fisiche ed organizzative).

Descrizione tecnica

L'attività viene svolta con l'utilizzo di appositi *tool* per la fase di *risk assessment* e *risk evaluation* comprensivi di una *dashboard* che permetta di monitorare in via continuativa lo stato nell'organizzazione della sicurezza informatica e della protezione dei dati.

L'azienda

Pragmema srl
sede sociale e sede operativa piazza della cancelleria 85 -00186 Roma
tel. 06/68392146 fax 06/68211644
REA 1078363 P.I. 01224680551
www.pragmema.it