La tassonomia degli eventi e minacce cyber

L'Agenzia per la Cybersecurity nazionale adotta delle specifiche linee guida sulla tassonomia cyber, al fine di utilizzare un linguaggio comune per lo scambio delle informazioni relative a eventi e minacce cyber che hanno oggetto sia le imprese che le pubbliche amministrazioni.

di Mauro Alovisio - Avvocato

Il panorama degli attacchi cyber è in continua e costante evoluzione e pone molteplici sfide alle nostre imprese. L'**Agenzia per la Cybersicurezza nazionale**, nell'ottica di supportare la pubblica amministrazione e le imprese nel complesso percorso di consapevolezza dei rischi cyber, **definisce la tassonomia** (categorizzazione) **degli incidenti informatici**.

Il documento in esame ha le seguenti **finalità**:

- **agevolare** lo scambio di informazioni a livello nazionale attraverso l'adozione di un lessico comune che rappresenti una base metodologica sia per la condivisione di informazioni riguardo agli eventi cyber sia per la notifica degli incidenti al CSIRT Italia;
- **identificare**, **definire** e **caratterizzare** gli eventi cyber attraverso un'unica tassonomia rilevante a livello nazionale;
- **fornire** alle organizzazioni un documento che si armonizzi con le tassonomie internazionali in materia di cybersecurity e che sia al contempo adeguato al contesto normativo nazionale.

Durante la redazione sono state opportunamente prese in esame, infatti, le tassonomie preesistenti utilizzate in ambito internazionale e le norme in vigore riguardo alla notifica degli incidenti in carico ai soggetti appartenenti al Perimetro di Sicurezza Nazionale Cibernetica (PSNC), già effettuate in accordo a una “tassonomia degli incidenti”.

Nella parte introduttiva le linee guida richiamano i documenti ENISA e Trusted Introducer, Mitre Corporation, Unione Europea e Nato. Si tratta di documenti e standard preziosi ma che secondo ACN non forniscono un livello di granularità sufficiente: al fine di colmare le lacune: sono state, pertanto, elaborate le linee guida ACN tassonomia Cyber (TC-ACN).

L'ENISA nell'ottica di definire una tassonomia unica per **supportare gli CSIRT europei** nel trattare di incidenti di cybersicurezza ha adottato la "*Reference Incident Classification Taxonomy*", che prende come riferimento la “*Incident Classification / Incident Taxonomy according to eCSIRT.net*” pubblicata nel 2012 da *Trusted Introducer Service* (anche noto come TI) e successivamente aggiornata nel 2015 sulla base della tassonomia degli incidenti elaborata dall'European CSIRT Network (eCSIRT).

Il documento ACN richiama la tassonomia così recepita da ENISA che classifica gli incidenti in 11 categorie con 32 relativi “esempi di incidenti”. Le **categorie** offerte da questa tassonomia sono generali e facilmente adattabili, per questo motivo sono state incluse nella TC-ACN (ad esempio *Abusive content, Availability, Fraud, Infomation Gathering*, etc).

Le linee guida consentono alle imprese e alle pubbliche amministrazioni di disporre un agile strumento per caratterizzare un evento attraverso 144 attributi al fine di specificarne la natura e fornire una descrizione granulare durante gli scambi informativi.

Si tratta di uno **strumento prezioso per aumentare la qualità delle informazioni scambiate e la velocità anche di reazione delle imprese agli eventi e minacce di cybersicurezza**.

Al fine di agevolare la lettura, **il documento si divide in tre parti**:

- un'introduzione di contesto;
- un secondo capitolo che contiene i riferimenti, in cui si forniscono i principali riferimenti e altre tassonomie cyber prese in considerazione nella definizione della tassonomia cyber;
- un terzo capitolo che descrive la tassonomia degli eventi cyber dell'ACN, in cui si riporta la tassonomia degli eventi cyber costituita da un insieme di attributi che li caratterizzano.

Al fine di agevolare la lettura e la comprensione delle linee guida il documento **si conclude con una sintesi grafica sulla Tassonomia Cyber dell'ACN**.

ACN specifica che **le linee guida forniscono**, a titolo esemplificativo e non esaustivo, **indicazioni di mero ausilio alle attività di sicurezza dell'Organizzazione** e non sollevano la

attività di sicurezza dell'Organizzazione e non sollevano la stessa dall'onere di porre in essere, nel rispetto della normativa vigente in materia di **cybersicurezza**, tutte le azioni ritenute necessarie per la prevenzione e mitigazione del rischio nonché la risoluzione degli impatti derivanti dal verificarsi di eventi e incidenti informatici. Inoltre, costituiscono un **documento importante** e utile perché individuano un **lessico** e un **linguaggio comune condiviso** e rappresentano una fotografia delle minacce e degli attacchi più frequenti (nel documento sono citati, in via esemplificativa: gli attacchi *vishing*, *ransomware*, *watering-hole, Denial of Service-DoS*).

Il provvedimento è frutto di uno sforzo apprezzabile ed è particolarmente utile per gli operatori di *Incident Response* e i consulenti ed esperti di *digital forensics* che dovranno collaborare a stretto contatto con i responsabili ICT e i legali per la ricostruzione e analisi degli incidenti alla luce anche delle importanti novità normativa di attuazione della direttiva Nis 2.