Il Perimetro Nazionale di Sicurezza Cibernetica si rafforza

Pubblicata la nuova tassonomia per agevolare le notifiche degli incidenti informatici degli altri beni "informatici" dei Soggetti Perimetro

Comunicato stampa del 12 gennaio 2023

www.acn.gov.it

Al fine di **rafforzare** il **Perimetro di Sicurezza Nazionale Cibernetica** è stato esteso l'ambito delle notifiche obbligatorie in caso di incidenti informatici. L'ACN, pertanto, ha elaborato la prevista tassonomia di tale ulteriore tipologia di incidenti informatici per renderne più agevole la notifica e il processo di valutazione degli impatti. Il processo di notifica, da compiersi entro 72 ore, riguarda tutti gli altri beni "informatici" dei soggetti compresi nel Perimetro.

Per dare attuazione all'emendamento nel decreto aiuti bis dell'estate scorsa che modifica le disposizioni di legge relative al Perimetro di Sicurezza Nazionale Cibernetica (articolo 1, comma 3-bis del decreto-legge n. 105 del 2019), **diventa obbligatorio notificare anche gli incidenti** che impattano su reti, sistemi e servizi informativi che non sono direttamente conferiti sotto il Perimetro stesso.

Questo vuole dire che **anche un tentativo di accesso agli altri beni "informatici"** rispetto a quelli protetti dal Perimetro **è da segnalare** al Computer Security Incident Response Team (CSIRT Italia) dell'Agenzia per la Cybersicurezza Nazionale - ACN.

Una piccola rivoluzione che dovrebbe facilitare la fase di supporto svolta dall'Agenzia a favore dei soggetti presi di mira dagli hacker.

La "**tassonomia**" (la categorizzazione), elaborata dai tecnici dell'ACN – alla stregua di quelle già pubblicate per gli incidenti in danno di Beni ICT conferiti nel Perimetro – è organizzata sotto forma di tabella, dove sono classificati in categorie gli incidenti informatici e le varie fasi dell'attacco, e indica per ogni tipologia di incidente un codice identificativo e la corrispondente categoria, accompagnata dalla descrizione di ciascuna tipologia.

A titolo esemplificativo, alla prima voce della tabella, l'incidente "ICP-C-1", riferito alla categoria "**Accesso Iniziale**", riguarda la situazione in cui un "soggetto ha evidenza dell'effettivo accesso non autorizzato all'interno della rete attraverso vettori di infezione, lo sfruttamento di vulnerabilità di risorse esposte pubblicamente o qualsiasi altra tecnica nota". Una diversa categoria, che riguarda i famigerati "**Movimenti Laterali**", prevede che si debba effettuare una notifica quando il "soggetto ha evidenza dell'impiego non autorizzato di tecniche utili a effettuare attività di ricognizione per acquisire conoscenze sul sistema e sulla rete interna". E così via.

Le categorie di incidente sono sei, dalla "Raccolta di dati" alla loro *esfiltrazione* fino al *phishing* mirato, ma ricomprendono la maggior parte delle tecniche di attacco informatico descritte dal MITRE ATT&CK un riferimento internazionale per le tecniche, tattiche e procedure di attacco informatico.

Quando sarà a regime (14 giorni da oggi) la notifica di tali incidenti sulla base della Tassonomia indicata **favorirà la tempestiva valutazione della situazione** e la stima di eventuali impatti sistemici. Questo significa che se, ad esempio, un fornitore nazionale di energia scopre e comunica velocemente un attacco, sarà possibile allertare subito altri fornitori potenzialmente oggetto della stessa aggressione. L'ampiezza dell'allerta e la velocità di risposta in questi casi possono fare la differenza tra un attacco riuscito e un attacco fallito.

Così, mentre **non cambia il percorso di notifica dei beni conferiti sotto il perimetro**, **le cui tempistiche vanno da 1 a 6 ore** in relazione al tipo di incidente, i soggetti perimetro che devono notificare gli incidenti che accadono fuori dei beni conferiti avranno tre giorni di tempo (72 ore) per segnalare il problema individuato. In questo modo l'ACN, a seguito delle fasi di triage, potrà fornire un'assistenza più rapida ed efficace oltre che valutare in anticipo eventuali attacchi sistemici e possibili spillover su asset conferiti nel perimetro dal soggetto.

La tassonomia adottata rappresenta insomma un altro tassello per favorire la collaborazione Istituzioni, PA e imprese, che erogano servizi critici per il nostro Paese, a beneficio della sicurezza nazionale cibernetica.

Che cos'è l'Agenzia per la Cybersicurezza Nazionale (ACN): L'ACN è l'Autorità nazionale per la cybersicurezza istituita con il D.L. 14 giugno 2021, n. 82, a tutela degli interessi nazionali nel cyberspazio. Garantisce l'implementazione della **strategia nazionale di cybersicurezza** adottata dal Presidente del Consiglio, promuove un quadro normativo coerente nel settore, ed esercita funzioni ispettive e sanzionatorie. Sviluppa collaborazioni a livello internazionale con agenzie omologhe. Assicura il coordinamento tra i soggetti pubblici e la realizzazione di azioni pubblico-private volte a **garantire la sicurezza e la resilienza cibernetica per lo sviluppo digitale del Paese**.