LE NUOVE REGOLE PER LE IMPRESE

Attacchi cyber da denunciare entro un'ora

Esame tra Camera e Senato per il Dpcm sulle notifiche degli incidenti informatici

Marco Ludovico
ROMA

In caso di attacco informatico, non c'è tempo da perdere. L'allarme deve scattare entro un'ora dalla scoperta, non un minuto di più. Nei casi meno gravi si può arrivare al massimo a sei ore.

L'incidente va notificato al Csirt (computer security incident response team) del Dis, dipartimento informazioni e sicurezza della presidenza del Consiglio. In caso di soggetti pubblici, il Dis invia poi le notifiche al ministero dell'Interno; se sono privati, al dicastero dello Sviluppo Economico. Gli enti colpiti, comunque, devono essere pronti a integrare la denuncia al più presto con le nuove informazioni e criticità sopraggiunte.

10
INDICAZIONI
Previste nel decreto dieci indicazioni sulla tutela delle informazioni con l'ausilio di strumenti elettronici e sette prescrizioni per la sicurezza fisica e documentale

È una rivoluzione per gli enti del cosiddetto perimetro di sicurezza nazionale cibernetica: soggetti pubblici ed operatori economici privati che svolgono funzioni essenziali per lo Stato o servizi «per il mantenimento di attività civili, sociali ed economiche fondamentali per gli interessi dello Stato». Il malfunzionamento delle loro reti, sistemi e servizi informatici può generare un rischio per la sicurezza nazionale.

In queste settimane tra Camera e Senato si discute un atto cruciale: il regolamento «in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici» inviato da Palazzo Chigi con uno schema di dpcm (decreto del presidente del Consiglio dei ministri). Dopo le osservazioni delle commissioni parlamentari – già espresso il parere del Consiglio di Stato - il dpcm nel testo riveduto avrà il sì definitivo dell'Esecutivo e si misurerà sul campo.

Le norme sono molto dettagliate e articolate. E tra le imprese circolano non poche perplessità. Il testo definisce le notifiche per gli attacchi, le misure di sicurezza da adottare, la classificazione degli incidenti e le azioni minime per la tutela delle informazioni. L'elenco degli incidenti è stato ripartito in quelli più gravi (infezione, guasto, installazione, movimenti laterali e azioni sugli obiettivi), con tempo massimo di notifica un'ora, e meno gravi, fino a sei ore per la denuncia.

Dopo l'attacco l'ente deve definire e avviare i piani di attuazione e ripristino e trasmettere al Csirt una relazione tecnica. A meno che, va messo nel conto, l'autorità giudiziaria non abbia comunicato esigenze di segretezza per l'azione investigativa. Ci sono poi 31 pagine di "allegato B" al decreto sulle misure di sicurezza da adottare, ecco i titoli: Identificazione, Protezione, Rilevamento, Risposta, Recupero.

C'è anche il quadro sulla tutela delle informazioni con «l'ausilio di strumenti elettronici» in dieci indicazioni; più quelle «per la sicurezza fisica e documentale» in sette prescrizioni. Tra le imprese, dunque, non mancano dubbi e riserve.

Osserva Andrea Chittaro, presidente di Aipsa (associazione italiana professionisti security aziendale): «L'intenzione è condivisibile ma il lavoro per le imprese sarà enorme. Il rischio è di conferire tante informazioni poco vagliate. A discapito della qualità».

@MarcoLUDOVICO