Sicurezza nazionale

PROTEZIONE DI SERVIZI E DATI SENSIBILI

Il provvedimento
Il decreto recepisce la direttiva europea Nis
Ora il parere delle commissioni parlamentari

I settori strategici
Le norme riguardano operatori di servizi essenziali come energia, trasporti, banche, sanità e finanza

Cybersecurity, nuove regole per le imprese

Multe fino a 150 mila euro - Sanzioni severe per chi non denuncia violazioni per evitare danni di immagine

Marco Ludovico
ROMA

Procedure, obblighi e sanzioni: palazzo Chigi detta le regole per un «livello elevato di sicurezza della rete e dei sistemi informativi». Consolida il ruolo centrale della Presidenza del Consiglio come autorità cyber con lo schema di decreto legislativo appena trasmesso alle commissioni parlamentari per il parere prescritto prima dell'ok definitivo.

Il testo definisce le regole per gli «operatori di servizi essenziali e dei fornitori di servizi digitali»: dovranno adeguarsi in modo uniforme per garantire prevenzione, difesa e tenuta contro gli attacchi. In ballo le grandi imprese di energia, trasporti, sanità, fornitura e distribuzione acqua potabile, il settore bancario e le infrastrutture dei mercati finanziari. E le infrastrutture digitali dove per «servizi digitali» il decreto annovera «mercato on line, motori di ricerca on line, servizi di cloud computing».

INTERESSI NAZIONALI
Le norme riguardano la sicurezza delle reti e dei sistemi informativi
La regìa della nuova governance a Palazzo Chigi

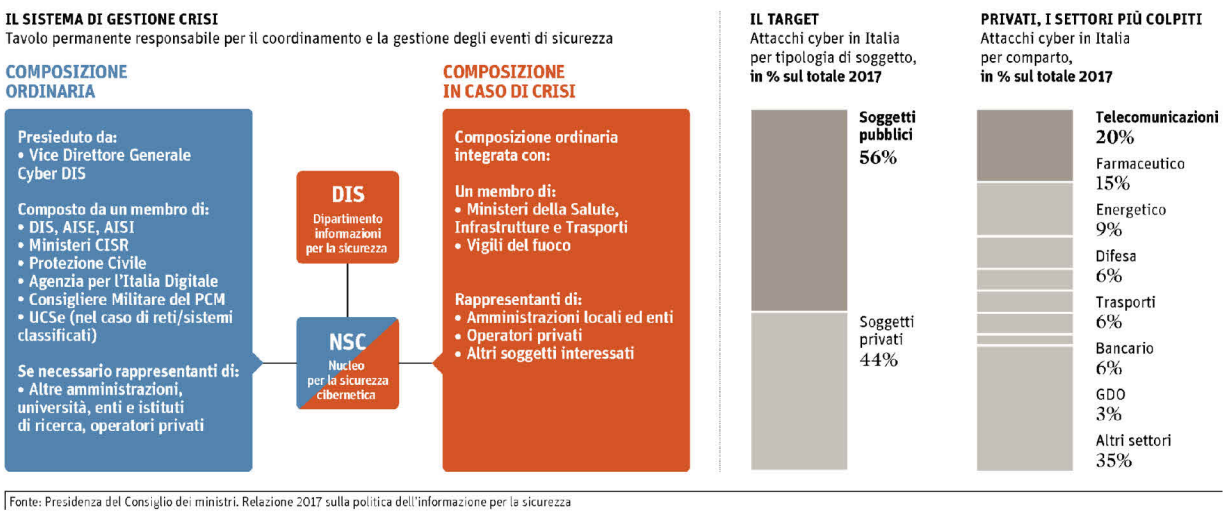
In caso di inadempienza alle nuove procedure, scattano sanzioni durissime: da un minimo di 12mila fino a 120mila euro - in otto ambiti di applicazione delle norme - ma nel caso di mancato rispetto di istruzioni vincolanti salgono fino a 150mila. Atteso da tempo, il provvedimento attua la direttiva Ue n. 1148/2016 Nis (Network and Information Security). È il seguito coerente e rispecchia in pieno il decreto del 17 febbraio 2017 del presidente del Consiglio, Paolo Gentiloni, sulla nuova architettura nazionale cyber dove al centro si pone il Dis (dipartimento informazioni sicurezza). Il nuovo decreto istituisce il Csirt (Computer Security Incident Response Team) nazionale presso la Presidenza del Consiglio: sostituirà il Cert (Computer Emergency Response Team) nazionale presso il Ministero per lo sviluppo economico e il Cert-Pa operante all'Agenzia per l'Italia digitale.

Il senso strategico del provvedimento è fissare l'unicità del comando nella catena decisionale, soprattutto in caso di attacco. Gli operatori di servizi essenziali non sono individuati nel concreto dal testo: lo dovranno fare «entro il 9 novembre 2018» i ministeri di riferimento, definiti «autorità competenti Nis» dei rispettivi settori. Mise (energia e infrastrutture digitali), Infrastrutture (trasporti), Mef (settore bancario e infrastrutture dei mercati finanziari), Salute (assistenza sanitaria), Ambiente (fornitura e distribuzione acqua potabile). Il Dis, invece, è definito «punto di contatto unico in materia di sicurezza delle reti e dei sistemi informativi» anche per «garantire la cooperazione transfrontaliera» delle autorità Nis con quelle «degli altri Stati membri» dell'Unione europea.

Dis e ministeri interessati, inoltre, «consultano» e «collaborano» con il Garante per la protezione dati personali e con «l'autorità di contrasto» ai crimini informatici, «organo centrale» del ministero dell'Interno guidato da Marco Minniti, vale a dire la Polizia postale e delle telecomunicazioni presso il dipartimento di Pubblica sicurezza. Prevista anche una «cooperazione a livello nazionale» con Regioni e Province autonome attraverso un «comitato tecnico di raccordo» presso palazzo Chigi composto da rappresentanti delle amministrazioni statali, regionali e provinciali. Certo, la sfida contro la minaccia cyber è immane. Nel 2017 sono state colpite oltre un miliardo di persone nel mondo con danni globali per oltre 500 miliardi di dollari, secondo il Rapporto Clusit 2018 presentato ieri a Milano: la crescita è stata del 240% degli attacchi informatici rispetto al 2011.

Ma l'Italia ora deve rendere organica ed efficiente anche la catena produttiva dei sistemi di difesa - e di attacco - in dotazione alle nostre imprese. È il senso di fondo della relazione di recente approvata del Copasir, presieduto da Giacomo Stucchi (Lega), sui sistemi informatici per l'intercettazione dati e comunicazioni, relatori Giuseppe Esposito (Udc) e Angelo Tofalo (M5S). Dopo casi critici di fughe di dati sensibili per la sicurezza nazionale - il caso Hacking Team del 2015 - il Copasir sottolinea l'urgenza di «accrescere il volume degli investimenti e delle risorse personali, tecnologiche e finanziarie per tutelare il principio della sovranità nazionale nel capo della sicurezza cibernetica». In campo ci sono lo Stato, le imprese pubbliche e private, ma serve garantire una filiera nazionale della sicurezza informatica sotto controllo e priva di punti deboli. Come avvalersi di software e hardware stranieri, tuttora in uso, in grado di riportare ai rispettivi stati di origine informazioni sensibili.

L'organizzazione per la difesa e gli attacchi



Fonte: Presidenza del Consiglio dei ministri. Relazione 2017 sulla politica dell'informazione per la sicurezza