

Lo scudo del Golden power a difesa del Cloud nazionale

Cyber, nella Pa si comprerà un altro antivirus contro i rischi dei software russi

Marco Ludovico

ROMA

Il Cloud di Stato entra tra «le attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale». Può essere così difeso da eventuali scalate ostili di soggetti stranieri con lo scudo del golden power. La novità è introdotta dall'articolo 27 intitolato «Ridefinizione dei poteri speciali in materia di comunicazione elettronica a banda larga basati sulla tecnologia 5G e cloud» del decreto legge sull'emergenza ucraina approvato ieri dal Consiglio dei ministri presieduto da Mario Draghi.

Nella protezione esercitata con i cosiddetti poteri speciali rientrano anche «i servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G». Così «le imprese che, anche attraverso contratti o accordi, intendano acquisire, a qualsiasi titolo, beni o servizi relativi alla progettazione, alla realizzazione, alla manutenzione e alla gestione delle attività» legate al 5G o al Cloud devono notificare alla Presidenza del Consiglio dei ministri «un piano annuale» su settori d'interesse, programma di acquisti, descrizione dei beni e servizi di interesse e una lunga serie di altre specifiche e dettagli indicati nell'articolo 27 della bozza di decreto legge. La protezione, tra l'altro, si estende senza più limiti temporali anche alle notifiche intraeuropee. L'ombrello di protezione con i poteri speciali contro gli attacchi, sempre più diffusi come hanno segnalato i nostri servizi di informazione e sicurezza, è così sempre più ampio. Per 5G e Cloud il comitato interministeriale sul golden power costituito presso la Presidenza del Consiglio si avvale anche degli esperti dell'Acn, agenzia per la cybersicurezza nazionale. Attenzione, poi, al rispetto delle prescrizioni indicate dall'esercizio dei poteri speciali e in generale sulla normativa dello scudo: chi viola queste disposizioni rischia «una sanzione amministrativa pecuniaria fino al tre per cento del fatturato del soggetto tenuto alla notifica».

Un'altra normativa di rilievo prevista dal decreto sull'emergenza Ucraina è inserita dal capo tre della bozza del Dl, «Cybersicurezza delle reti, dei sistemi informativi e dei servizi informatici e degli approvvigionamenti». È il cosiddetto

problema dell'antivirus Kaspersky di produzione russa, ottima fattura, adottato da anni in migliaia di uffici pubblici e privati. Ora però è una potenziale e insidiosa minaccia hacker. Le nuove norme, concertate tra i ministeri interessati, l'Acn e l'ufficio del sottosegretario Franco Gabrielli, «al fine di prevenire pregiudizi alla sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche», prevedono che la Pa provveda «tempestivamente alla diversificazione dei prodotti in uso». Va così fatto «l'acquisto di un ulteriore prodotto o servizio tecnologico di sicurezza informatica». Un antivirus, un antimalware, un firewall. L'urgenza dell'intervento e l'emergenza conclamata escludono per gli uffici pubblici il rischio di un intervento della Corte dei Conti a censurare i nuovi acquisti.

© RIPRODUZIONE RISERVATA