

Ministero della Difesa spagnolo sotto attacco: si tratta di cyber spionaggio

Floriana Giannotti

L' 11 marzo scorso, a distanza di circa tre mesi dall'accaduto, il Ministero della Difesa spagnolo ha dichiarato di aver subito un attacco cibernetico alla propria rete Intranet. Per oltre tre mesi, infatti, il virus non era stato rilevato.

L'indagine, condotta dal Mando conjunto de ciberdefensa e dal Centro de sistemas y tecnologías de la información y las telecomunicaciones, è ancora in corso, ma per il momento non sembra siano stati compromessi dati di rilevanza strategica.

Si teme, tuttavia, che nel corso dei tre mesi il malware, introdotto presumibilmente attraverso un'azione di "spear phishing", possa aver colpito altre reti, con l'obiettivo di rubare segreti tecnologici dell'industria militare spagnola.

E sebbene la rete Intranet non gestisca dati riservati ma solo quelli relativi alla gestione degli uffici, non si può sottovalutare che essa conta circa 50000 utenti e che collega il ministero della Difesa allo Stato maggiore della Difesa e alle unità dell'esercito spagnolo.

A ciò si aggiunga che il Centro nazionale di crittografia (CCN) ha rilevato, solo nel corso del 2018, circa 34000 "incidenti" legati al cyber spazio, che avrebbero colpito il settore pubblico spagnolo e imprese di rilevanza strategica (in particolare dei settori energetico, finanziario e dei trasporti), mettendo a rischio non solo la tutela di dati sensibili e riservati, ma addirittura la sicurezza nazionale della Spagna: secondo alcuni studi, il Ministero della Difesa e degli Affari Esteri sarebbero particolarmente esposti ad attacchi cibernetici, tanto è vero che l'Informe anual de seguridad nacional, approvato lo scorso 15 marzo, qualifica il cyber spionaggio come grave minaccia alla sicurezza nazionale.

Lo stesso CCN sostiene inoltre che dietro il 90% degli attacchi cibernetici contro le istituzioni e le imprese spagnole ci sarebbe uno Stato.

Anche in questo caso si ripropone il problema di individuare gli autori degli attacchi. Un attacco cyber come questo subito dalla Spagna sembrerebbe troppo complesso per essere attribuito ad hackers o hacktivisti, tanto che il governo di Madrid ritiene che dietro ci sia una potenza straniera. Evidentemente le misure di salvaguardia da eventuali attacchi cyber annunciate nel novembre del 2017 (alla vigilia del referendum sull'indipendenza della Catalogna) dal Ministro dell'Interno Zoido e dalla Ministra della Difesa Dolores de Cospedal Garcia non sono state efficaci se per oltre tre mesi il virus ha potuto agire indisturbato.

Si ripropone, quindi, la vexata quaestio: chi c'è dietro questi attacchi? A questo proposito c'è da aggiungere che la Spagna non ha mai avuto dubbi nell'attribuire gli attacchi alla Russia (senza però fornire le prove del J'accuse). In ogni caso non è possibile fare ipotesi accusatorie fin tanto che non saranno (semmai lo saranno) rese note le caratteristiche del virus: più è sofisticato e anomalo, meno è probabile che sia stato creato da normali, per quanto geniali, pirati informatici.

E quanto peso hanno simili attacchi nel modificare i rapporti di forza nello scacchiere internazionale? A tale riguardo va sottolineato il tentativo della Spagna di coinvolgere l'Unione Europea in questo suo "conflitto" con la Russia, ben sapendo che l'isolamento nei rapporti internazionali non è di certo il miglior alleato.

Questo ultimo attacco dimostra l'impreparazione di fatto dei sistemi europei. Nonostante, infatti, l'adozione della Direttiva NIS (Network Information Security) raccomandi una collaborazione interstatale, sembra non più procrastinabile il progetto di un partenariato pubblico-privato volto a contrastare minacce cibernetiche che possano colpire servizi pubblici essenziali.

Pur essendo la dimensione cibernetica a tutti gli effetti una delle cinque dimensioni della conflittualità, rimane tuttora la più difficile da regolamentare così come difficili da prevedere sono gli effetti di eventuali attacchi nelle relazioni internazionali.

Una cosa è certa: le guerre ibride mettono a serio rischio le democrazie.