IL SOLE 24 ORE.it

«L’attacco hacker? Forse un diversivo che nasconde una strategia più complessa»

Il presidente di Netgroup Giuseppe Mocerino spiega i dubbi sull’attacco dello scorso weekend: «Chi è stato risparmiato potrebbe essere sotto scacco»

di Giancarlo Calzetta

Venerdì 3 febbraio è stato lanciato un attacco informatico su larga scala che sfruttava una vulnerabilità nota scoperta due anni fa nei server EXSi di VMware per la quale esiste già un aggiornamento correttivo dal 23 di febbraio del 2022. L'impatto principale sembra essersi concentrato sulla Francia, da dove sono arrivate molte segnalazioni di richieste di riscatto portate da criminali che sono riusciti a installare un ransomware sfruttando quella falla informatica.

Nel nostro Paese, invece, le conseguenze sono state molto contenute e da un vertice tenutosi tra il sottosegretario alla Presidenza del Consiglio Alfredo Mantovano, il dg di Acn Roberto Baldoni e la direttrice del Dis-Dipartimento informazione e sicurezza, Elisabetta Belloni, ha rilevato che, anche se l'attacco è classificabile come grave, «nessuna Istituzione o azienda primaria che opera in settori critici per la sicurezza nazionale è stata colpita».

Giuseppe Mocerino, presidente di Netgroup

Ma c'è un altro scenario possibile: Giuseppe Mocerino, presidente dell'azienda specializzata in digitalizzazione del business e cybersecyrity Netgroup, sostiene che lo scenario potrebbe essere ben più complesso.

L'attacco è stato indicato come un evento probabilmente scollegato da eventi geopolitici e lanciato da cyber criminali interessati a ottenere un vantaggio economico. Lei forse non è così convinto. Qual è il problema?

«Quello che non convince in questo attacco è innanzitutto la scala rilevata. VMware dichiara di aver decine di migliaia di installazioni in Italia, ma i server colpiti sarebbero stati una manciata, un numero insignificante? Perché gli altri non sono stati colpiti? Siamo sicuri che siano davvero stati ignorati?»

In effetti, le segnalazioni di ransomware nel nostro Paese sono state pochissime e la maggior parte dei server colpiti erano degli honeypot, server trappola disseminati in Internet dalle agenzie e aziende specializzate in sicurezza per intercettare eventuali attacchi e osservare il comportamento dei pirati. Cosa è successo?

«Credo che esista la possibilità concreta che gli attacchi ransomware fossero solo un diversivo per indurre a credere chi non fosse stato colpito d'esser stato risparmiato dalla campagna d'attacco, ma non c'è nessuna garanzia in questo senso. Chi ci assicura che, invece, i server colpiti non fossero molti di più, ma invece di ricevere un ransomware non siano stati

destinatari di un malware silente pensato per spiare l'organizzazione proprietaria e carpirne le informazioni?»

VMware vanta installazioni in aree sensibili e centrali dei sistemi informatici di moltissime aziende e di ministeri o organi statali. Potrebbero essere i dati il vero obiettivo?

«Non possiamo saperlo con certezza e quello che mi preoccupa è che se si è trattato di un diversivo, sembrerebbe aver funzionato benissimo: non vedo preoccupazione e azioni di controllo prese dalle aziende e dal governo per scartare questa ipotesi. Anche perché il software attaccato è spesso usato per la gestione dei backup, un bersaglio ghiotto per criminali informatici e hacker di stato, dal momento che contengono tutte le informazioni più sensibili».

Cosa bisognerebbe fare per mettere al sicuro l'infrastruttura?

«La prima cosa è quella di attivarsi anche se non si hanno avuto segnali di attacco ransomware e verificare esattamente tutte le installazioni presenti in azienda, cercando segni di compromissione silente. Poi attivare delle misure per evitare che problemi del genere si ripresentino».

Che tipo di contromisure si dovrebbero adottare?

«È indispensabile, secondo me, appoggiarsi a strutture esterne per gestire correttamente le policy di *cyber hygene*, lasciando a un Msp, un fornitore di servizi esterni, l'onere di aggiornare e mantenere aggiornati tutti i sistemi. In quegli ambiti in cui non è possibile affidarsi ad aziende esterne, bisogna prevedere un team dedicato a questa incombenza. Non c'è una vera alternativa. Non dimentichiamo che questo attacco è stato portato sfruttando una falla vecchia di due anni e già corretta».