Aziende

Business is business

Attacchi informatici, Netgroup: «Attenzione agli hackeraggi a orologeria»

Il presidente di Netgroup Giuseppe Mocerino avverte: «Ci sono attacchi informatici silenziosi che fanno danno non immediatamente, bisogna attrezzarsi». Resta preoccupazione per le azioni dei gruppi cybercriminali filorussi.

Pubblicato il **14 Febbraio 2023 11:46** | Aggiornato il **14 Febbraio 2023 12:13**

di **Debora Faravelli**

Continuano gli **attacchi informatici** su larga scala da parte di gruppi cybercriminali filorussi. Il gruppo **Killnet** ha rivendicato sul suo profilo Telegram la responsabilità degli attacchi informatici di domenica mattina ai danni dei server della Nato. Un attacco semplice ma incredibilmente potente che – grazie alla **tecnica Ddos** (Distributed denial of service) – consente di coordinare migliaia di tentativi di accesso simultanei ai siti dell'organizzazione, facendo così crollare i server. La Nato ha fatto sapere che l'attacco ha riguardato solo i siti rivolti al pubblico, mentre la rete di comunicazioni protette, dove girano le informazioni classificate, non è stata toccata. Tuttavia, la preoccupazione è forte. Anche perchè quella del Ddos è una tecnica già sperimentata con successo in passato, e continua rivelarsi efficace. Lo scorso maggio, infatti, il gruppo aveva preso di mira diversi siti istituzionali italiani, tra cui quello del Senato e del Ministero della Difesa, e alcuni tedeschi collegati al Bundestag.

La preoccupazione per gli attacchi informatici

Una situazione allarmante che due settimane fa aveva reso necessario un vertice 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**. In quel caso sul tavolo c'era il dossier relativo al gigantesco attacco informatico ai server EXSi di VMware di venerdì 3 febbraio. Un attacco globale mirato principalmente ai server francesi che in Italia ha interessato solo marginalmente alcuni sistemi informatici. E, mentre qualche esperto del settore ridimensiona la gravità dell'attacco, c'è invece chi pensa che la vicenda potrebbe rivelarsi più grave di quanto sia apparsa.

L’avvertimento del Presidente di Netgroup Mocerino

È questa è l’opinione di **Giuseppe Mocerino**, importante imprenditore della cybersecurity e presidente di Netgroup – società con oltre mille dipendenti leader nelle soluzioni IT utili a fronteggiare i rischi della digitalizzazione. «Siamo sicuri che i tanti server non colpiti siano stati davvero ignorati?», si è chiesto l’esperto affermando che «è più probabile, invece, che questi attacchi fossero solo un diversivo per nascondere un malware silente pensato per spiare l’organizzazione che lo riceve e carpirne le informazioni». Al riguardo non vi è nessuna certezza, ha sottolineato, ma, se così fosse, gli hacker entrerebbero in contatto con le informazioni più sensibili dei server dato che questo tipo di malware attacca i software spesso usati per la gestione dei backup.

Logo Netgroup

La tesi di Mocerino parte dal presupposto che non avrebbe senso, per chi ha messo in campo un intervento su scala internazionale, procurare danni solo decine (in Italia) o a centinaia (su scala europea) di soggetti. Per questo non è azzardato pensare che abbiano colpito silenziosamente, cioè senza che le vittime ne abbiano percezione e quindi siano indotte a fare controlli, per poi danneggiare a orologeria nel tempo. Di qui la necessità, secondo l’imprenditore, di proteggere tutte le infrastrutture, per esempio verificando tutte le istallazioni presenti in azienda e lasciando ad un fornitore esterno esperto l’aggiornamento periodico di tutti i sistemi. Solo il fattore umano, secondo lui, può giocare un ruolo chiave nella protezione dei nostri dati: proprio Mocerino più volte ne ha ribadito l’importanza, ricordando anche la mancanza in Italia di almeno 100 mila risorse da impiegare nel settore della **cybersecurity**. Se ci dovessimo preparare alla Prima Guerra Mondiale informatica, ha concluso, occorre dunque ripensare alle politiche di cyber hygene e agli investimenti di cybersicurezza, sia a livello pubblico che a livello privato.