IL SECOLO XIX

VIRUS

Attacco cyber, “panico ingiustificato in un Paese ancora immaturo”

Il ransomware avvistato tra il 3 e il 5 febbraio continua a colpire. L’Italia è impreparata, ma ha un’occasione per fare il salto di qualità. Il parere degli esperti

Il data center di Liguria Digitale, società della Regione Liguria (ansa)

FRANCESCO MARGIOCCO

08 Febbraio 2023 alle 08:46 | 2 minuti di lettura

Genova – L’attacco informatico avvistato il 3 febbraio dal Computer emergency response team francese e poi dall’Agenzia per la cybersicurezza nazionale italiana sta colpendo ovunque, in Francia, Italia, Canada, Stati Uniti, e **potrebbe colpire ancora a lungo**.

È un **ransomware**, un virus che rende inaccessibili i dati del computer infettato e chiede il pagamento di un riscatto per ripristinarli, e che sceglie i bersagli senza criterio. Michele Zunino lo paragona alla pesca a strascico, oppure, immagine più efficace, a una **bomba a grappolo**. “Ma non drammatizziamo. Dopo anni di sottovalutazione del problema, è un bene che se ne parli”. Zunino è amministratore delegato di Netalia, azienda italiana di **cloud computing** con sede a Genova ed è logico che veda nel cloud computing (che consiste nell’archiviare dati, ed elaborarli, in un hardware remoto raggiungibile via internet, invece di usare un server locale) la soluzione. “I cloud sono gestiti da grandi aziende specializzate che, sfruttando economie di scala, costruiscono sistemi di difesa complessi e robusti”.

Il passaggio al cloud, dice Zunino, è un cammino lento. «Le aziende più grandi e strutturate si sono incamminate, per quelle più piccole la strada è in salita. Pensano di non averne bisogno, perché tanto nessuno le colpirà, dicono. Si sbagliano: **questi attacchi sono indiscriminati**”.

L’attacco di questi giorni sfrutta una falla del **Vmware Esxi** che è una macchina virtuale, un software che simula un computer che non esiste, per distrarre il virus, attrarlo e lasciargli credere di avere infettato il computer vero quando invece è caduto in trappola. “Questa volta il virus è stato più intelligente”, commenta Rodolfo Zunino, che non è parente di Michele e insegna cybersecurity al corso di ingegneria elettronica dell’**Università di Genova**. “Si è accorto dell’inganno e ha fatto un salto sul computer vero”.

Marco Bavazzano ricorda che “sono cose che accadono tutti i giorni” e pensa che l’allarme sia “ingiustificato”. Bavazzano è amministratore delegato di un’azienda, Axitea, con sede a Milano, 1.600 dipendenti in Italia e 50 a Genova, e che fornisce servizi per la sicurezza digitale e fisica delle aziende. “Forse tutta questa attenzione è dovuta al **disservizio di Tim**, che però non ha niente a che fare con il ransomware”. Il 5 febbraio, domenica, sono state migliaia le segnalazioni di malfunzionamenti o assenza di segnale della rete Tim. «Un problema però dovuto a un incidente di servizio interno. I virus possono bloccare la contabilità, la gestione di un’azienda, non una rete telefonica”.

La concomitanza dei due eventi, il guasto di Tim e le bombe e grappolo del ransomware, ha creato il clamore. Per Luca Busi, amministratore delegato di una srl genovese, Gmg Net, che analizza l’esposizione agli attacchi cyber delle aziende sue clienti e sviluppa software per proteggerle, è comunque una buona notizia. “Forse servirà a fare maturare tante aziende che in questo caso, è evidente, hanno peccato di **negligenza**”. La falla nel Vmware era nota da due anni. Dal 23 febbraio 2021, sul servizio Vmware era disponibile un aggiornamento del sistema. **Sarebbe bastato quell’aggiornamento per non farsi colpire dal virus**.

Il professor Zunino, Rodolfo, paragona questo comportamento a quello del malato che compra le medicine per averle sullo scaffale. «Bisogna anche prenderle, se si vuole guarire», e dà un consiglio buono per tutti, aziende e privati cittadini: avere sempre un backup del computer, un disco esterno al pc collegato con cavo usb e su cui salvare i dati. «Molte aziende li salvano ogni dieci minuti, un privato può limitarsi a una volta al giorno. Attenzione però, **anche il backup è attaccabile**. Quindi prendete due precauzioni: quando fate il backup, aumentate le difese, alzate il profilo del vostro sistema di sicurezza; a backup finito, staccate la spina usb».