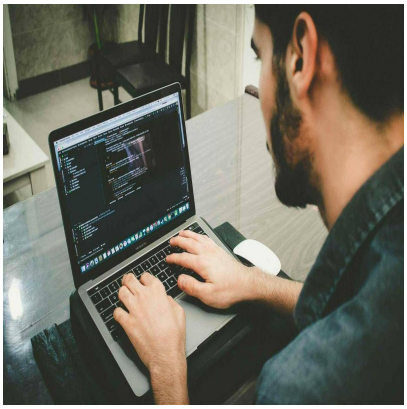

â??Ma quale software spiaâ??. Lâ??esperto smonta lâ??allarme sul ministero della Giustizia

Descrizione

(Adnkronos) â?? Non un â??Watergate digitaleâ??, ma lâ??ennesimo cortocircuito tra tecnologia, politica e percezione pubblica. Ã? questa la conclusione a cui arriva il docente ed esperto di cybersicurezza Matteo Flora, che nellâ??ultima puntata del suo video-podcast Ciao Internet analizza e smonta la polemica sul presunto â??software spiaâ??, installato nei computer del ministero della Giustizia.

Secondo la narrazione emersa dopo unâ??inchiesta di Report, il ministero disporrebbe di uno strumento capace di accedere ai computer dei magistrati senza lasciare traccia. Una ricostruzione che, secondo Flora, non regge a una verifica tecnica.

Il sistema al centro delle polemiche Ã¨ Microsoft Endpoint Configuration Manager (MECM), in precedenza noto come SCCM. Non un malware nÃ© un trojan, ma una piattaforma di gestione centralizzata degli endpoint, utilizzata da governi e grandi organizzazioni in tutto il mondo per aggiornamenti di sicurezza, distribuzione software, inventario e assistenza tecnica da remoto.

â??Gestire decine di migliaia di computer senza strumenti di questo tipo Ã¨ tecnicamente impossibile e pericolosoâ?•, spiega Flora. Nel caso della giustizia italiana si parla di circa 40.000 postazioni.

Uno dei punti piÃ¹ contestati Ã¨ lâ??idea che il sistema non lasci evidenze delle operazioni svolte. Al contrario, sottolinea Flora, MECM funziona su audit trail e log dettagliati, che registrano ogni intervento, soprattutto quelli che richiedono privilegi elevati. Cancellare sistematicamente queste tracce sarebbe, paradossalmente, molto piÃ¹ complesso che lasciarle.

Altro equivoco centrale: lâ??idea che â??qualsiasi tecnicoâ?• possa spiare un magistrato. In realtÃ , spiega Flora, lâ??accesso Ã¨ regolato dal principio del minimo privilegio, con ruoli separati, autorizzazioni limitate e controlli incrociati. I profili con poteri piÃ¹ estesi sono pochissimi e monitorati da strutture di sicurezza dedicate, come i Security Operations Center.

Il problema, semmai, non sarebbe la tecnologia, ma lâ??eventuale cattiva definizione dei processi e dei controlli umani. Â«Se câ??Ã¨ un abuso, Ã¨ un fallimento organizzativo, non una colpa del softwareÂ», osserva.

Câ??Ã¨ poi un elemento temporale che indebolisce la lettura politica del caso: il sistema Ã¨ stato adottato nel 2019, durante il governo Conte I, quando il ministero di Giustizia era guidato dal 5 Stelle Alfonso Bonafede. Un dato che, secondo Flora, rende poco credibile lâ??idea di un piano recente per il controllo della magistratura.

Il punto piÃ¹ delicato non Ã¨ tecnico, ma culturale. Flora richiama concetti come il â??chilling effectâ?• e lâ??â??agenda settingâ?•: anche unâ??accusa tecnicamente infondata puÃ² produrre un clima di intimidazione e sfiducia, incidendo sul comportamento delle istituzioni e sulla percezione della separazione dei poteri.

Il paradosso Ã¨ che uno strumento pensato per rafforzare la sicurezza finisce per diventare, nel dibattito pubblico, un simbolo di controllo e abuso. Con un risultato opposto a quello desiderato: piÃ¹ sospetto, meno resilienza.

Nel quadro piÃ¹ ampio, avverte Flora, demonizzare strumenti standard di gestione IT significa indebolire la sovranitÃ digitale dello Stato. Rinunciare a infrastrutture di sicurezza per paura della loro rappresentazione mediatica renderebbe la Pubblica Amministrazione piÃ¹ vulnerabile ad attacchi esterni e a interferenze ostili.

La conclusione Ã¨ netta: â??Il vero bug non Ã¨ nel codice, ma nel modo in cui raccontiamo e comprendiamo la tecnologiaâ?•. E senza un salto di qualitÃ nellâ??alfabetizzazione digitale di politica e media, il rischio Ã¨ restare intrappolati in un ciclo continuo di allarmi e smentite, mentre le minacce reali restano sullo sfondo.

â??

cronaca

webinfo@adnkronos.com (Web Info)

Categoria

1. Comunicati

Tag

1. Ultimora

Data di creazione
Gennaio 22, 2026
Autore
redazione