



Ma quale software spia? L'esperto smonta l'allarme sul ministero della Giustizia

Descrizione

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

Secondo la narrazione emersa dopo un'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 è Microsoft Endpoint Configuration Manager (MECM), in precedenza noto come SCCM. Non un malware né 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.

Gestire decine di migliaia di computer senza strumenti di questo tipo è tecnicamente impossibile e pericoloso, spiega Flora. Nel caso della giustizia italiana si parla di circa 40.000 postazioni.

Uno dei punti più contestati è l'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 più complesso che lasciarle.

Altro equivoco centrale: l'idea che qualsiasi tecnico possa spiare un magistrato. In realtà, spiega Flora, l'accesso è regolato dal principio del minimo privilegio, con ruoli separati, autorizzazioni limitate e controlli incrociati. I profili con poteri più estesi sono pochissimi e monitorati da strutture di sicurezza dedicate, come i Security Operations Center.

Il problema, semmai, non sarebbe la tecnologia, ma l'eventuale cattiva definizione dei processi e dei controlli umani. «Se c'è un abuso, è un fallimento organizzativo, non una colpa del software», osserva.

C'è poi un elemento temporale che indebolisce la lettura politica del caso: il sistema è 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 l'idea di un piano recente per il controllo della magistratura.

Il punto più delicato non è tecnico, ma culturale. Flora richiama concetti come il «chilling effect» e l'«agenda setting»: anche un'accusa tecnicamente infondata può produrre un clima di intimidazione e sfiducia, incidendo sul comportamento delle istituzioni e sulla percezione della separazione dei poteri.

Il paradosso è 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: più sospetto, meno resilienza.

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

La conclusione è netta: il vero bug non è nel codice, ma nel modo in cui raccontiamo e comprendiamo la tecnologia. E senza un salto di qualità nell'alfabetizzazione digitale di politica e media, il rischio è 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

default watermark