# Il cloud della Commissione Europea cade vittima del furto dei dati

A metà marzo, la **Commissione Europea** ha subito un'**infiltrazione malevola sui suoi servizi cloud.** A distanza di un paio di settimane, il Computer emergency response team (**CERT**) europeo ha offerto un resoconto del danno: almeno 42 apparecchi interni alla Commissione risultano potenzialmente compromessi, ma a essere colpiti sono anche altre **29 "enti dell'Unione"** che hanno fatto uso dei servizi di hosting offerti da "europa.eu" gestito da Amazon Web Services (**AWS**).

Martedì 24 marzo, il Cybersecurity Operations Centre (CSOC) della Comunità Europea nota delle attività sospette: le interfacce di programmazione di Amazon registrano un uso anomalo e, soprattutto, un **traffico dati fuori scala**. Il giorno seguente, vengono avvisate le autorità competenti. Secondo la ricostruzione offerta dal CERT, l'infiltrazione era ormai in atto dal 19 marzo ed è riconducibile a una serie di criticità concatenate. Il punto di partenza originale sarebbe riconducibile a **Trivy**, uno strumento open-source che, paradossalmente, è pensato per scansionare le vulnerabilità dei sistemi. Vittima di un precedente incidente informatico, l'azienda che gestisce lo strumento, Aqua, non sarebbe stata in grado di sistemare le falle pregresse, incappando in una compromissione che ha avuto effetti a cascata.

Essendo un sistema gratuito e utilizzabile da chiunque, Trivy è finito con l'essere **integrato in molti sistemi di cloud**, compresi quelli della Commissione Europea. Il gruppo responsabile della violazione, identificato con il nome TeamPCP, ha dunque verificato le credenziali di Amazon intercettate attraverso lo scanner infetto e, da lì, ha creato una nuova chiave di accesso, riuscendosi a infiltrare nei sistemi europei. Dopo aver violato il sistema cloud, gli hacker hanno **esfiltrato una mole di dati imprecisata** che è poi finita in vendita sul dark web sulla bacheca digitale del gruppo estorsivo ShinyHunters. Il materiale messo online corrisponde a circa 340 GB di contenuti e custodirebbe al suo interno **documenti confidenziali, contratti, email e altro "materiale sensibile"**.

Il CERT conferma che il maltolto includa la presenza di dati personali legati ai siti web della Commissione Europea e, potenzialmente, agli altri enti connessi al sistema. In tutto questo, sono **trapelati almeno 2,22 GB di email** di risposta automatica – quasi 52.000 file –, un fenomeno che ha quasi certamente esposto informazioni e dettagli privati di terzi. Chiunque abbia inviato una mail o un file alle caselle colpite in quei giorni, deve ipotizzare che le informazioni contenute nei loro messaggi siano ora in vendita sulla Rete. Le indagini per definire i danni effettivi dell'incidente informatico vanno avanti, tuttavia gli investigatori mettono in guardia: vista la mole dei dati rubati, ci vorrà tempo.

Gli accessi AWS compromessi sono stati nel frattempo bonificati e i programmatori hanno reintegrato una versione di Trivy che non dovrebbe essere afflitta da fatali vulnerabilità.

**Questa crisi non rappresenta però un caso isolato**: lo scorso gennaio, la Commissione aveva scoperto che la sua piattaforma di gestione degli apparecchi mobili era stata violata, quindi smartphone e tablet dello staff istituzionale sono rimasti virtualmente accessibili per la durata di nove ore. Le istituzioni sostengono che in quel lasso di tempo non si siano registrate fughe di dati.

In generale, questo genere di incidenti sembra essere destinato a consolidarsi e a ripetersi. Le filiere di approvvigionamento dei servizi digitali sono sempre più intricate e fanno affidamento su di una **catena infinita di subappaltatori**, attingendo frequentemente a strumenti open-source, i quali sono accessibili in via gratuita e possono essere impiegati liberamente, anche dalle grandi aziende, ma sono frequentemente soggetti a un grado di verifica inferiore alle soluzioni for-profit. Allo stesso tempo anche i servizi cloud, presentati spesso e volentieri come la soluzione definitiva per proteggere le reti istituzionali, continuano a dimostrarsi propensi al fallimento, evidenziando come il compromesso tra accessibilità e sicurezza sia valido solamente fino a un certo punto e che ancora oggi sia il caso di gestire i dati gravemente sensibili internamente, magari su server non direttamente accessibili da internet.


## Walter Ferri

Giornalista milanese, per *L'Indipendente* si occupa di analisi nel campo della tecnologia, dei diritti informatici, della privacy e dei nuovi media, indagando le implicazioni sociali ed etiche delle nuove tecnologie. È coautore e curatore del libro *Sopravvivere nell'era dell'Intelligenza Artificiale*.