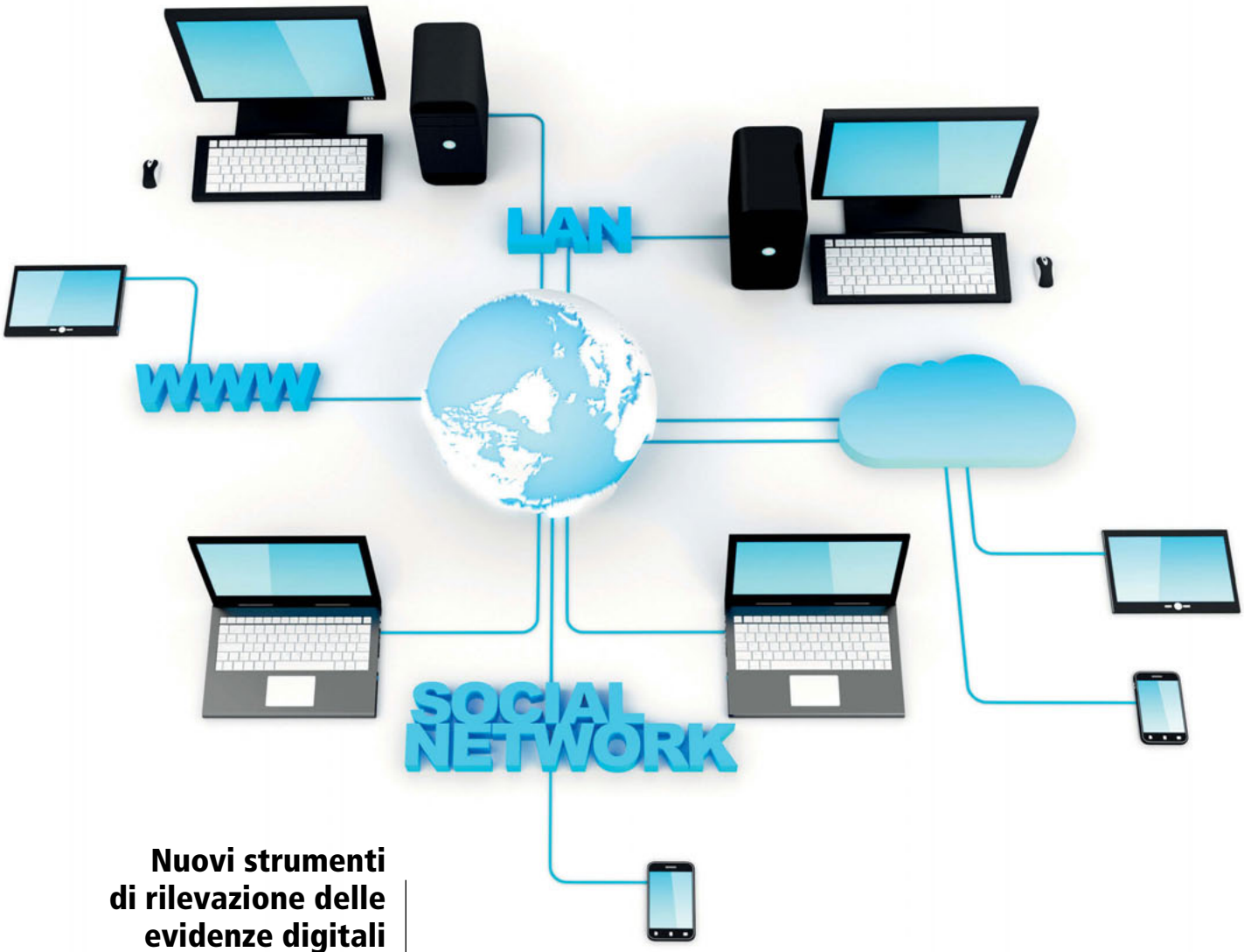

Nuovi strumenti di rilevazione delle evidenze digitali per i servizi di *Cloud*

CLOUD FORENSICS

L'evoluzione del mondo dell'informatica degli ultimi anni ha visto la nascita di un nuovo settore che, per taluni aspetti, può apparire in controtendenza rispetto al *trend* generale. La novità, infatti, è stata quella di introdurre dispositivi che non seguissero più l'idea di avere una potenza di calcolo o caratteristiche tecniche sempre maggiori a disposizione, bensì agevolare la portabilità e maneggevolezza, mediante l'introduzione di *smartphone* e *tablet*.

La diffusione degli *smartphone* e dei *tablet* ha anche avvalorato l'ipotesi che ciascun utente utilizzi, in media, più di un dispositivo e, pertanto, possa avere bisogno di accedere ai propri contenuti da ognuno di essi, facendo in modo che una modifica ad essi, indipendentemente da quale sia il dispositivo utilizzato per apportarla, sia immediatamente riflessa su tutti i restanti.

Questa tipologia di servizio rientra nel concetto di *cloud*, ovvero l'utilizzo di risorse che non sono fisicamente in possesso dell'utente, ma sono fornite da un soggetto terzo. Queste risorse possono includere, oltre allo spazio di archiviazione (come nei casi di *Google Drive, iCloud* o *Dropbox*), anche potenza computazionale (utilizzata dalle aziende per le proprie elaborazioni, come *AmazonWebServices*) o vere e proprie applicazioni da fruire *online* (ad esempio *Google Documents*). La necessità di sincronizzazione tra diversi dispositivi, unitamente alla facilità d'uso di questi servizi, li ha resi un tassello

fondamentale nell'utilizzo degli strumenti con i quali quotidianamente si lavora e si interagisce.

Dal punto di vista della *digital forensics* lo scenario descritto ha delle notevoli conseguenze. Ci si deve preparare, infatti, ad affrontare situazioni in cui le evidenze digitali utili all'attività investigativa possono essere archiviate anche su servizi di tipo *cloud*.

In aggiunta, per le realtà organizzate di dimensioni medio-grandi il *cloud* è una valida scelta per gestire in *outsourcing* tutta l'attività informatica aziendale, in quanto permette di realizzare delle importanti economie sui costi connessi ai sistemi informativi, e, pertanto, potrebbero essere del tutto assenti i dispositivi di archiviazione centralizzati con i contenuti dell'azienda medesima.

Durante l'esecuzione degli approfondimenti investigativi, il primo passo è cercare di individuare un possibile uso del *cloud* da parte di una persona o di un'impresa: tale attività potrebbe risultare complessa poiché richiede un'analisi delle attività effettuate sui dispositivi locali in uso (*client*) ovvero sui cd. *artifact* potenzialmente rinvenibili nei *browser* utilizzati per accedere alle risorse *cloud*.

Gli *artifact* possono essere costituiti, ad esempio, dai *cookie*, dalla cronologia del *browser*, da *file* temporanei o ancora da "*file* di servizio" (tipicamente nella forma di *database* autoconsistenti) e raccolgono importanti informazioni per capire non solo il tipo ma anche eventuali contenuti dei servizi *cloud* che vengono utilizzati.

Un tipo di utilizzo della tecnologia *cloud*, attribuibile ad uno scenario di livello *enterprise*, riguarda la virtualizzazione dei sistemi affidata a terzi ovvero gestita direttamente in *house* laddove, ad esempio, una complessa realtà aziendale può trarne enormi vantaggi in un'ottica di elevata versatilità e grado di accessibilità alle informazioni anche in mobilità a costi vantaggiosi.

In ambito investigativo riuscire a comprendere fin dalle prime fasi di un intervento se sono in uso tali servizi, potrebbe rappresentare la chiave di volta per lo sviluppo di approfondimenti proprio su materiale appositamente detenuto in questi spazi virtuali.

Si pensi alle procedure per poter attivare i consueti provvedimenti per richiedere la collaborazione del gestore del servizio di *cloud computing* ovvero individuare le figure professionali che hanno l'onere della gestione delle piattaforme virtualizzate (responsabile dei sistemi informativi, amministratori di rete, ecc.) che possono "collaborare" nel corso di un'operazione di polizia. Tendenzialmente la fase di acquisizione delle evidenze digitali è rimessa alla collaborazione dei *provider* che gestiscono il servizio.

L'importanza della *Cloud Forensics* quale scenario meno esplorato della *Digital Forensics* impone ad una moderna Forza di polizia, come il Corpo della Guardia di Finanza, un approccio scientifico e metodologico ai temi connessi alle investigazioni informatiche, oggi più che in altri tempi, utili – per non dire necessarie – ai più svariati comparti e settori di servizio in cui quotidianamente ci si trova ad operare.

Gli investimenti effettuati nella formazione di personale qualificato e in dotazioni tecnologiche all'avanguardia rappresentano un imprescindibile connubio per poter affermare nuove valide metodologie da applicare all'attività di servizio. ■