Confermare la password tramite SMS? Non è sicuro

Date : 5 settembre 2016

Uno dei metodi più usati per controllare che chi sta eseguendo l'accesso è effettivamente autorizzato a farlo è la 2FA: SMS-based Two-Factor Authentication. Il sistema invia un messaggio contenente un codice direttamente sul cellulare dell'utente. Il National Institute for Standards and Technology mette tutti in guardia sull'efficacia di questo metodo.

I più cauti lo sanno: le password sono una misura di sicurezza piuttosto debole, soprattutto se scelte senza attenzione. La soluzione può sembrare semplice, basta usare più di una chiave. Molti siti lo fanno attraverso la verifica in due passaggi -o due fasi, la SMS-based Two-Factor Authentication, 2FA- la quale, oltre a chiedere la password, invia un codice sul cellulare dichiarato dal fruitore. Se ad esempio disponete di un account G-mail potete attivare la 2FA, questa invierà un codice di sei cifre al vostro cellulare al fine di verificare che siate proprio voi ad effettuare l'accesso.

Ma siamo sicuri che questo sia un sistema sicuro come sembra?

Seppur più affidabile della sola password, neanche questo metodo sembra essere soddisfacente.

Nell'ultima bozza dell'Authentication Digital Guideline emessa dall'americano NIST - National Institute for Standards and Technology - si legge che la 2FA andrebbe scoraggiata perchè non abbastanza sicura per sistemi delicati come ad esempio quelli bancari.

Mostrando quanto sia elevato il rischio che gli SMS vengano intercettati o reindirizzati il NIST incoraggia e invita qualsiasi servizio che si avvalga della 2FA a prendere in considerazione autenticatori alternativi.

Nel documento rilasciato il NIST afferma che i siti dovrebbero innanzitutto attivare un sistema che verifichi se il numero cui invia il codice appartiene ad una rete legittima e non ad un servizio VoIP - Voice over IP, ovvero un'innovativa tecnologia che permette alle informazioni vocali di viaggiare attraverso una qualunque rete basata su un protocollo IP.

Quest'ultima risulta non solo molto vulnerabile per chi ne fruisce legittimamente ma anche sospetta perchè spesso utilizzata dagli stessi hacker.

Nel mese di marzo la banca inglese NatWest ha ammesso il bisogno urgente di un nuovo sistema bancario online, si sarebbero infatti verificati dei casi in cui il loro sistema di verifica in due fasi non ha funzionato. I conti di alcuni clienti sono stati svuotati, i criminali hanno dirottato la scheda SIM del telefono dei clienti facendo credere ai loro operatori di telefonia mobile che la vittima di frode volesse attivare una nuova scheda.

Non è questo l'unico modo in cui la 2FA può fallire, il telefono potrebbe venire semplicemente rubato o il messaggio potrebbe essere intercettato da terzi.

Non c'è modo in cui lo strumento di verifica possa effettivamente accertarsi che il codice sia stato letto solo da chi dovrebbe e la truffa sembra davvero troppo facile da attuare.

Cosa propone il NIST?

La biometrica sembra essere la soluzione del futuro, i più recenti dispositivi mobili hanno infatti sensori in grado di rilevare le impronte digitali.

Come detto però questa risulta ancora essere una soluzione del futuro, lo stesso NIST dichiara che anche i più moderni test biometrici possono generare falsi positivi e falsi negativi, non sono poi ancora tanto sofisticati da evitare che i criminali riescano a falsificare le impronte digitali o il riconoscimento facciale utilizzando stampe da oggetti toccati dalla vittima o prendendo foto ad alta risoluzione del volto della stessa.