Open Authorization (OAuth) e Social Network

È veloce. È facile. È sicura? Ma soprattutto cosa è?

Pochi sanno di cosa si tratta veramente, eppure viene utilizzata tutti i giorni da milioni di utenti al fine di accedere a siti Web o servizi con account di terzi parti forniti da Facebook, Google, Microsoft, Twitter, Linkedin e altri.

Sempre più spesso, infatti, all'atto di accedere a un nuovo sito o un nuovo servizio, oltre alla classica form per la creazione di un account, si ha la possibilità di registrarsi automaticamente mediante appositi pulsanti quali "Login con Facebook", "Login con Google ", etc. e la tendenza dei gestori per il futuro è proprio quella di non dare più nemmeno la possibilità di accedere utilizzando l'indirizzo e-mail o creando un account specifico.

Ma cosa succede quando ci registriamo ad esempio su un sito utilizzando questi account ? Quali sono i rischi, quali sono i vantaggi? Facciamo luce su questi due ultimi aspetti.

Normalmente la procedura di registrazione consiste nel creare un nuovo username e una password fornendo un indirizzo e-mail a cui il sito invierà una mail di conferma (con le consuete problematiche) contenente generalmente, oltre al benvenuto, un link di autenticazione che serve ai gestori del sito o del servizio per accertarsi che dietro la procedura di registrazione ci sia una persona vera e non qualche tipo di bot.

Utilizzando invece un account di terzi per eseguire la registrazione, è possibile evitare tutto ciò, poiché sarà uno di questi servizi che garantirà l'identità al sito e gestirà l'account mediante **OAuth**, un protocollo di rete aperto e standard, progettato specificamente per consentire all'utente di condividere informazioni circa il proprio account con altre applicazioni o siti Web senza fornire loro alcuna password, ma utilizzando token revocabili.

L'utente però, dopo un primo momento di *gaudium magnum* per non doversi ricordare l'ennesima coppia username e password, spesso subito dopo aver **accettato le condizioni** (generalmente ignorate), viene colto da dubbi su quello che sta facendo: sarà sicuro? i miei dati dove vanno? chi ci guadagna da ciò? e soprattutto dove è "il tranello"? Perché ovviamente un "tranello" esiste.

Come dissipiamo questi dubbi allora? L'indicazione dell'imperatore filosofo Marco Aurelio è più che mai attuale: "di ogni singola cosa chiedi cos'è in sé, qual è la sua natura"

Il "tranello". Stiamo interagendo con realtà che vivono di informazioni: nel migliore dei casi, il servizio a cui ci si sta registrando avrà accesso al nostro profilo pubblico, all' indirizzo e-mail e utilizzerà tali informazioni per azioni quali marketing, profilazione o statistiche che poi possono essere rivendute (generando profitto). È anche possibile che il gestore del servizio o sito cui si accede con credenziali di terzi possa spingersi oltre: potrebbe accedere all'elenco dei contatti o riuscire a pubblicare qualcosa a nome dell'utente, anche se per contratto i gestori dei social dovrebbero garantire un certo controllo su cosa può essere condiviso.

Ma è sicuro? Per deciderlo possiamo formulare una prima considerazione: l**a password non viene mai fornita al portale su cui ci si sta registrando**, quindi, nel caso in cui il sito venisse violato, non ci sarà nessun account e nessuna informazione personale da rubare e quando si decide di non usufruire più del servizio o del sito è

possibile revocare il token per rimuovere l'accesso ai dati da parte del sito. In secondo luogo occorre considerare che, con la procedura descritta, si **fa affidamento sulla sicurezza di colossi informatici (i citati Facebook o Google ad esempio) che hanno** ingenti risorse da investire per proteggersi, a differenza probabilmente del fornitore del servizio a cui ci si sta iscrivendo. Infine, è possibile utilizzare l'autenticazione a due fattori, il che aumenta considerevolmente la sicurezza. Con **OAuth** è possibile quindi focalizzare l'attenzione sulla creazione di una password che non risulti vulnerabile e che sarà anche l'unica password da ricordare, poiché più password da gestire, più aumenta la vulnerabilità.

In conclusione, se si imposta una password sicura e l'autenticazione a due fattori per l'account di terze parti, l'accesso risulterà più sicuro della maggior parte delle alternative disponibili ,a patto di rinunciare ad un pezzo della nostra privacy.

Di Ing. Vincenzo Singuaroli

CCO/DPO presso Planetel S.p.A. - Delegato della Comm. ICT al C3I e al Cdr Ordine Ingegneri di Bergamo – Certificato Certing Sicurezza Informatica e Protezione dei Dat