

## **Configurare i requisiti minimi di sicurezza con un Macintosh**

di Giorgio Ginelli

Fin dagli albori della storia dell'informatica, la sicurezza, per Apple, ha rappresentato un riferimento importante, in quanto il Macintosh come piattaforma nasce negli anni ottanta con già i requisiti di sicurezza ottimali per il collegamento con altri computer.

Fin dalla versione 7 del sistema operativo, l'utilizzo di un Macintosh è regolato da un regime di password che possono essere di differenti generi: per la protezione del disco rigido oppure per l'accesso remoto, che può essere a sua volta di tre tipi diversi: per il collegamento a un server remote access, per il collegamento a un altro computer come utente registrato oppure come proprietario.

Ma lavorare in sicurezza non vuol dire solo digitare delle password, e Apple in questo senso ha da sempre dotato i propri sistemi operativi di tutti gli strumenti adeguati per lavorare con tranquillità.

Alla base di tutto il sistema di connettività di Apple si è sempre situato il protocollo AppleTalk, che racchiude tutte le procedure necessarie per collegare in rete due computer oppure collegarlo a un dispositivo esterno; per un Macintosh avere i requisiti di sicurezza è perciò indispensabile, sia si tratti di collegarsi alla rete, che a una semplice stampante, in quanto è parte della normale modalità di funzionamento. Resta solo da stabilire livelli differenti di sicurezza, a seconda del genere di collegamento, anche se comunque tutto è basato sui privilegi attribuiti da una password anziché un'altra.

La differenza, comunque, fra il concetto di sicurezza in ambito di rete intranet oppure ethernet è molto sfumato sui computer di Apple. Sicurezza, per coloro che hanno progettato i vari sistemi operativi di casa Cupertino, è sinonimo di differenti termini, tutti egualmente importanti: riservatezza, condivisione, collegamento, risorse, gruppi, utenti, ospiti.

Viene fatta salva, comunque, una condizione generale: a chiunque utilizzi un Macintosh viene concesso o meno di impostare operazioni in funzione dei privilegi che possiede come utilizzatore.

L'evoluzione del sistema operativo di Apple, ha determinato nel tempo anche sostanziali cambiamenti nella gestione delle connessioni e dunque nella sicurezza, mantenendone però sempre molto alti i requisiti minimi.

### **MacOs 8.6**

La sicurezza con le vecchie versioni del sistema operativo che rappresentano però ancora un target significativo per il numero di utilizzatori, è racchiusa principalmente nel pannello Condivisione documenti, che consente anzitutto al computer di essere identificato sulla rete. Viene assegnata una password e un nome identificativo del computer, che assieme al nome del proprietario dovrà essere digitato ad ogni connessione. Sempre dallo stesso pannello potrà poi essere attivata la condivisione dei documenti, necessaria affinché gli utenti della rete possano condividere il contenuto.

Ogni connessione remota prevede che il computer sia identificato attraverso la password idonea, in caso contrario la connessione potrà avvenire solo in qualità di ospite al quale sono vietate praticamente la maggior parte dei privilegi utili.

La connessione vera e propria è invece stabilita attraverso il pannello AppleTalk, che definisce il protocollo utilizzato e la tipologia fisica di connessione. Con i controlli AppleTalk, Internet. Modem, Remote Access e Tcp/Ip, utilizzati per configurare le connessioni, è possibile lavorare in tre diverse modalità utente.

- Base (modalità standard): è possibile regolare solo le impostazioni principali.
  - Avanzata: è possibile modificare ulteriori impostazioni.
  - Amministratore: viene utilizzata una password per proteggere le impostazioni di gruppo.
- L'ottimale utilizzo del Macintosh in termini di sicurezza, si basa anche sull'uso dei Gruppi di

impostazioni (postazioni). Si possono creare differenti impostazioni del software di sistema che soddisfano diversi modi di lavoro. Ad esempio, si possono creare gruppi di impostazioni per differenti luoghi nei quali si utilizza il computer, oppure, per ogni tipo di connessione di rete che viene utilizzato (Tcp/Ip, Ppp e AppleTalk). Altra situazione tipica nella quale sono creati gruppi di lavoro è la condivisione del computer fra differenti utilizzatori; in questo caso le impostazioni di ogni singolo utente sono create come gruppi separati.

Gli utenti collegati poi, sono gestiti dal pannello Utenti & Gruppi, che consente di impostare i parametri di condivisione degli elementi presenti nel computer, presi con interi volumi o come singoli file.

### **MacOs 9.x**

Con la versione 9 di MacOS, diviene importante anche il nuovo pannello Multiutenza, che normalmente è disattivato. Questo pannello di controllo permette di assegnare una parola d'ordine e una serie di privilegi a ciascun utente di uno stesso Macintosh. Sono definite quattro classi di utenti (la prima e quella dell'amministratore, che ha pieni poteri su tutto) e ciascun utente usa preferenze personali; ad esempio la scrivania di ciascun utente è differente, contiene documenti diversi ed ha uno sfondo proprio.

Agli utenti normali è semplicemente impedita la modifica della configurazione di basso livello del sistema; non possono operare in pratica attraverso i pannelli di controllo Memoria, TCP/IP e Remote Access. Per questa categoria è però possibile lasciare i documenti in una cartella che ha il loro nome e che viene automaticamente creata.

Agli utenti limitati può essere ristretto l'uso di alcune applicazioni, alcuni documenti, alcuni dischi (compresi i rimovibili, i CD e i DVD); è possibile negare a questi utenti l'accesso ad alcuni elementi del menu Apple, a Scelta Risorse o alle stampanti.

L'ultimo profilo è quello degli utenti a pannelli, che sono tipicamente i bambini oppure i principianti assoluti; non hanno l'uso del Finder e sul loro schermo appaiono semplicemente le icone degli elementi che possono utilizzare.

Un tipo di gestione della sicurezza che senz'altro segna un passo in avanti e che fa da apripista alle procedure di sicurezza inserite nella versione definitiva del sistema operativo degli Apple della nuova generazione.

### **MacOs X**

Mac OS X garantisce i più alti livelli di protezione grazie allo sviluppo software open source e all'adozione di standard precisi. Il cuore open source di MacOS X si chiama Darwin e offre Kerberos, Secure Shell (OpenSSH), un framework per transazioni sicure via Internet (OpenSSL) e la protezione dei documenti con permessi UNIX in stile BSD. Darwin presenta un'architettura a memoria protetta che assegna uno spazio unico a ciascuna applicazione, consentendo in questo modo un uso continuo del computer, senza che il malfunzionamento di un'applicazione vada a bloccare l'intero sistema.

Il fulcro del sistema di sicurezza è il Portachiavi, che diviene una vera e propria centrale di controllo. Nato con la versione 9 del MacOS, la sua funzione era semplicemente quella di tenere traccia delle password delle utenze registrate su un computer. Con la versione MacOS X, il portachiavi è creato alla prima configurazione del sistema, può essere poi modificato e aggiornato costantemente e viene attivato al momento del login, quando si digita la password dell'utente.

Fondamentalmente la sua funzione è comunque quella di gestire le decine di password e permessi tipici di un utilizzo on-line del computer; in effetti il Portachiavi archivia tutte le informazioni necessarie per accedere a server file, ftp e web, oltre a utilizzare immagini disco criptate. Per sicurezza, infatti, è possibile con MacOS X criptare parte del disco rigido

utilizzando un'immagine disco per inviarla ad altri utenti in possesso della password. Un disco criptato compare sulla scrivania come un volume, ma l'utilizzo del contenuto è possibile solo sbloccando il Portachiavi con la password adeguata.

È possibile creare portachiavi diversi per conservare password che possono servire a diversi scopi, ad esempio per il lavoro e per lo shopping su Internet; oppure è possibile fare una copia di un portachiavi in modo da poterlo portare su altri computer.

La trasparenza è comunque l'elemento caratteristico della sicurezza in ambito Macintosh; vale a dire che le operazioni necessarie affinché si operi con gli adeguati criteri non è mai visto dall'utente come un'elaborata ed intricata serie di operazioni da condurre in porto.

## **DIDASCALIE**

UTE\_GRU.tif - Utenti & Gruppi consente di impostare tutti i parametri di condivisione degli elementi presenti nel computer.

APPLETALK.tif - Fino alla versione MacOS 9.x, il pannello AppleTalk decretava l'avvio di qualsiasi tipo di connessione.

GEST\_POST.tif - A seconda dei differenti modi di utilizzo del computer possono essere impostate delle postazioni di lavoro personalizzate.

MOD\_UTENTE.tif - È possibile selezionare una differente modalità utente dalla maggior parte dei controlli che prevedono una connessione remota.

COND\_DOC.tif - Il pannello Condivisione Documenti è la centrale di controllo che consente a un Macintosh di essere identificato sulla rete e di condividere documenti.

INFO.tif - Attraverso il comando Informazioni è possibile gestire la condivisione di diversi elementi, dal disco rigido al singolo file.

KEY9.tif - Il Portachiavi fa la sua comparsa con la versione 9 del MacOS.

MULTI.tif - Il pannello Multiutente amministra le differenti utenti di un computer, consentendo l'abilitazione di questa modalità.

NEW\_UTE.tif - Con il MacOS 9, la gestione della multiutenza si basa su tre tipi di accesso che hanno differenti privilegi.

CRIPTA.tif - Il massimo della sicurezza è rappresentato dalla criptatura di volumi o di interi dischi, che necessitano poi di essere sbloccati dal Portachiavi per poterne utilizzare il contenuto.

KEY10.tif - Dal Portachiavi di MacOS X è possibile gestire gli attributi degli elementi inseriti al suo interno, definendo un completo controllo dell'accesso.

ACCESSO.tif - Qualsiasi elemento inserito nel portachiavi per poter essere utilizzato o letto, ha bisogno di un'adeguata password.

SPLASH.tif - L'avvio di MacOS X prevede una fase di login nella quale si digita la password corrispondente all'utente che a sua volta abilita il contenuto del Portachiavi.