SOFTWARE SPECIFICO
PER LE ASSOCIAZIONI DI
PUBBLICA ASSISTENZA

S A L I X

GUIDA OPERATIVA

SICUREZZA E PROTEZIONE DEI DATI

Salix Alba – Salice Bianco

Emilio Panozzo

Aggiornamento: 20-05-2018, 03-06-2018

Questa guida descrive come funziona il sistema di sicurezza e protezione dei dati nell'applicativo Salix e come poterlo personalizzare in modo che risponda alle esigenze legali e gestionali dell'associazione.

Il sistema di accesso ai dati di Salix è fortemente personalizzabile, permette infatti di:

- generare password anche con scadenza per ciascun operatore;
- rendere invisibili intere parti di programma nascondendo le corrispondenti voci nel menù;
- rendere invisibili parti dei pannelli di lavoro;
- rendere non modificabili parte dei campi di lavoro dell'interfaccia;
- disabilitare l'uso di pulsanti e panelli di lavoro.

Questa personalizzazione operativa viene associata all'utente, o meglio al suo ruolo, in modo che ciascun operatore/ruolo abbia l'opportunità di vedere soltanto ciò che è di sua competenza e che è stato autorizzato a trattare.

Dato che Salix è una applicazione Client/Server anche il sistema di protezione e sicurezza è anch'esso basato su questa struttura.

Nel seguito viene descritto il sistema di protezione a livello client, a livello server e come personalizzare la struttura di sicurezza.

Nomenclatura

Amministratore del Sistema

E' il tecnico che si occupa del funzionamento dell'impianto informatico dell'Associazione e che cura tutti gli aspetti relativi all'hardware, al software e alla sicurezza informatica.

Amministratore Locale di Salix

E' il referente e responsabile del buon funzionamento di Salix all'interno dell'Associazione, ci si rivolgerà a lui per qualsiasi situazione anomala prima di - o comunque anche se si dovrà - contattare l'assistenza di Salix. Gestisce le password e la personalizzazione di Salix.

Tecnico di Salix

E' il tecnico che effettua interventi sul sistema Salix (e non può occuparsi di questioni che riguardano il sistema, le stampanti, la rete locale, internet, ecc..) in locale o in remoto per aggiornamento, formazione operativa, assistenza operativa o personalizzazione specifica di parti di programma.

Utente (di Salix)

E' l'operatore di terminale che svolge i compiti assegnatigli attraverso un regolare accesso al sistema informatico, l'accesso normalmente avverrà in due passi: il primo è l'accesso al computer e alla rete con le credenziali assegnate dall'Amministratore di Sistema, il secondo è l'acceso a Salix con le credenziali fornite dall'Amministratore Locale di Salix, tramite il cuale si attiva il Profilo Operativo specifico per il ruolo assegnato.

1. Livello Client

a. Al momento dell'installazione viene identificato almeno un utente con funzioni privilegiate nell'ambito della sicurezza e protezione dei dati registrati in Salix, nominato nel seguito Amministratore Locale di Salix.

b. L'Amministratore Locale di Salix può accedere a tutte le aree del sistema Salix ad eccezione delle cartelle crittate con password, ci si riferisce alla sezione dei dati sanitari. Per l'Amministratore Locale di Salix non sono richieste particolari conoscenza informatiche e sistemistiche, quindi non è necessario che sia l'Amministratore del Sistema; è invece opportuno che esso conosca il funzionamento della propria organizzazione, le procedure operative, le figure professionali e le persone che le mettono in atto.

c. L'Amministratore Locale di Salix, inizialmente insieme al Tecnico di Salix e successivamente in modo autonomo, individua il necessario numero di "Profili Operativi" uno per ciascun ruolo utile nella gestione delle procedure e assegna a ciascun Profilo Operativo creato le voci di menù utilizzabili, i pannelli utilizzabili e quelli in sola lettura (e di conseguenza quelli nascosti), le opzioni, le abilitazioni ai pulsanti di azione e agli accessi ai dati.

d. L'amministratore Locale di Salix assegna, in accordo con la il resto della struttura associativa che utilizza Salix, la combinazione sigla utente / password e Profilo Operativo per ciascun utente di Salix.

e. L'Amministratore Locale di Salix provvede a comunicare agli operatori l'account assegnato istruendo circa le modalità di cambiamento della password al primo utilizzo e alla scadenza programmata.

f. Ciascun Utente che accede a Salix, per prima cosa, declina l'account di accesso costituito dalla propria personale sigla utente e della propria password.

g. L'Utente provvederà, come disposto, a modificare la propria password quando il sistema ne chiede la modifica per raggiunta scadenza (o primo impianto).

h. L'Utente utilizzerà Salix nelle funzioni messe a disposizione dal Profilo Operativo a lui associato, Salix non permette l'accesso ad aree dell'interfaccia utente che non siano previste nel profilo, nella maggior parte dei casi tali aree sono completamente nascoste.

2. Livello server

a. I dati sono conservati in un unico file di database relazionale strutturato secondo le specifiche del motore di database open-source Firebird nella versione 2.1.7. I dati registrati nel file non sono riconoscibili attraverso i software di elaborazione di testi, tuttavia il database stesso non è crittato.

b. Salix è rilasciato per questa versione del database, l'installazione di versioni successive da parte dei sistemisti è possibile, sappiamo che funziona, ma non abbiamo effettuato prove complete di compatibilità nel nostro laboratorio di sviluppo.

c. Il file è registrato nel disco del server in una apposita cartella ad esso destinata e ospitata sul disco principale. I sistemisti degli impianti possono decidere per una diversa collocazione in funzione delle loro politiche organizzative e di sicurezza.

d. E' cura del proprietario dei dati effettuare copie di sicurezza del database e conservarle in luogo sicuro e protetto.

e. E' cura del proprietario dei dati assicurare che il server sia fisicamente e logicamente sicuro e protetto.

f. L'accesso al file di database avviene esclusivamente tramite una sola istanza del motore di database Firebird che nei file di configurazione conserva la posizione fisica del database.

g. Il database è proiettato sulla rete locale attraverso il protocollo Firebird che risponde sulla porta programmata durante la configurazione iniziale del sistema.

h. Il protocollo Firebird è un protocollo open-source per il quale sono disponibili in Rete utility e DLL di collegamento.

i. Il collegamento ai dati, tramite il motore di database, è protetto da combinazione utente/password, la password è creata in fase di installazione del motore.

j. La combinazione utente/password necessaria per accedere al database è sconosciuta e tenuta nascosta agli utilizzatori di Salix; è disponibile all'Amministratore di Sistema e conservata secondo le procedure di sicurezza da lui adottate.

k. Ciascun client che accede al database tramite l'apposita porta definita in configurazione deve declinare la combinazione utente/password stabilita, che - come già detto - è conservata crittata nei sistemi e non è conosciuta dagli utenti, essa viene trattata automaticamente dai moduli software.

l. L'accesso al motore di database e tramite esso ai dati conservati non è quindi possibile senza la convenuta combinazione utente/password definita in configurazione e modificabile secondo necessità.

3. Personalizzazione

Il livello di sicurezza in Salix è personalizzabile, tuttavia non si può prescindere da:

- Assegnare una password personale a ciascun utente
- Creare Profili Operativi a cui associare gli utenti
- Creare una combinazione utente/password di accesso al motore di database
- Aprire la porta di accesso al servizio Firebird sul server

Salix non è dal suo interno protetto contro virus informatici e, benché sia sicuro e collaudato, non è stato progettato per resistere a tentativi di hakeraggio o di manomissione sull'hardware, quindi il sistema dovrà essere dotato di software specifico contro i virus informatici e accessi fraudolenti, il server dovrà essere fisicamente protetto sia verso danneggiamenti e furti sia verso scariche elettriche o altre manifestazioni atmosferiche pericolose e infine bisogna fare copie di sicurezza con frequenza almeno giornaliera e conservare queste copie, insieme alle corrispondenti password, in luogo sicuro e protetto.

Gli account di tutti gli utenti di Salix sono memorizzati nel database, il nome utente è in chiaro, la password è crittata e non è possibile risalire a una password assegnata. In caso di perdita della password un operatore dovrà rivolgersi all'Amministratore Locale di Salix per farsene assegnare una nuova. Se l'Amministratore Locale di Salix perde l'accesso dovrà rivolgersi al Tecnico di Salix per il ripristino. Se l'Amministratore di Sistema perde la password del database tutto il sistema dovrà essere riconfigurato - oppure reinstallato - con interruzione di servizio per il recupero dei dati dalle copie di back-up (ammesso che le password di accesso a tali copie siano disponibili).

Da ciò si comprende l'estrema importanza di conservare con cura oltre che i back-up anche le corrispondenti password.

Non esiste possibilità alcuna di estrarre l'elenco in chiaro delle password degli Utenti di Salix.

Può essere personalizzato il periodo di validità delle password in mesi, 1, 2, 3 eccetera, la scadenza delle password può essere disabilitata impostando 0 come numero di mesi di scadenza, l'accesso a questa personalizzazione è riservato all'Amministratore Locale di Salix.

Salix è dotato di un timer di inattività che chiude automaticamente qualsiasi sessione di lavoro avviata da un utente dopo il periodo di inattività prestabilito, questo meccanismo previene dall'uso non autorizzato del sistema in caso di abbandono urgente della postazione da parte dell'operatore.