Overview dell’applicazione e planning dei cambiamenti

Overview

Greenhouse è il progetto per un sistema di controllo e gestione di una serra di grandi dimensioni che viene utilizzato dai dipendenti per la visualizzazione della distribuzione delle colture, la gestione dell’impianto idrico e la regolazione dei parametri ambientali fondamentali per la corretta crescita delle piante, quali l’umidità, la temperatura e l’irradianza.

La serra è composta da più sezioni, ovvero dei capannoni fisicamente separati, e all’interno di ogni sezione sono presenti varie aree coltivate, disposte per file. Ogni area coltivata assume una determinata posizione numerata all’interno della fila ed è descritta da una estensione in mq e un tipo di terreno che indica quali sono le coltivazioni che si possono piantare. In ciascuna area coltivata può essere piantata una determinata coltivazione per la quale è importante conoscere lo stato di avanzamento della lavorazione, la data della prossima operazione, il tipo di coltivazione e una descrizione. Infine, il software deve includere un meccanismo per notificare gli addetti ad una determinata coltivazione, in modo da ricevere in tempo reale aggiornamenti sullo stato di lavorazione o avvisi importanti.

Modifiche

Focalizziamoci per adesso sulla parte di gestione. Precedentemente un software monolitico a layer ha la necessità di diventare una web app per questioni di espansione del business, deve permettere quindi di accedere ai servizi da remoto.

Con la migrazione si pongono però numerosi problemi di sicurezza, ragion per cui dobbiamo prevedere contromisure per rendere l’applicazione sicura.

Identification and authentication

-Dobbiamo mettere in sicurezza l’accesso al server, la precedente operazione di autenticazione, che era una semplice login con dati salvati sul DB ora va gestita in maniera più sicura e va reingegnerizzata per modificabilità. Il requisito prevede l’utilizzo di uno strumento esterno, Keycloack, per rendere l’autenticazione più sicura, flessibile e modificabile. Prevediamo metodi avanzati di autenticazione come OTP per ruoli critici come il direttore della serra, l’agronomo e l'amministratore software e l’amministratore della sicurezza, oltre alla standard login con password basata su username o mail personali.

Una volta eseguito l’accesso il token fornito serve per identificare il client nelle successive interazioni col web server.

1. Una sessione di login non deve durare più di 5 ore. Un token deve essere valido per al massimo 5 minuti previo refresh. Una sessione in idle viene fatta cadere dopo 30 minuti.
2. L’OTP è di 6 cifre basato sul timestamp attraverso l’applicazione FREE OTP. Hashing sha-256 e finestra di 1 minuto (30 di validità +30 lookahead).
3. Per i fallimenti di login deve essere presente un lock temporaneo per 15 minuti degli account dopo 30 tentativi di login falliti in 12 ore tramite Keycloak. Lo stesso deve essere fatto sui SO sottostanti.

Inoltre, la connessione tra front end e back end deve essere protetta (i.e. SSL/HTTPS) per evitare attacchi al canale di comunicazione.

- Il database deve autenticare il web server con ID, password e in base all’IP, e deve riconoscere il richiedente in base al suo certificato in modo da autenticare solo il server per l’accesso ai dati (e all’amministratore di sistema con account dedicato).

- Le policy dell’organizzazione devono essere messe in sicurezza, quindi il database su cui vengono salvate deve essere separato dall’altro e deve garantire una forma di identificazione e autenticazione per l’accesso da parte solo del server keycloak come l’altro database.

-Le macchine utilizzate all’interno della rete aziendale devono essere protette anche a livello di SO con identificazione e autenticazione tramite password.

-Le password devono essere di almeno 8 caratteri, con 1 uppercase, 1 carattere speciale, non possono essere uguali all’username, non possono essere usate le tre più recenti. La password scade dopo 182 giorni. Deve essere salvata in maniera cifrata. I dispositivi OTP possono essere cancellati e rifatti in caso di smarrimento.

-La connessione al broker MQTT deve anche essere regolata da una login con username e password

Authorization

-Dobbiamo prevedere forme di autorizzazione avanzate e modificabili, mentre finora erano embedded nell’interfaccia grafica. Anche per questo punto è richiesto l’utilizzo delle potenzialità di Keycloack.

I ruoli previsti nell’azienda sono: i contadini, gli agronomi, il direttore e il responsabile software

Ribadiamo le policy che l’azienda ci richiede:

-Solo gli agronomi possono modificare i parametri ambientali target delle coltivazioni delle sezioni a cui afferiscono. Inoltre possono visualizzare le coltivazioni delle altre sezioni. Eventualmente possono dare l’autorizzazione ad un altro agronomo di modificare una coltivazione della propria sezione.

-I contadini possono visualizzare le coltivazioni della propria sezione. In particolare, possono visualizzare una lista di coltivazioni nella sezione o i dettagli relativi a una specifica coltivazione. Un agronomo può affidargli il compito di modificare temporaneamente (fino a quando non decide di revocarlo esplicitamente) una coltivazione della propria sezione. Un agronomo di un’altra sezione può dargli il permesso di visualizzare una coltivazione della propria sezione, volendo temporaneamente (fino a quando non decide di revocarlo esplicitamente).

-L’amministratore della sicurezza è l’unico che deve poter gestire gli utenti (aggiungere, rimuovere, modificare),

-L’amministratore software è l’unico in grado di avviare il sistema e decifrare i file di configurazione. Inoltre, può modificare i file di configurazione della serra previa autorizzazione del direttore (i.e. modificare il file XML di configurazione del software)

(Only policy implemented) -Gli agronomi possono gestire le coltivazioni della sezione a cui afferiscono (aggiungere, modificare, rimuovere). Per aggiungere l’URI è [https://.../sezione/{idsez}/coltivazioni](https://sezione/%7Bidsez%7D/coltivazioni) con metodo PUT

(Only policy implemented) -Il direttore può gestire le coltivazioni di tutte le sezioni (operazioni CRUD)

(not implemented yet) -Il direttore deve essere l’unico a poter gestire le aree di coltivazione (aggiungere, modificare, rimuovere)

(Only policy implemented) -Il direttore deve essere l’unico a poter gestire le sezioni (creare, modificare ed eliminare, se la sezione è non vuota il direttore riceve un warning).

Inoltre, va gestita la transizione dei ruoli (i.e. un agronomo diventa direttore), o un cambiamento di afferenza alla sezione di un agronomo o un contadino.

-Bisogna mettere in sicurezza i file di configurazione XML del software per escludere modifiche o accessi non autorizzati. Quindi il file va settato con i permessi corretti e va cifrato.

-Deve esistere una pagina ad accesso pubblico senza necessità di autenticazione o identificazione che faccia da home page pubblicitaria per il sito.

Comunicazione

-Dobbiamo mettere in sicurezza la connessione tra server e DB (che avviene attualmente tramite il framework hibernate) che potrebbe stare non più in locale, ma essere migrato potenzialmente anche in cloud, per questo dobbiamo instaurare una connessione sicura SSL mutuamente autenticata col DB per evitare disclosure o peggio accessi con permessi di modifica e delete non autorizzati. Il DB deve prevedere una forma di autenticazione del backend appropriata, che non sia root.

-Le informazioni del sistema devono viaggiare verso l’esterno del dominio dell’organizzazione solo su canali cifrati. Anche i canali interni devono essere crittati per evitare attacchi che bypassano il firewall.

-La comunicazione col broker MQTT deve essere messa in sicurezza per evitare tampering dei comandi inviati o disclosure delle informazioni. Si richiede pertanto una connessione SSL mutuamente autenticata con il web server che invia richieste.

-La comunicazione tra il web server e il server keycloak deve essere cifrata e mutuamente autenticata (SSL).

-I pacchetti provenienti dall’esterno devono essere protetti da un firewall di perimetro. Per proteggersi eventualmente da attacchi DoS.

-I firewall devono fare anche da divisori di zona. È presente una DMZ, una zona DB e una zona per la comunicazione con MCU.

-I filesystem devono essere cifrati, i bios devono essere protetti da password, il database MariaDB deve avere le tabelle cifrate. Il file XML del java web server deve essere cifrato con PBE.

-L’accesso alle macchine deve essere fisicamente protetto per evitare memory dump che possono portare al disclosure di informazioni critiche.

Key management

-Le chiavi generate con OpenSSL per RSA devono essere di 2048 bit almeno.

-Le chiavi devono essere mantenute in maniera sicura, possibilmente in keystore protetti da password, che devono essere immesse da tastiera per poter essere conservate su un mezzo fisico differente. Non deve essere possibile per un utente esterno leggerle. Ogni anno e mezzo i certificati interni vanno rigenerati, ogni anno vanno rigenerati i certificati offerti all’esterno. Le chiavi devono essere manenute in keystore crittati e/o deve esserne proibito l’accesso tramite i controlli di sicurezza del sistema operativo.

I certificati sostituiti vanno aggiunti alla CRL dei vari componenti del sistema per evitare la validazione di un certificato non più utilizzato.

-Il segreto condiviso tra il web server e keycloak deve essere rigenerato una volta ogni due mesi.