Verbale esterno del 2020-03-26

Gruppo VarTmp7 - Progetto Stalker vartmp7@gmail.com

Informazioni sul documento	
Versione	1.0.0-INC-9
Approvatore	Lorenzo Taschin
Redattori	Marco Ferrati
Verificatori	Stefano Cavaliere
Uso	Esterno
Distribuzione	Prof. Tullio Vardanega Prof. Riccardo Cardin VarTmp7

Descrizione

Verbale dell'incontro del gruppo *VarTmp7* con *Davide Zanetti*, referente di Imola Informatica, tenutosi il 2020-03-26.

Registro delle modifiche

Versione	Data	Descrizione	Nominativo	Ruolo
1.0.0-INC-9	2020-04-02	Documento approvato	Lorenzo Taschin	*Responsabile*
1.0.0-INC-9	2020-04-02	Verifica con esito positivo	Stefano Cavaliere	*Verificatore*
0.0.1-INC-8	2020-03-28	Stesura verbale del 2020-03-26	Marco Ferrati	*Redattore*
0.0.1-0	2019-12-01	Creazione scheletro del documento	Claudia Zattara	*Redattore*

Indice

1 Informazioni generali **3**
1.1 Informazioni incontro: 3
1.2 Ordine del giorno 3

2 Verbale della riunione **4**
2.1 Autenticazione tramite LDAP 4
2.2 Varie ed eventuali 4

3 Tracciamento delle decisioni **5**

1 Informazioni generali

1.1 Informazioni incontro:

- **Luogo**: Hangouts;
- **Data**: 2020-03-26;
- **Ora di inizio**: 10:00;
- **Ora di fine**: 12:00;
- **Presenze**:
  - interni:
    - Xiaowei Wen;
    - Marco Ferrati;
  - esterni:
    - Davide Zanetti, referente di Imola Informatica.
    - referente gruppo qbteam;
    - referente gruppo GruppOne

1.2 Ordine del giorno

Gli argomenti discussi sono:

1. autenticazione tramite LDAP;
2. varie ed eventuali.

2 Verbale della riunione

Durante questo incontro sono state poste una serie di domande riguardanti soprattutto il funzionamento dell'autenticazione tramite LDAP.

2.1 Autenticazione tramite LDAP

La discussione è iniziata con delle proposte da parte dei gruppi su come avrebbe potuto funzionare l'accesso tramite LDAP, riportate di seguito:

1. l'applicazione Android manda le credenziali per l'autenticazione del dipendente al backend di Stalker che si occupa di verificarne la validità connettendosi al server LDAP;
2. l'applicazione Android si autentica al server LDAP;
3. utilizzare strumenti come Kerberos per l'autenticazione.

Il proponente ha subito sconsigliato l'opzione 3 per eccessiva complicatezza nell'utilizzo di strumenti come Kerberos ed era, invece, molto interessato all'opzione 2 in quanto preferirebbe che i dati di autenticazione dei dipendenti restino nel loro smartphone.
I gruppi hanno spiegato che durante ricerche fatte nei giorni precendenti all'incontro non erano riusciti a trovare un metodo per controllare se un dipendente aveva o meno eseguito l'accesso in maniera corretta al server LDAP dall'applicazione e questo metteva a rischio il sistema in quanto facilmente ingannabile poichè chiunque poteva spacciarsi per un dipendente e registrare spostamenti nei luoghi delle organizzazioni.
È stata avanzata l'idea di considerare le applicazioni come affidabili e quindi non porsi il problema del fatto che i dipendenti si fossero autenticati correttamente.
Alla fine si è giunti alla conclusione che l'opzione più fattibile fosse la prima, ovvero che l'onere dell'autenticazione del dipendente passasse al backend Stalker purchè le credenziali non passasero in chiaro (quindi stato imposto l'uso del protocollo HTTPS per le comunicazioni tra applicazione e backend)

2.2 Varie ed eventuali

È stato chiesto a Davide Zanetti se conoscesse qualcuno al quale chiedere qualche informazione riguardo alla piattaforma Android e lui ci ha mandato la mail del suo collega Pietro Zito pzito@imolainformatica.it.

3 Tracciamento delle decisioni

Codice	Decisione
2020-03-26/01	L'applicazione non deve più occuparsi di autenticare i dipendenti.
2020-03-26/02	Il backend si occupa di autenticare i dipendenti tramite LDAP.
2020-03-26/03	Il requisito R-5-V-F diventa obbligatorio.
2020-03-26/04	Viene scartata l'idea di "applicazione trusted".
2020-03-26/05	Viene scartata l'idea di usare strumenti come Kerberos per l'autenicazione dei dipendenti.