MODELLIZZAZIONE DELLE MINACCE
FRAMEWORK ADAM SHOSTACK

INDICE:

FRAMEWORK

SU COSA STIAMO LAVORANDO?

Il gruppo BCC Iccrea si sta concentrando sull'implementazione di una funzione che consenta agli utenti di accedere al proprio HomeBanking senza dover reinserire la password per un periodo di almeno 48 ore dall'ultimo accesso. Questa iniziativa mira a migliorare l'esperienza utente rendendo il processo di accesso più semplice e conveniente, senza compromettere la sicurezza.

Ecco alcuni punti chiave che argomentano questa iniziativa:

1. **Convenienza per gli utenti:** Eliminando la necessità di reinserire la password ad ogni accesso per un periodo di tempo prolungato, si semplifica notevolmente l'esperienza degli utenti. Questo riduce la frizione nel processo di accesso e aumenta la comodità, incoraggiando gli utenti a utilizzare regolarmente i servizi di HomeBanking.
2. **Risparmio di tempo:** Gli utenti non devono più preoccuparsi di ricordare e inserire la password ogni volta che vogliono accedere al proprio account bancario online. Ciò risparmia tempo e sforzi, migliorando l'efficienza complessiva del processo di accesso.
3. **Sicurezza incrementata:** Nonostante l'eliminazione della necessità di reinserire la password frequentemente, il sistema mantiene comunque un livello adeguato di sicurezza. Il periodo di 48 ore senza richiesta di password è sufficientemente lungo da fornire un equilibrio tra comodità e sicurezza. Inoltre, è possibile implementare ulteriori misure di sicurezza come la verifica in due passaggi per rafforzare la protezione dell'account.
4. **Adozione tecnologica:** Questa iniziativa riflette un'impostazione moderna e all'avanguardia nell'utilizzo della tecnologia per migliorare i servizi bancari online. Il gruppo BCC Iccrea dimostra la sua volontà di adattarsi alle esigenze e alle aspettative degli utenti, fornendo soluzioni innovative che semplificano e migliorano l'esperienza bancaria digitale.

In conclusione, l'implementazione di una funzione che consente agli utenti di accedere al proprio HomeBanking senza reinserire la password per almeno 48 ore dall'ultimo accesso rappresenta un passo significativo verso l'ottimizzazione dell'esperienza utente e la promozione della sicurezza nell'ambito dei servizi bancari online.

COSA PUÒ ANDARE STORTO?

Assolutamente, una cattiva implementazione della funzione potrebbe certamente esporre gli utenti del gruppo BCC Iccrea a rischi per la privacy e accessi non autorizzati. Ecco alcuni motivi per cui ciò potrebbe accadere:

1. **Vulnerabilità dei dati:** Se il meccanismo per mantenere attivo l'accesso senza richiedere la password non è adeguatamente protetto, potrebbe essere soggetto a violazioni dei dati. Se le informazioni sullo stato di accesso dell'utente (come il flag che indica se è attivo o meno) sono compromesse, gli hacker potrebbero sfruttare questa vulnerabilità per ottenere accesso non autorizzato agli account degli utenti.
2. **Mancanza di controlli di sicurezza:** Se non vengono implementati controlli di sicurezza aggiuntivi, come la verifica in due passaggi o il monitoraggio delle attività sospette, potrebbe essere più facile per gli attaccanti sfruttare l'accesso continuo senza password per compiere attività dannose sugli account degli utenti.
3. **Rischi legati alla perdita o al furto del dispositivo:** Se un dispositivo su cui è attivo l'accesso continuo senza password viene perso o rubato, chiunque abbia fisicamente accesso al dispositivo potrebbe ottenere facilmente l'accesso al conto dell'utente senza la necessità di una password. Questo scenario può portare a gravi violazioni della privacy e al furto di informazioni finanziarie sensibili.
4. **Mancanza di consapevolezza degli utenti:** Se gli utenti non sono adeguatamente informati sui rischi associati all'accesso continuo senza password o se non sono istruiti su come proteggere i propri dispositivi e account, potrebbero diventare vulnerabili ad attacchi di phishing o altri tipi di attacchi che sfruttano la loro fiducia nell'accesso automatico.

In conclusione, una cattiva implementazione della funzione per mantenere attivo l'accesso senza password potrebbe esporre gli utenti del gruppo BCC Iccrea a una serie di rischi per la privacy e accessi non autorizzati. È fondamentale che vengano adottate misure di sicurezza appropriate e che gli utenti siano educati sui rischi associati all'accesso continuo senza password e su come proteggere i propri account.

CHE COSA FAREMO AL RIGUARDO?

La decisione di eseguire una revisione approfondita del codice e dei processi di autenticazione, insieme alla considerazione dell'implementazione di meccanismi aggiuntivi di autenticazione multifattoriale, è una mossa saggia e responsabile da parte del gruppo BCC Iccrea. Ecco perché:

1. **Identificazione delle vulnerabilità:** Una revisione approfondita del codice e dei processi di autenticazione consentirà di individuare eventuali debolezze o vulnerabilità nel sistema. Questo è cruciale per garantire che l'implementazione della funzione di accesso senza password sia sicura e robusta, riducendo al minimo il rischio di exploit da parte di attaccanti esterni.
2. **Miglioramento della sicurezza:** L'implementazione di meccanismi aggiuntivi di autenticazione multifattoriale aggiunge un ulteriore livello di sicurezza al sistema. Questi meccanismi richiedono agli utenti di fornire più di un tipo di prova di identità (come una password e un codice generato da un'applicazione mobile o inviato tramite SMS) per accedere al proprio account. Ciò rende molto più difficile per gli attaccanti compromettere gli account degli utenti anche se riescono a ottenere la password.
3. **Protezione della privacy degli utenti:** Implementare misure di sicurezza aggiuntive non solo protegge gli account degli utenti da accessi non autorizzati, ma contribuisce anche a preservare la loro privacy. L'adozione di meccanismi di autenticazione multifattoriale assicura che solo gli utenti autorizzati possano accedere ai propri account, riducendo il rischio di violazioni della privacy e furto di dati sensibili.
4. **Conformità normativa:** In molte giurisdizioni, esistono regolamenti rigidi in materia di sicurezza dei dati e protezione della privacy, che richiedono l'implementazione di misure di sicurezza avanzate. L'adozione di meccanismi di autenticazione multifattoriale può aiutare il gruppo BCC Iccrea a conformarsi a queste normative e ad evitare sanzioni legali.

In conclusione, eseguire una revisione approfondita del codice e dei processi di autenticazione e considerare l'implementazione di meccanismi aggiuntivi di autenticazione multifattoriale sono passi essenziali per garantire la sicurezza degli account degli utenti e la protezione della privacy nel conte del servizio di HomeBanking del gruppo BCC Iccrea.

ABBIAMO FATTO UN BUON LAVORO?

Eseguire simulazioni di attacchi informatici dopo aver completato la revisione e implementato le modifiche raccomandate è una pratica cruciale per garantire l'efficacia delle misure di sicurezza adottate dal gruppo BCC Iccrea. Ecco perché questa fase è fondamentale:

1. **Test di vulnerabilità:** Le simulazioni di attacchi informatici consentono di testare le nuove misure di sicurezza in un ambiente controllato, identificando potenziali vulnerabilità o falle nel sistema. Questi test simulano gli stessi metodi e tecniche che potrebbero essere utilizzati dagli attaccanti reali, offrendo una panoramica accurata delle vulnerabilità ancora presenti.
2. **Valutazione dell'efficacia:** Le simulazioni di attacchi informatici consentono di valutare l'efficacia delle misure di sicurezza implementate nel mitigare i rischi. Questo aiuta il gruppo BCC Iccrea a determinare se le modifiche apportate sono state sufficienti per proteggere gli account degli utenti e i dati sensibili da accessi non autorizzati o compromissioni.
3. **Identificazione di potenziali miglioramenti:** Qualsiasi debolezza o vulnerabilità rilevata durante le simulazioni di attacchi informatici fornisce opportunità per identificare ulteriori miglioramenti nella sicurezza del sistema. Questi risultati possono essere utilizzati per iterare sulle misure di sicurezza esistenti e implementare ulteriori contromisure per ridurre ulteriormente i rischi.
4. **Conferma della conformità normativa:** Le simulazioni di attacchi informatici aiutano anche a dimostrare la conformità del sistema con le normative di sicurezza e protezione dei dati. Le organizzazioni spesso sono tenute a dimostrare di aver adottato misure adeguate per proteggere le informazioni sensibili degli utenti, e le simulazioni di attacchi informatici forniscono una prova tangibile di questo impegno.

In conclusione, eseguire simulazioni di attacchi informatici dopo aver completato la revisione e implementato le modifiche raccomandate è essenziale per confermare che i rischi siano stati mitigati adeguatamente e che il sistema sia protetto in modo efficace. Solo attraverso questo approccio di test e verifica è possibile garantire un elevato livello di sicurezza e protezione per gli account degli utenti e i dati sensibili del gruppo BCC Iccrea.

GAP ANALYSIS DETTAGLIATA

ANALISI BACK END

Java:

1. **Revisione del codice e processi di autenticazione attuali:**
   - Identificare i metodi attuali di autenticazione e i processi di gestione delle sessioni.
   - Valutare la sicurezza dei processi esistenti rispetto agli standard attuali.
2. **Identificazione delle vulnerabilità:**
   - Condurre test di vulnerabilità per individuare possibili falle nel sistema.
   - Identificare le vulnerabilità che potrebbero essere sfruttate per compromettere l'autenticazione degli utenti.
3. **Implementazione di meccanismi di autenticazione multifattoriale:**
   - Valutare la necessità e la fattibilità di aggiungere meccanismi di autenticazione multifattoriale.
   - Esaminare le migliori pratiche e i framework disponibili per l'implementazione.
4. **Test di sicurezza post-implementazione:**
   - Eseguire simulazioni di attacchi informatici per valutare l'efficacia delle nuove misure di sicurezza.
   - Identificare eventuali lacune o debolezze rimanenti nel sistema e pianificare azioni correttive.

ANALISI FRONT END

Angular:

1. **Revisione del codice e processi di autenticazione attuali:**
   - Esaminare il codice frontend esistente per l'autenticazione degli utenti.
   - Valutare la sicurezza dei processi di gestione dell'autenticazione e delle sessioni.
2. **Integrazione con il backend Java:**
   - Verificare l'integrazione corretta con il backend Java per l'autenticazione e la gestione delle sessioni.
   - Assicurarsi che le richieste di autenticazione siano gestite in modo sicuro e che i token JWT siano gestiti correttamente.
3. **Aggiornamenti dell'interfaccia utente:**
   - Implementare le modifiche necessarie all'interfaccia utente per supportare l'accesso senza password e l'autenticazione multifattoriale.
   - Assicurarsi che gli utenti siano informati e guidati attraverso il processo di autenticazione senza password.
4. **Test di sicurezza post-implementazione:**
   - Condurre test di penetrazione e simulazioni di attacchi per verificare la sicurezza delle nuove funzionalità implementate.
   - Identificare eventuali falle nella sicurezza o nei processi di autenticazione e pianificare azioni correttive.