CONSEGNA 24 APRILE S1L3

INTRODUZIONE

Utilizzando il framework di modellizzazione delle minacce di Adam Shostack, identifica una minaccia per un'azienda di sviluppo software.

Il framework di Shostack si basa su quattro domande chiave per identificare le minacce:

Su cosa stiamo lavorando?
Cosa può andare storto?
Che cosa faremo al riguardo?
Abbiamo fatto un buon lavoro?

Ripeti il processo, eseguendo una gap analysis per trovare i punti di miglioramento.

INDICE

1 Il contesto

L'azienda di sviluppo software in questione è una società di medie dimensioni, operante prevalentemente nel settore dei servizi finanziari, con una specializzazione in applicazioni per la gestione delle transazioni bancarie e dei pagamenti online.

Profilo dell'Azienda

- **Nome:** BCC iccrea
- **Numero di dipendenti:** Circa 200
- **Fatturato annuale:** Circa 30 milioni di euro
- **Sede principale:** Roma, Italia
- **Mercato di riferimento:** Italia, con particolare focus su clienti aziendali come banche, assicurazioni e società di gestione degli investimenti.

Caratteristiche Organizzative

- **Dipartimenti:**
  - Sviluppo e Ricerca (circa 100 ingegneri software)
  - Vendite e Marketing (40 persone)
  - Supporto tecnico e Manutenzione (30 persone)
  - Sicurezza IT e Compliance (15 persone)
  - Risorse Umane e Amministrazione (15 persone)
- **Struttura IT:**
  - Infrastruttura cloud ibrida per la flessibilità e l'efficienza nell'elaborazione dei dati sensibili.
  - Utilizzo di soluzioni di sicurezza all'avanguardia per la protezione delle informazioni e per mitigare i rischi di attacchi cyber.

1.1 Il threat modelling

Il processo di identificazione delle minacce (threat modelling) è un processo di identificazione dei rischi che prevede l'esame di ogni possibile attore malevolo, azione o evento, vettore di attacco e vulnerabilità per un determinato sistema, bene o processo. Questo processo di identificazione di rischi si serve di strumenti e procedure specifici, chiamati Threat modelling framework, che ci aiutano ad identificare, analizzare e mitigare le minacce. Tra i vari framework a disposizione, per identificare le minacce che possono colpire la nostra azienda ci serviremo di quello proposto da Adam Shostack.

1.2 Il framework di Adam Shostack

Il framework di modellizzazione delle minacce proposto da Adam Shostack è un approccio strutturato per identificare le minacce alla sicurezza nel contesto di un'organizzazione o di un progetto software. È incentrato sulla comprensione e mitigazione dei rischi di sicurezza a partire da quattro domande chiave:

1. Su cosa stiamo lavorando?
2. Cosa può andare storto?
3. Che cosa faremo al riguardo?
4. Abbiamo fatto un buon lavoro?

Andremo ad applicare questo framework all'azienda in esame.

1.3 Applicazione del framework al contesto aziendale

Esempio di come potremmo applicare il framework di Shostack alla BCC iccrea:

1. **Su cosa stiamo lavorando?**

    - Lavoriamo su un'azienda di sviluppo software che lavora su applicazioni commerciali per clienti aziendali. Queste applicazioni gestiscono dati sensibili come informazioni finanziarie e personali degli utenti.

2. **Cosa può andare storto?**

    - Una delle principali minacce potrebbe essere una violazione dei dati dovuta a vulnerabilità nel codice dell'applicazione, come SQL Injection o Cross-Site Scripting (XSS), che potrebbero permettere agli attaccanti di accedere o manipolare dati sensibili.
    - Un'altra minaccia significativa potrebbe essere l'insider threat, ovvero il rischio che dipendenti interni o collaboratori sfruttino il loro accesso per compiere azioni dannose.
    - Infine, attacchi DDoS potrebbero mirare a rendere l'applicazione non disponibile, danneggiando la reputazione aziendale e causando interruzioni del servizio.

3. **Che cosa faremo al riguardo?**

    - **Mitigazione delle vulnerabilità nel codice**: Implementare pratiche di secure coding, revisioni periodiche del codice e testing di sicurezza come penetration testing e static/dynamic code analysis.
    - **Prevenzione insider threat**: Adottare politiche di controllo degli accessi basate sul principio del minimo privilegio, effettuare regolarmente audit di sicurezza e promuovere una cultura aziendale di consapevolezza sulla sicurezza.
    - **Protezione da attacchi DDoS**: Utilizzare servizi di mitigazione DDoS, bilanciamento del carico e infrastrutture resilienti per ridurre l'impatto degli attacchi di denial of service.

4. **Abbiamo fatto un buon lavoro?**

    - Questa domanda richiede un'analisi continua e valutazioni regolari delle misure di sicurezza in atto. L'efficacia delle strategie di mitigazione dovrebbe essere monitorata attraverso audit di sicurezza, test di penetrazione periodici e l'utilizzo di metriche per valutare la sicurezza delle applicazioni. Inoltre, il feedback degli utenti e degli stakeholder interni può fornire indicazioni preziose su eventuali aree di miglioramento.

2 Analisi dei gap del contesto aziendale

La Gap analysis è un processo che coinvolge la valutazione delle discrepanze o della lacune tra la situazione attuale e quella desiderata in termini di gestione del rischio.

Applicata al control gap, la gap analysis permette di individuare quali controlli sono necessari, quali mancano o sono insufficienti e quali azioni correttive possono essere intraprese per colmare queste lacune e migliorare complessivamente la sicurezza e la gestione dei rischi, attraverso la definizione di un piano d'azione (action plan) e di una tabella di marcia (roadmap).

Un piano d'azione è un piano dettagliato che elenca le azioni specifiche da intraprendere, insieme a tempistiche, responsabilità e risorse necessarie, per raggiungere un'obbiettivo definito entro un periodo di tempo determinato.

Una tabella di marcia è una rappresentazione visiva o un documento che illustra le tappe e le fasi necessarie per raggiungere un'obbiettivo a lungo termine, includendo minestrone, obbiettivi intermedi e obbiettivi finali nel corso del tempo.

L'analisi dei gap costringe a pensare alla situazione attuale, allo stato futuro desiderato, alle cause principali del divario tra i due e al piano d'azione per colmare il divario in modo molto strutturato e chiaro.

È da considerare come il ponte che ci porterà dal punto A (lo stato attuale) al punto B (lo stato desiderato). (Fig.1)

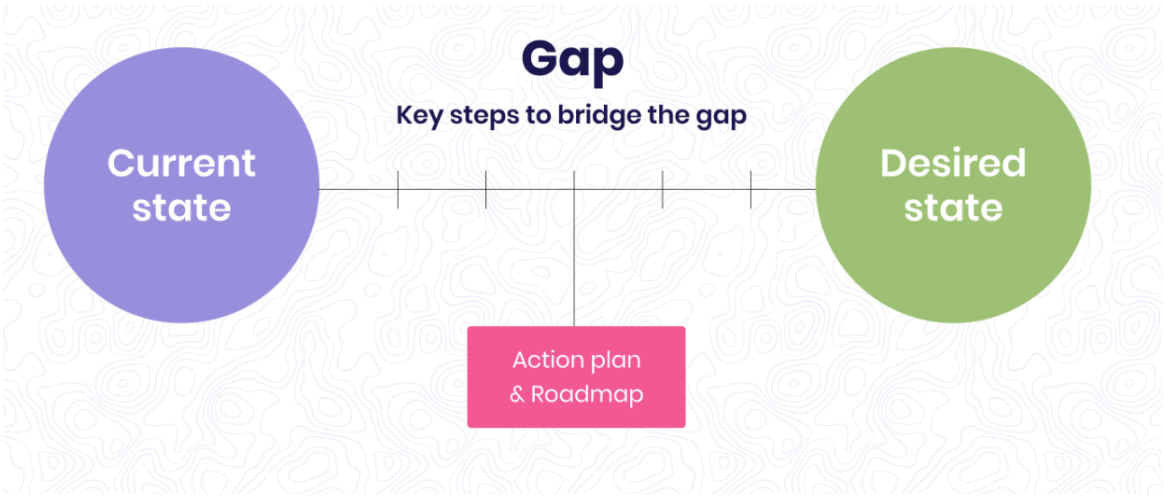

Fig.1.

Concentreremo ora l'analisi su una delle aree principali della nostra azienda, quella della **conformità normativa**:

Stato Attuale:

- Conformità con le normative locali sul trattamento dei dati personali.
- Politiche di privacy e sicurezza che rispettano i requisiti base del GDPR.

Stato Desiderato:

- Essere un punto di riferimento nel settore per la conformità normativa.
- Superare regolarmente audit esterni senza alcuna non conformità.

Gap:

- Mancano procedure regolari di audit esterni.
- Necessità di migliorare la documentazione e le procedure di conformità.