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

Identificazione della minaccia:

- ***Su cosa stiamo lavorando?***
- Stiamo sviluppando un'applicazione software per la gestione di dati sensibili dei clienti di un'azienda.

- ***Cosa può andare storto?***
- Una possibile minaccia potrebbe essere un attacco di tipo injection, come ad esempio un attacco SQL injection, che potrebbe compromettere la sicurezza dei dati memorizzati nell'applicazione.

- ***Che cosa faremo al riguardo?***
- Implementeremo controlli di sicurezza come la validazione e l'escape dei dati di input, l'utilizzo di parametrized queries per le interrogazioni al database e l'adozione di pratiche di codifica sicura per prevenire l'iniezione di codice dannoso.

- ***Abbiamo fatto un buon lavoro?***
- Per valutare l'efficacia delle misure di sicurezza implementate, condurremo test di penetrazione e revisioni del codice.

Gap analysis utilizzando i controlli NIST SP 800-53 Rev. 5:

Esaminiamo i controlli forniti da NIST SP 800-53 Rev. 5 per identificare eventuali lacune nella nostra attuale postura di sicurezza.

Possiamo notare che alcuni controlli specifici, come "AC-3: Access Enforcement" (Applicazione del principio del minimo privilegio), "SI-7: Software, Firmware, and Information Integrity" (Verifica dell'integrità del software) e "SI-9: Information Input Validation" (Validazione dei dati di input), potrebbero essere ulteriormente rafforzati per affrontare specificamente la minaccia di SQL injection.

Inoltre, potremmo trovare opportunità di miglioramento nei controlli relativi alla rilevazione e alla risposta agli incidenti, come "IR-4: Incident Handling" (Gestione degli incidenti) e "IR-6: Incident Reporting" (Segnalazione degli incidenti), per garantire una risposta tempestiva e efficace in caso di violazioni della sicurezza.

Azioni correttive e miglioramenti:

Basandoci sulla gap analysis, possiamo pianificare azioni correttive per rafforzare ulteriormente la sicurezza dell'applicazione.

Possibili azioni includono l'implementazione di controlli aggiuntivi per l'applicazione del principio del minimo privilegio, l'implementazione di meccanismi per la verifica dell'integrità del software e l'aggiornamento delle procedure di gestione degli incidenti per migliorare la risposta agli eventi di sicurezza.