BCC Iccrea - S1/L3
Sara Spaccialbelli

Identificazione del rischio

Traccia:

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. I controlli NIST SP 800-53 Rev. 5. possono aiutare nella modellizzazione delle minacce.

Shostack Threat modelling framework:

1. Su cosa stiamo lavorando?

Stiamo sviluppando un'applicazione di gestione di dati per i clienti, che include informazioni finanziarie, personali e sensibili.

2. Cosa può andare storto?

Una minaccia potenziale è la "violazione dei dati", che potrebbe avvenire attraverso:

1. Accesso non autorizzato: Un attaccante potrebbe ottenere accesso ai dati sensibili a causa di vulnerabilità nel sistema o mancanza di controlli di accesso.
2. Smarrimento o furto di dispositivi: Se un dispositivo contenente dati sensibili viene perso o rubato, i dati potrebbero essere compromessi.
3. Attacchi di phishing: Dipendenti o clienti potrebbero essere ingannati da attacchi di phishing, che potrebbero portare alla divulgazione di credenziali di accesso.

3. Che cosa faremo al riguardo?

Per mitigare questa minaccia, abbiamo adottato le seguenti misure:

a. Crittografia dei dati: Tutti i dati sensibili saranno crittografati sia in transito che a riposo.
b. Controlli di accesso: Implementiamo un sistema di gestione degli accessi con autenticazione a due fattori (2FA) per ridurre il rischio di accesso non autorizzato.
c. Formazione sulla sicurezza: Offriamo formazione regolare ai dipendenti per riconoscere e prevenire gli attacchi di phishing.
d. Monitoraggio e rilevamento: Utilizziamo sistemi di monitoraggio per individuare attività sospette o accessi non autorizzati.

4. Abbiamo fatto un buon lavoro?

Sì, abbiamo compiuto passi significativi per mitigare la minaccia di violazione dei dati. Tuttavia, è importante continuare a valutare e aggiornare le nostre misure di sicurezza per rimanere al passo con le nuove minacce. Potremmo anche considerare una revisione periodica dei nostri protocolli di sicurezza e coinvolgere un'agenzia esterna per testare la nostra sicurezza (penetration testing) e identificare eventuali punti deboli.

Gap Analysis con controlli NIST SP 800-53 Rev. 5:

Una gap analysis ci permette di individuare quali controlli sono necessari e quali azioni correttive possono essere intraprese per migliorare la sicurezza e la gestione dei rischi.
In questo caso andiamo ad analizzare la minaccia di violazione dei dati nella gestione di dati sensibili.

Controllo: AC-2 Controlli d'Accesso

Stato attuale: Implementazione di controlli di accesso base con autenticazione username/password.

Punto di miglioramento: Implementare l'autenticazione a due fattori (2FA) per tutti gli utenti.

Controllo: AC-3 Controlli di accesso alla rete

Stato attuale: Controllo di accesso alla rete basato su ACL (Access Control List).

Punto di miglioramento: Implementare controlli di accesso basati su ruoli per limitare l'accesso solo ai dati necessari per il compito.

Controllo: AC-5 Gestione degli account

Stato attuale: Politiche per la gestione delle password.

Punto di miglioramento: Implementare una politica di revisione degli account per rimuovere gli account inattivi o non autorizzati.

Controllo: SC-7 Monitoraggio dell'uso dei sistemi

Stato attuale: Monitoraggio delle attività degli utenti.

Punto di miglioramento: Implementare un sistema di allarme per rilevare attività sospette o accessi non autorizzati.

Controllo: SI-7 Protezione delle informazioni

Stato attuale: Crittografia dei dati sensibili.

Punto di miglioramento: Implementare la crittografia dei dati in transito utilizzando protocolli sicuri come TLS .

Controllo: IR-4 Risposta agli incidenti e analisi

Stato attuale: Pianificazione di risposta agli incidenti di base.

Punto di miglioramento: Sviluppare e testare un piano dettagliato di risposta agli incidenti, incluso un processo per la notifica delle violazioni dei dati.

Azioni di Miglioramento:

- **Integrazione 2FA:** Implementare l'autenticazione a due fattori (2FA) senza sostituire l'autenticazione username/password esistente.
- **Aggiunta di controlli di accesso basati su ruoli:** Integrare controlli di accesso basati su ruoli per limitare l'accesso solo ai dati necessari per il compito, senza sostituire l'ACL attuale.
- **Politica di revisione degli account:** Integrare una politica di revisione degli account per rimuovere gli account inattivi o non autorizzati, senza sostituire le politiche attuali.
- **Sistema di allarme per monitoraggio:** Aggiungere un sistema di allarme per rilevare attività sospette o accessi non autorizzati senza impattare l'infrastruttura attuale.
- **Integrazione della crittografia dei dati in transito**: Implementare la crittografia dei dati in transito utilizzando protocolli sicuri come TLS senza modificare l'infrastruttura esistente.
- **Miglioramento del piano di risposta agli incidenti**: Aggiungere dettagli al piano di risposta agli incidenti, incluso un processo per la notifica delle violazioni dei dati, senza richiedere nuovo personale o formazione significativi.

Considerazioni aggiuntive:

- **Costi per i nuovi controlli**: Verificare che i costi per l'integrazione dei nuovi controlli siano ragionevoli e non superino il valore dell'asset.
- **Implementazione in altre aree:** Esaminare la possibilità di implementare i nuovi controlli anche in altre aree dell'azienda per ridurre il rischio globale senza aumentare significativamente i costi.
- **Valore dell'asset vs. costo del controllo:** Sebbene il costo del controllo possa superare il valore dell'asset, se il controllo è essenziale per mitigare una minaccia critica come la violazione dei dati, potrebbe essere necessario implementarlo comunque.

Considerazioni finali:

Questa gap analysis e le raccomandazioni fornite considerano l'integrazione e l'aggiunta di nuovi controlli senza necessariamente sostituire quelli attuali. Questo approccio mira a migliorare la sicurezza dell'applicazione di gestione di dati sensibili senza creare significative interruzioni nell'infrastruttura esistente o richiedere nuovi investimenti significativi. Le azioni proposte dovrebbero aumentare la robustezza dei controlli di sicurezza e ridurre il rischio di violazioni dei dati.

GRAZIE

Sara Spaccialbelli