IDENTIFICAZIONE DEL RISCHIO S1L3

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: NIST SP 800-53 Rev. 5-Security and Privacy Controls for Information Systems and Organizations NIST SP 800-53A Rev. 5 -Assessing Security and Privacy Controls in Information Systems and Organizations

UTILIZZO FRAMEWORK ADAM SHOSTACK

Su cosa stiamo lavorando? Stiamo lavorando su un'applicazione software che gestisce dati sensibili degli utenti, come informazioni personali e dettagli finanziari.

Cosa può andare storto? Una possibile minaccia potrebbe essere un attacco di phishing da parte di un hacker, che potrebbe compromettere i dati sensibili degli utenti inviando e-mail fasulle ai dipendenti delle aziende clienti, fingendo di essere noi o un'affidabile autorità aziendale, al fine di ottenere accesso non autorizzato al sistema o di raccogliere informazioni sensibili tramite tecniche di ingegneria sociale.

- **Che cosa faremo al riguardo**. Implementeremo controlli di sicurezza robusti, come la validazione dell'input, l'uso di prepar ed statements o stored procedures, e l'implementazione di principi di minimo privilegio. Inoltre, utilizzeremo i controlli NIST SP 800-53 Rev. 5 per valutare e migliorare ulteriormente la nostra sicurezza.
- **Abbiamo fatto un buon lavoro?** Per determinare se abbiamo fatto un buon lavoro, dovremmo condurre regolari audit di sicurezza e test di penetrazione per identificare eventuali vulnerabilità. Inoltre, dovremmo monitorare continuamente i nostri sistemi per rilevare qualsiasi attività sospetta.

GAP ANALYSIS

- Consapevolezza e formazione: Fornire regolarmente corsi di formazione sui rischi della sicurezza informatica e sul riconoscimento delle tecniche di phishing ai dipendenti dell'azienda.
- Filtraggio delle email: Implementare filtri antispam e antiphishing per identificare e bloccare le email sospette in arrivo.
- Autenticazione multi-fattore (MFA): Richiedere l'utilizzo di MFA per l'accesso a sistemi sensibili o contenenti dati sensibili.
- Politiche di sicurezza delle password: Implementare politiche robuste per la creazione e l'aggiornamento delle password, incluso il requisito di password complesse e la rotazione periodica.
- Monitoraggio dell'accesso e delle attività: Implementare strumenti di monitoraggio per rilevare comportamenti anomali o tentativi di accesso non autorizzati

VALUTAZIONE DEI CONTROLLI NIST SP 800-53 REV. 5:

Controlli Raccomandati:

- AC-SC-1: Training and Awareness
- SC-7: Boundary Protection
- IA-2: Identification and Authentication (Organizational Users)
- SI-4: Information System Monitoring
- Valutazione dell'Efficienza:
- I controlli NIST SP 800-53 Rev. 5 forniscono una solida base per affrontare la minaccia del phishing.
- L'implementazione dei controlli proposti fornirà un livello significativo di protezione contro gli attacchi di phishing, riducendo il rischio di compromissione dei dati e dei sistemi.

CONCLUSIONE:

- La minaccia del phishing rappresenta una seria preoccupazione per la sicurezza del nostro software di gestione delle risorse umane. Tuttavia, con l'adozione delle contromisure appropriate e l'implementazione dei controlli raccomandati dal NIST SP 800-53 Rev. 5, possiamo ridurre significativamente il rischio e proteggere efficacemente i dati sensibili dei nostri clienti.