RISK MANAGEMENT

IDENTIFICAZIONE DEL RISCHIO

MARIA HUAPAYA

INDICE

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:
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

INTRODUZIONE

Presentazione del framework di modellizzazione delle minacce di Adam Shostack

Il framework di modellizzazione delle minacce di Adam Shostack è un approccio strutturato alla sicurezza che aiuta le organizzazioni a identificare, comprendere e mitigare le minacce. Il modello si basa sull'analisi sistematica degli asset, dei nemici, delle vulnerabilità e dei punti di ingresso che gli attaccanti potrebbero sfruttare. Il framework è progettato per essere iterativo, promuovendo un miglioramento continuo delle pratiche di sicurezza. Uno degli aspetti chiave di questo framework è la sua enfasi sulle domande guidate, che aiutano a strutturare il pensiero e la discussione:

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

Presentazione dell'azienda di sviluppo software: EpiSec Solutions S.p.A.

EpiSec Solutions S.p.A. è specializzata in soluzioni di sicurezza informatica per il settore bancario e finanziario. Fondata nel 2010, l'azienda conta 250 dipendenti e ha sedi in Italia, Germania e Stati Uniti. EpiSec Solutions offre prodotti che aiutano le banche e le istituzioni finanziarie a proteggere i dati dei clienti, a monitorare le transazioni in tempo reale e a prevenire frodi finanziarie. Gli asset critici includono il software di gestione delle transazioni, i database dei clienti e le infrastrutture cloud distribuite.

IDENTIFICAZIONE DELLA MINACCIA

In questa fase, analizzeremo gli asset critici di EpiSec Solutions S.p.A. e identificheremo le potenziali minacce. Questo passaggio è cruciale per stabilire come proteggere efficacemente l'azienda.

a) Descrizione degli asset (Su cosa stiamo lavorando?)

Gli asset principali di EpiSec Solutions includono:

- Software di gestione delle transazioni: questo software è il cuore delle operazioni per i clienti di EpiSec, gestendo e archiviando transazioni finanziarie sensibili.
- Database dei clienti: contiene informazioni personali e finanziarie dei clienti, il che lo rende un bersaglio primario per gli attacchi.
- Infrastrutture cloud distribuite: queste infrastrutture supportano l'operatività continua e l'accessibilità dei servizi software, ma introducono complessità e potenziali vulnerabilità.

b) Identificazione delle potenziali minacce (Cosa può andare storto?)

Le potenziali minacce che possono interessare gli asset di EpiSec Solutions sono:

1. Attacchi di iniezione SQL: potrebbero essere utilizzati per manipolare o rubare dati dai database.
2. Violazioni dei dati: accesso non autorizzato ai dati sensibili dei clienti, che potrebbe derivare da attacchi esterni o interni.
3. Interruzioni del servizio: attacchi DDoS o errori di configurazione potrebbero rendere il software di gestione delle transazioni non disponibile, influenzando gravemente le operazioni dei clienti.
4. Leakage di informazioni tramite cloud: mancata configurazione adeguata o vulnerabilità nelle infrastrutture cloud potrebbero esporre dati sensibili.
5. Phishing e altre truffe mirate: attacchi mirati ai dipendenti per ottenere credenziali di accesso o altre informazioni sensibili.

PIANIFICAZIONE DELLE CONTROMISURE

Elaborazione delle strategie di mitigazione (Che cosa faremo al riguardo?)

1. Attacchi di iniezione SQL
    - Contromisure: implementazione di controlli di validazione dell'input rigorosi per tutte le applicazioni che interagiscono con il database. Utilizzo di prepared statements e ORM (Object-Relational Mapping) che riducono il rischio di iniezione SQL.
    - Formazione: corsi regolari per gli sviluppatori sull'importanza della sicurezza del codice e le migliori pratiche per prevenire iniezioni SQL.
2. Violazioni dei dati
    - Contromisure: criptazione dei dati sensibili sia a riposo che in transito. Adozione di una politica di accesso minimo necessario per limitare l'accesso ai dati sensibili solo agli utenti autorizzati.
    - Monitoraggio: implementazione di soluzioni avanzate di monitoraggio e rilevamento delle intrusioni per identificare e reagire rapidamente a potenziali violazioni dei dati.
3. Interruzioni del servizio
    - Contromisure: implementazione di architetture resilienti e ridondanti, utilizzando tecniche di bilanciamento del carico e failover automatico.
    - Pianificazione della continuità operativa: sviluppo di piani di continuità operativa e di disaster recovery che includano regolari test di ripristino.
4. Leakage di informazioni tramite cloud
    - Contromisure: miglioramento delle configurazioni di sicurezza del cloud, inclusa la revisione e l'hardening delle impostazioni di sicurezza. Utilizzo di servizi di sicurezza del cloud offerti dai provider per rafforzare la protezione.
    - Auditing: condurre regolarmente audit di sicurezza e assessment di conformità per le infrastrutture cloud.
5. Phishing e altre truffe mirate
    - Formazione: programmi di formazione sulla sicurezza informatica per tutti i dipendenti, focalizzati sulla consapevolezza del phishing e altre tecniche di ingegneria sociale.
    - Soluzioni di sicurezza email: implementazione di filtri anti-phishing avanzati e meccanismi di autenticazione degli email per ridurre il rischio di attacchi di phishing.

VALUTAZIONE DELLE CONTROMISURE

Analisi dell'efficacia delle contromisure implementate (Abbiamo fatto un buon lavoro?)

1. Revisione e Testing
    - Test di Penetrazione: eseguiamo regolarmente test di penetrazione per simulare attacchi contro i nostri sistemi, inclusi tentativi di iniezione SQL e attacchi di phishing. Questo aiuta a identificare e correggere le vulnerabilità prima che possano essere sfruttate.
    - Audit di Sicurezza: condurre audit di sicurezza interni e esterni per verificare la conformità con le politiche di sicurezza e le normative applicabili.
2. Monitoraggio e Risposta
    - Sistemi di Rilevamento delle Intrusioni: monitoriamo costantemente i nostri sistemi con strumenti di rilevamento delle intrusioni per catturare e rispondere a qualsiasi attività sospetta o non autorizzata.
    - Analisi dei Log: analizziamo regolarmente i log di sicurezza per identificare pattern insoliti che potrebbero indicare un tentativo di attacco o una violazione della sicurezza.
3. Feedback e Miglioramento Continuo
    - Raccolta di Feedback: otteniamo feedback dai team di sviluppo, dal personale IT e dalla direzione per capire come le misure di sicurezza influenzano il flusso di lavoro quotidiano e l'efficacia operativa.
    - Aggiornamento delle Politiche e delle Tecniche: aggiorniamo le nostre politiche di sicurezza e le tecniche di mitigazione basandoci sulle lezioni apprese dagli incidenti di sicurezza e dai risultati degli audit.
4. Valutazione dei Risultati
    - Metriche di Successo: definiamo chiare metriche di successo per ogni misura di sicurezza implementata, come il numero di attacchi bloccati, il tempo di risposta a incidenti e la riduzione degli incidenti di sicurezza nel tempo.
    - Report di Sicurezza: creiamo report periodici che riassumono l'efficacia delle contromisure, le aree di rischio rimanenti e le raccomandazioni per miglioramenti futuri.

RIPETIZIONE DEL PROCESSO E GAP ANALYSIS

Ripetizione del processo per ulteriori minacce

Ripetere il processo di modellizzazione delle minacce è fondamentale per mantenere la sicurezza dell'organizzazione aggiornata con le nuove minacce emergenti e i cambiamenti nei sistemi interni. Questo include:

- Aggiornamento continuo degli asset: rivedere e aggiornare l'elenco degli asset critici all'interno dell'organizzazione in risposta ai cambiamenti tecnologici o di business.
- Identificazione di nuove minacce: monitorare l'ambiente esterno per nuove minacce e aggiornare la nostra modellizzazione di conseguenza.
- Aggiornamento delle contromisure: adattare e potenziare le contromisure esistenti in base alle nuove informazioni e alle tecnologie emergenti.

Esecuzione di una gap analysis per identificare i punti di miglioramento

La gap analysis ci permette di confrontare lo stato attuale della sicurezza con uno stato desiderato e ideale, identificando così le aree che necessitano di miglioramenti. I passaggi principali includono:

- Valutazione delle misure esistenti: esaminare le misure di sicurezza attuali per determinare la loro efficacia e identificare eventuali carenze.
- Confronto con best practices e standard di settore: utilizzare standard come NIST SP 800-53 per confrontare le nostre pratiche con quelle consigliate a livello di settore.
- Identificazione di lacune: determinare le aree in cui le misure di sicurezza attuali non soddisfano gli standard desiderati o non coprono completamente le minacce identificate.
- Sviluppo di un piano di azione: creare un piano dettagliato per affrontare le lacune identificate, includendo scadenze, responsabilità e risorse necessarie.

UTILIZZO DEI CONTROLLI NIST SP 800-53 REV. 5

Per rafforzare ulteriormente la modellizzazione delle minacce e l'implementazione delle contromisure in EpiSec Solutions S.p.A., integreremo i controlli specificati nel NIST SP 800-53 Rev. 5. Questo standard fornisce un framework comprensivo per la gestione dei rischi e la sicurezza delle informazioni, che può essere adattato per soddisfare le esigenze specifiche di un'organizzazione.

Introduzione ai controlli NIST SP 800-53 Rev. 5

Il NIST SP 800-53 Rev. 5 offre un set di controlli di sicurezza organizzati in famiglie di controlli, come Access Control, Incident Response, e System and Communications Protection. Questi controlli sono progettati per essere applicabili a una varietà di tecnologie e ambienti operativi, fornendo una guida dettagliata per la protezione degli asset informativi.

Applicazione dei controlli NIST per migliorare la modellizzazione delle minacce

Per EpiSec Solutions S.p.A., applicheremo i seguenti controlli NIST per indirizzare specificamente le minacce identificate:

- AC-1 Access Control Policies and Procedures: implementazione di politiche di controllo degli accessi più rigide per proteggere i database dei clienti e le infrastrutture cloud.
- SI-3 Malicious Code Protection: installazione di software antivirus avanzato e sistemi di prevenzione delle intrusioni per difendere contro attacchi di iniezione SQL e malware.
- IR-4 Incident Response: sviluppo di un programma di risposta agli incidenti più robusto che includa procedure specifiche per rispondere rapidamente alle violazioni dei dati e alle interruzioni del servizio.
- CP-2 Contingency Planning: rafforzamento della pianificazione di continuità operativa e di disaster recovery per garantire che i servizi possano essere ripristinati rapidamente in caso di interruzioni maggiori.

Utilizzando questi controlli, EpiSec Solutions può non solo migliorare la propria sicurezza informatica, ma anche garantire una conformità più stretta con le normative di settore e internazionali.

Monitoraggio e valutazione continua

- CA-7 Continuous Monitoring: implementare il monitoraggio continuo delle misure di sicurezza per valutare la loro efficacia e fare aggiustamenti tempestivi basati su nuove minacce e vulnerabilità emergenti.

Questo approccio sistemico aiuta a garantire che la sicurezza di EpiSec Solutions sia mantenuta a un livello elevato e che l'organizzazione possa rapidamente adattarsi a nuovi sviluppi nel panorama delle minacce.

CONCLUSIONI

Sintesi dei risultati

- Identificazione degli Asset e delle Minacce: abbiamo identificato gli asset critici come il software di gestione delle transazioni, i database dei clienti e le infrastrutture cloud, e abbiamo delineato le minacce principali come gli attacchi di iniezione SQL, le violazioni dei dati e le interruzioni del servizio.
- Implementazione delle Contromisure: sono state implementate contromisure specifiche per ciascuna minaccia, comprese politiche di sicurezza rafforzate, sistemi di monitoraggio e risposta agli incidenti, e formazione continua per i dipendenti.
- Valutazione dell'Efficacia: le contromisure sono state valutate attraverso test di penetrazione, audit di sicurezza e monitoraggio continuo, dimostrando una riduzione significativa delle vulnerabilità e un miglioramento nella capacità di risposta agli incidenti.
- Gap Analysis e Miglioramenti: la gap analysis ha rivelato aree di miglioramento, che sono state affrontate con aggiornamenti alle politiche e alle tecnologie di sicurezza, basati sui controlli del NIST.

Punti di azione futuri

1. Monitoraggio Continuo: continuare a monitorare l'efficacia delle contromisure di sicurezza e fare aggiustamenti in risposta a nuove minacce e cambiamenti tecnologici.
2. Formazione e Consapevolezza: mantenere un programma di formazione regolare per i dipendenti per rafforzare la consapevolezza delle minacce e delle pratiche di sicurezza.
3. Revisione e Aggiornamento dei Controlli di Sicurezza: rivedere periodicamente i controlli di sicurezza in linea con il NIST SP 800-53 per assicurarsi che siano aggiornati e adeguatamente rigorosi.
4. Collaborazione e Condivisione delle Informazioni: promuovere la collaborazione tra i team interni e la condivisione delle informazioni su minacce e vulnerabilità per migliorare la sicurezza complessiva.

GRAZIE

MARIA HUAPAYA