EPICODE

GRUPPO BCC ICCREA

S4_L5_Authorization_Packet

Gestione del rischio informatico per un caso aziendale specifico

23 maggio 2024

Team

- Davide Di Turo
- Lisa Bonato
- Manuel Di Gangi
- Maria Flavia Minotti
- Oliviero Camarota

Con la presente, desideriamo sottoporre alla sua attenzione il pacchetto di autorizzazione relativo all'implementazione dei controlli di sicurezza per il nostro sistema informativo, conformemente ai requisiti di sicurezza e privacy dell'organizzazione.

Il pacchetto include una dettagliata valutazione dei controlli implementati per i seguenti aspetti critici della sicurezza:

SOMMARIO

SC-05 Denial of Service Protection:

Descrizione del controllo e degli obiettivi.

Implementazione di contromisure per proteggere i servizi, le risorse e i sistemi informativi dagli attacchi di denial of service (DoS) e distributed denial of service (DDoS), inclusa l'adozione di tecnologie e politiche per rilevare, mitigare e rispondere tempestivamente agli attacchi al fine di garantire la disponibilità continua dei servizi e delle risorse digitali.

Per il report di valutazione che dimostra l'implementazione corretta delle contromisure contro gli attacchi DoS/DDoS si fa riferimento al file ***S4_L4_Assesment_Report.pdf****.*

Raccomandazioni per migliorare ulteriormente la protezione contro tali minacce

Filtri IP e Geo-blocking*: Configura filtri IP per bloccare il traffico proveniente da indirizzi IP noti per essere fonti di attacchi DDoS. Inoltre, considera l'implementazione di blocchi geografici per limitare il traffico proveniente da regioni o paesi noti per essere fonti di attacchi.*

Utilizzo di CDN (Content Delivery Network)*: Utilizza un CDN per distribuire il carico di traffico su una vasta rete di server. Questo può aiutare a mitigare gli effetti di un attacco DDoS distribuendo il traffico su una vasta rete anziché concentrarsi su un singolo server.*

Mitigazione DDoS basata su Cloud: *Considera l'utilizzo di servizi di mitigazione DDoS basati su cloud che possono filtrare il traffico malevolo prima che raggiunga la tua infrastruttura.*

Pianificazione di Risposta agli Incidenti: *Sviluppa un piano di risposta agli incidenti DDoS che delinei le azioni da intraprendere in caso di attacco, inclusi i ruoli e le responsabilità del personale coinvolto.*

SC-07 Boundary Protection:

Descrizione del controllo e degli obiettivi.

Implementazione di misure di sicurezza per proteggere i confini della rete da accessi non autorizzati o compromessi. Questo controllo è fondamentale per garantire che le reti dell'organizzazione siano adeguatamente protette da minacce esterne e che solo le comunicazioni autorizzate possano attraversare i confini della rete.

Per il report di valutazione che dimostra l'implementazione corretta delle misure di difesa perimetrali ed interne alla rete aziendale si fa riferimento al file ***S4_L4_Assesment_Report.pdf****.*

Analisi dei rischi associati

Interruzione delle operazioni critiche: Un'interruzione delle operazioni critiche può derivare da eventi imprevisti come catastrofi naturali, guasti hardware, attacchi informatici o errori umani.

Perdita di dati critici: In caso di incidente, potrebbe verificarsi la perdita di dati critici necessari per le operazioni aziendali o la conformità normativa.

Downtime dei sistemi critici: Il downtime prolungato dei sistemi critici può causare perdite finanziarie significative, danneggiare la reputazione dell'azienda e compromettere la soddisfazione del cliente.

Violazione della conformità normativa: Una perdita di continuità operativa può portare a violazioni delle normative settoriali o delle leggi sulla privacy dei dati, con conseguenti sanzioni legali e reputazionali.

Strategie di mitigazione.

Pianificazione della continuità operativa (BCP):

Sviluppare e implementare un piano di continuità operativa (BCP) dettagliato che identifichi le operazioni critiche, le risorse necessarie e i protocolli di ripristino.

Condurre regolarmente esercitazioni e test di simulazione per valutare l'efficacia del BCP e identificare eventuali aree di miglioramento.

Backup e ripristino dei dati:

Implementare una politica di backup dei dati regolare e affidabile per garantire la disponibilità e l'integrità dei dati critici.

Archiviare i backup in luoghi sicuri e remoti per proteggerli da eventi catastrofici che potrebbero colpire il sito principale.

Ridondanza e tolleranza ai guasti:

Implementare sistemi ridondanti e tolleranti ai guasti per i componenti critici dell'infrastruttura IT, come server, storage e reti.

Utilizzare servizi cloud e infrastrutture distribuite per migliorare la resilienza e la disponibilità dei servizi aziendali.

Gestione del rischio:

Condurre valutazioni periodiche del rischio per identificare le minacce emergenti e valutare l'impatto potenziale sugli obiettivi aziendali.

Implementare controlli di sicurezza proporzionati al livello di rischio e alle esigenze operative dell'organizzazione.

Formazione e sensibilizzazione del personale:

Fornire formazione e consapevolezza al personale sull'importanza della continuità operativa e sulle procedure da seguire in caso di emergenza.

Designare e addestrare un team di risposta alle emergenze per coordinare le attività di ripristino durante un'incidenza.

Monitoraggio e risposta agli incidenti:

Implementare sistemi di monitoraggio continuo per rilevare tempestivamente gli eventi che potrebbero influenzare la continuità operativa.

Stabilire procedure di risposta agli incidenti per gestire prontamente le emergenze e mitigare gli impatti sulle operazioni aziendali.

AC-02 Account Management:

Descrizione del controllo e degli obiettivi.

Il sistema di gestione degli account è implementato per garantire che solo individui autorizzati abbiano accesso ai sistemi e alle informazioni dell'organizzazione.

Per il report di valutazione che attesta l'efficacia del sistema di gestione degli accessi si fa riferimento al file ***S4_L4_Assesment_Report.pdf****.*

Procedure per l'identificazione

Creazione di Identità Utente:

Assegna un'identità univoca a ciascun utente del sistema. Questo può includere l'assegnazione di nomi utente, password e altri attributi identificativi.

Autenticazione Utente:

Implementa un sistema di autenticazione robusto per verificare l'identità degli utenti al momento dell'accesso al sistema. Questo può includere l'uso di password, biometria, token OTP (One-Time Password) o altre forme di autenticazione multi-fattore (MFA).

Autorizzazione Utente:

Definisci i privilegi di accesso per ciascun utente in base al loro ruolo e alle loro responsabilità all'interno dell'organizzazione. Questo può includere l'assegnazione di permessi di lettura, scrittura, esecuzione e amministrazione per risorse specifiche.

Monitoraggio degli Accessi:

Implementa sistemi di logging e monitoraggio per registrare e tracciare tutte le attività di accesso degli utenti al sistema. Questo consente di individuare e investigare accessi non autorizzati o comportamenti sospetti.

Controllo degli accessi al sistema.

Politiche di Accesso:

Definisci politiche di accesso chiare e applicabili che regolano l'accesso alle risorse del sistema. Queste politiche dovrebbero essere documentate e comunicate a tutto il personale.

Gestione delle Password:

Implementa politiche robuste per la gestione delle password, comprese le regole di complessità delle password, la scadenza delle password e il divieto di condivisione delle password. Inoltre, incoraggia l'uso di password univoche e sicure per ciascun utente.

Controllo degli Accessi Basato sui Ruoli (RBAC):

Utilizza il modello di controllo degli accessi basato sui ruoli per semplificare la gestione degli accessi e garantire che gli utenti ottengano solo i privilegi di cui hanno bisogno per svolgere le proprie funzioni lavorative.

Revisione Periodica degli Accessi:

Conduci revisioni regolari degli accessi per garantire che gli utenti mantengano solo i privilegi di accesso necessari per svolgere il loro lavoro. Rimuovi immediatamente gli accessi non più necessari o non autorizzati.

Autenticazione a Più Fattori (MFA):

Implementa l'autenticazione a più fattori per aumentare la sicurezza degli accessi al sistema. Richiedi agli utenti di fornire più di un metodo di autenticazione, come password e token OTP, per accedere alle risorse sensibili.

Limitazione degli Accessi:

Applica regole di controllo degli accessi per limitare l'accesso a risorse specifiche in base al principio del bisogno di sapere. Assicurati che gli utenti possano accedere solo alle risorse necessarie per svolgere le proprie responsabilità lavorative.

Monitoraggio Continuo degli Accessi:

Implementa sistemi di monitoraggio continuo degli accessi per rilevare e rispondere tempestivamente a comportamenti anomali o tentativi di accesso non autorizzati.

RA-03 Risk Assessment:

Descrizione del controllo e degli obiettivi.

La valutazione periodica dei controlli di sicurezza è effettuata per identificare e mitigare le vulnerabilità, comprese quelle relative alla privacy.

Per il report di valutazione che attesta l'efficacia del sistema di gestione degli accessi si fa riferimento al file ***S4_L4_Assesment_Report.pdf****.*

Raccomandazioni per migliorare il processo di valutazione dei rischi.

Ecco alcune raccomandazioni per migliorare il processo di valutazione dei rischi:

Coinvolgimento di Stakeholder Chiave:

Assicurarsi di coinvolgere tutti gli stakeholder chiave nel processo di valutazione dei rischi, inclusi membri del team di sicurezza, responsabili IT, dirigenti e rappresentanti delle varie funzioni aziendali. Questo assicura una visione completa delle minacce e dei rischi per l'intera organizzazione.

Aggiornamento Periodico della Valutazione dei Rischi:

La valutazione dei rischi non dovrebbe essere un evento unico, ma un processo continuo e in evoluzione. Aggiornare regolarmente la valutazione dei rischi per riflettere i cambiamenti nell'ambiente operativo, nelle minacce emergenti e nelle tecnologie.

Utilizzo di Metodologie Standard:

Utilizzare metodologie standardizzate e riconosciute per la valutazione dei rischi, come ISO 27005, NIST SP 800-30 o OCTAVE. Queste metodologie forniscono un approccio strutturato e completo alla valutazione dei rischi.

Identificazione delle Minacce e delle Vulnerabilità:

Effettuare una rigorosa identificazione delle minacce e delle vulnerabilità che potrebbero mettere a rischio l'organizzazione. Questo include minacce interne ed esterne, vulnerabilità tecnologiche, errori umani e fattori ambientali.

Valutazione dell'Impatto:

Valutare l'effettivo impatto che le minacce potrebbero avere sull'organizzazione, inclusi i costi finanziari, la perdita di dati sensibili, la reputazione aziendale e la continuità operativa.

Prioritizzazione dei Rischi:

Classificare e priorizzare i rischi in base alla loro gravità e alla probabilità di accadimento. Concentrare gli sforzi sulle minacce più critiche e sulle vulnerabilità più significative che potrebbero causare danni maggiori all'organizzazione.

Sviluppo di Piani di Mitigazione:

Sviluppare piani di mitigazione chiari e specifici per affrontare i rischi identificati. Questi piani dovrebbero includere azioni concrete per ridurre o eliminare le vulnerabilità, nonché procedure per la risposta agli incidenti in caso di violazione della sicurezza.

Monitoraggio Continuo e Valutazione delle Misure di Mitigazione:

Implementare un processo di monitoraggio continuo per valutare l'efficacia delle misure di mitigazione e identificare eventuali cambiamenti nell'ambiente dei rischi. Questo consente un adattamento tempestivo delle strategie di sicurezza.

Formazione e Consapevolezza:

Fornire formazione e sensibilizzazione al personale sull'importanza della gestione dei rischi e sulle migliori pratiche di sicurezza informatica. Un personale ben informato è fondamentale per identificare e mitigare i rischi in modo proattivo.

Revisione da Parte di Esperti Esterni:

Considerare la possibilità di coinvolgere esperti esterni o consulenti per condurre una revisione indipendente del processo di valutazione dei rischi. Questo può portare a nuove prospettive e miglioramenti significativi nel processo.

SC-13 Use of Cryptography:

Descrizione del controllo e degli obiettivi.

L'organizzazione implementa la protezione fornita dalla crittografia in conformità alle leggi federali, ordini esecutivi, direttive, politiche normative, standard e linee guida pertinenti.

*Per il report di valutazione che verifica l'implementazione corretta e sicura della crittografia si fa riferimento al file **S4_L4_Assesment_Report.pdf**.*

SC-28 Protection of Information at Rest:

Descrizione del controllo e degli obiettivi.

Implementare la crittografia corretta e sicura per proteggere le informazioni sensibili e le comunicazioni da accessi non autorizzati o compromessi quando i dati sono a riposo.

Per il report sull'implementazione della crittografia per proteggere i dati a riposo si fa riferimento al file ***S4_L4_Assesment_Report.pdf****.*

Chiediamo rispettosamente la sua autorizzazione per la piena implementazione dei controlli sopra descritti, al fine di garantire la sicurezza e la protezione dei nostri sistemi informativi e delle informazioni sensibili dell'organizzazione.