Progetto S3L5

Gestione del rischio informatico in un contesto aziendale

Marco D'Antoni
Marco Fasani
Manuel Di Gangi
Guglielmo Carratello
Oliviero Camarota
Mattia Chiriatti

Traccia

La settimana scorsa abbiamo visto come strutturare il Risk Assessment NIST SP 800-30, che è utilizzato in diversi punti del NIST RMF SP 800-37 che a sua volta è una componente del NIST CSF 2.0 CSWP 29. In questo progetto andremo a sviluppare uno dei documenti fondamentali per la gestione del rischio:
• Politica di gestione del rischio: questo documento definisce gli obiettivi, i principi e le linee guida generali per la gestione dei rischi all'interno dell'organizzazione.

Scenario
FinCompany è un'importante istituzione finanziaria che offre servizi bancari tradizionali e digitali. Opera in diversi paesi con una vasta rete di filiali fisiche e sistemi informatici interconnessi.

Questi sistemi includono:
• Sistema bancario core per l'elaborazione di transazioni, gestione dei conti e servizi ai clienti
• Applicazioni bancarie online/mobile per l'online banking dei clienti
• Rete aziendale per operazioni interne, comunicazioni e gestione dei dati
• Infrastruttura di sicurezza come firewall, IDS/IPS, autenticazione, crittografia

Essendo un'istituzione finanziaria, gestisce dati altamente sensibili come informazioni finanziarie, identificative e di transazione dei clienti. È fondamentale proteggere questi sistemi e dati da minacce informatiche come attacchi di malware, accesso non autorizzato, furto di dati e interruzioni del servizio.
Scegliete uno o più step (in base alla numerosità del vostro gruppo) del NIST RMF, per ogni task degli step selezionati, definite la politica di gestione del rischio (basta una piccola descrizione) in linea con lo scenario organizzativo proposto, individuando nello specifico se il RA è utilizzato in quella attività e come.
Non va implementato il RA ma vanno definiti solo delle linee guida o dei principi (gli obiettivi sono un plus), su argomenti come:

• Ruoli, responsabilità, processi decisionali e requisiti di segnalazione per la gestione dei rischi.
• Metodologie e criteri per identificare, analizzare e valutare i rischi informatici, tenendo conto di minacce, vulnerabilità, probabilità e impatti.
• Procedure per selezionare, implementare e mantenere i controlli tecnici, operativi e gestionali per mitigare i rischi identificati.
• Processi di test, valutazione e autorizzazione per garantire che i sistemi soddisfino i requisiti di sicurezza e abbiano un livello di rischio accettabile.
• Procedure per monitorare continuamente i controlli di sicurezza, rilevare e rispondere agli eventi di sicurezza e mantenere un livello di rischio accettabile.
• Controlli e requisiti per proteggere la riservatezza, l'integrità e la disponibilità dei dati dei clienti. Formazione e consapevolezza
• Piani per formare e sensibilizzare il personale e gli utenti finali sui rischi informatici e le pratiche di sicurezza.
• Processi di risposta agli incidenti, contenimento, indagine, ripristino e comunicazione per fronteggiare efficacemente le violazioni di sicurezza.
• Cadenze e modalità per la revisione e il reporting della posizione di rischio dell'organizzazione ai dirigenti e alle parti interessate.
• Requisiti di sicurezza per le relazioni con i fornitori e l'approvvigionamento di servizi e tecnologie.

TASK	RESPONSIBLE	POLICY	RA USAGE	GOALS
S-4 Documentation of Planned Control Implementations	System Owner, Common Control Provider	I piani di sicurezza e privacy contengono una panoramica dei requisiti di sicurezza e privacy per il sistema e i controlli selezionati per soddisfarne i requisiti. I piani descrivono l'applicazione prevista di ciascun controllo selezionato nel contesto del sistema con un livello di dettaglio sufficiente per implementare correttamente il controllo e per valutare l'efficacia dello stesso. Non è necessario, inoltre, fornire dettagli di implementazione per i controlli comuni. Tali dettagli sono forniti nei piani per i fornitori di controlli comuni e sono resi disponibili ai proprietari dei sistemi.	L'approccio di selezione dei controlli generati dall'organizzazione può differire dall'approccio indicato dalla normativa, in quanto si hanno due metodi per l'elaborazione di questa documentazione. Piuttosto, l'organizzazione utilizza il proprio processo di RA per selezionare i controlli più idonei, scegliere i metodi di valutazione e i controlli susseguenti.	Elaborare una documentazione che permetta all'organizzazione di monitorare a 360° l'efficacia e l'efficienza dell'implementazione di controlli esistenti o nuovi.
R-5 Authorization Reporting	Authorizing Official (AO) or Authorizing Official Designated Representative	Reportare le decisioni di autorizzazione e le carenze nei controlli che rappresentano rischi significativi per la sicurezza o la privacy.	Utilizzare il RA per identificare e valutare le carenze nei controlli e determinare l'impatto delle decisioni di autorizzazione.	Garantire la trasparenza nelle decisioni di autorizzazione; Identificare e segnalare tempestivamente le carenze nei controlli; Supportare il miglioramento continuo dei controlli di sicurezza; Assicurare la conformità normativa e la protezione dei dati sensibili
S-1 Selezionare i controlli per il sistema e l'ambiente di funzionamento.	System Owner, Common Control Provider	Lo scopo del Selectstep è selezionare, personalizzare e documentare i controlli necessari per la protezione il sistema informativo e l'organizzazione siano commisurati al rischio per le operazioni organizzative e beni, individui, altre organizzazioni e la Nazione.	L'approccio di selezione dei controlli generati dall'organizzazione differisce dall'approccio di selezione di base perché l'organizzazione non inizia con un insieme di controlli predefinito. Piuttosto, l'organizzazione utilizza il proprio processo di RA per selezionare i controlli più idonei.	Identificare i controlli di sicurezza e privacy appropriati, Adattare i controlli alle esigenze specifiche dell'organizzazione, Incorporare i controlli nel ciclo di vita del sistema, Garantire la conformità e la responsabilità
C-2 Security Categorization	System Owner Information Owner or Steward	La politica richiede che le decisioni di categorizzazione della sicurezza considerino gli impatti negativi potenziali sulle operazioni organizzative, sugli asset organizzativi, sugli individui, su altre organizzazioni e sulla Nazione derivanti dalla perdita di confidenzialità, integrità o disponibilità delle informazioni.	Il processo di categorizzazione della sicurezza utilizza i risultati delle valutazioni dei rischi di sicurezza (e delle valutazioni dei rischi sulla privacy quando il sistema elabora informazioni personalmente identificabili). Questi risultati influenzano la decisione di categorizzazione della sicurezza e sono coerenti con la strategia di gestione del rischio dell'organizzazione.	Determinare gli impatti; Categorizzare la sicurezza; Documentare i risultati; Facilitare la prioritizzazione
R-3 Risk response	Authorizing Official or Authorizing Official Designated Representative	Gestione delle risposte al rischio all'interno delle organizzazioni. Le azioni di mitigazione pianificate vengono incluse e monitorate tramite un piano d'azione. Una volta mitigati, vengono riesaminati i controlli per verificare che siano implementati correttamente e producano i risultati desiderati.	Fornisce le linee guida fondamentali per condurre un'analisi dei rischi efficace e per assicurare che le risposte ai rischi siano coerenti con le politiche e gli obiettivi dell'organizzazione.	Identificare e implementare una linea d'azione preferita in risposta al rischio determinato.
R-2 Analyze and determine the risk from the operation or use of the system or the provision of common controls	Authorizing Official or Authorizing Official Designated Representative	la gestione dei rischi derivanti dall'operazione, dall'uso del sistema o dalla fornitura di controlli comuni. Si applica sia ai nuovi sistemi durante la fase di implementazione e valutazione, sia ai sistemi esistenti durante le operazioni e la manutenzione.	l'analisi del rischio viene utilizzata come parte del processo decisionale per determinare i potenziali rischi derivanti dalle operazioni	Analisi accurata del rischio; Determinazione del rischio; Collaborazione interfunzionale; Documentazione accurata; Valutazione continua del rischio