CONSEGNA 30 APRILE S2L1

Traccia

Un'azienda di servizi finanziari gestisce un'applicazione web che consente ai clienti di accedere ai propri account e effettuare transazioni finanziarie online. L'applicazione web memorizza e gestisce dati sensibili dei clienti, come informazioni personali, dettagli finanziari e credenziali di accesso. Il rischio principale è rappresentato da potenziali attacchi informatici volti a compromettere la sicurezza dell'applicazione web e a ottenere l'accesso non autorizzato ai dati dei clienti. Supponendo di aver già effettuato l'analisi del rischio per lo scenario identificato, l'azienda decide di non accettare il rischio e procedere con la mitigazione del rischio applicando degli ulteriori controlli.
Utilizzando NIST SP 800-53, seleziona 5 controlli, uno per ogni funzione di controllo (Deterrent, Preventive, Detective, Corrective, Compensating) e stabilisci come agisce il controllo sul rischio (può essere anche una combinazione):

- diminuendo la probabilità che un threat agent avvii una minaccia;
- diminuendo la probabilità che una minaccia sfrutti una vulnerabilità;
- diminuendo la vulnerabilità;
- diminuendo l'impatto se la minaccia riesce a sfruttare la vulnerabilità;

Indice

1 - Scenario del rischio

L'azienda in analisi si occupa di servizi finanziari e gestisce un'applicazione web che consente ai clienti di accedere ai propri account e effettuare transazioni finanziarie online. L'applicazione web memorizza e gestisce dati sensibili dei clienti, come:

- Informazioni personali
- Dettagli finanziari
- Credenziali di accesso

Il rischio principale è rappresentato da potenziali attacchi informatici volti a compromettere la sicurezza dell'applicazione web e ottenere l'accesso non autorizzato ai dati dei clienti

1.1 - Rischio da trattare

In questo scenario, un rischio importante da considerare è il "**SQL Injection**". Questo tipo di attacco avviene quando un malintenzionato inserisce o "inietta" un codice SQL malevolo nei moduli di input previsti per interagire con il database dell'applicazione web. Un attacco di SQL Injection può permettere a un attaccante di visualizzare, modificare o eliminare dati sensibili, compromettendo così l'integrità e la riservatezza dei dati dei clienti.

2 - Trattamento del rischio

A fronte di un processo di selezione e implementazione di misure per la modifica del rischio individuato, l'azienda ha deciso di non accettare il rischio e procedere con la mitigazione del rischio applicando degli ulteriori controlli.

Importante sottolineare che il trattamento del rischio non deve solamente ridurre il rischio ma deve soddisfare le esigenze dell'organizzazione, la mission, gli obbiettivi aziendali e la strategia organizzativa.
Ne concludiamo quindi che il trattamento del rischio individuato deve diminuire il rischio senza impattare negativamente sui processi aziendali.

2.1 - Mditigazione del rischio

Andremo a trattare il rischio di SQL Injection attraverso l'uso di contromisure e controlli, un insieme di attività che possono minimizzare la probabilità o l'impatto del rischio. Andremmo quindi a modificare il livello di rischio aggiungendo nuovi controlli o migliorando quelli esistenti.

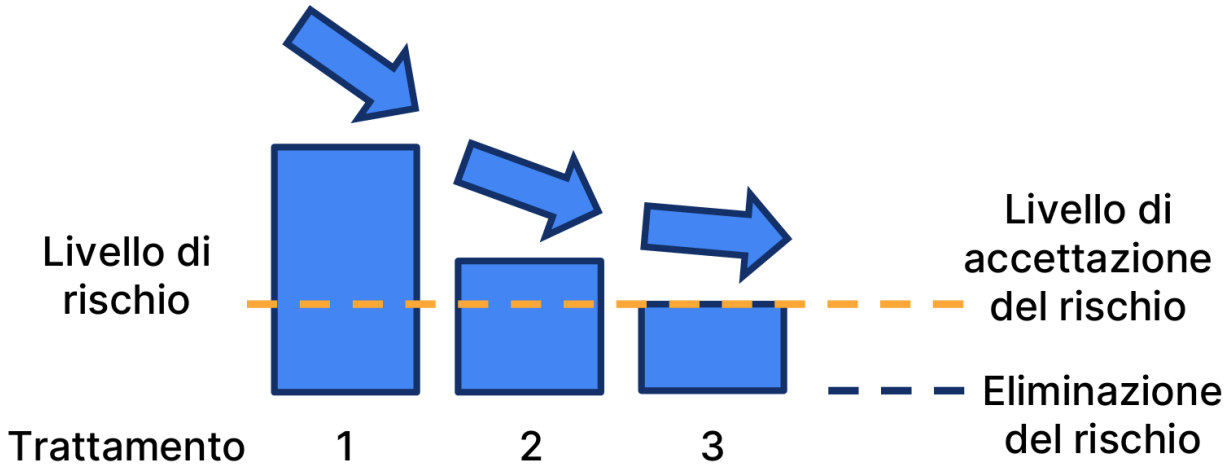


Fig.1 - Mitigazione del rischio di SQL Injection

2.2 - Valutazione del trattamento

Prima di procedere con il trattamento del rischio, è fondamentale valutare le diverse opzioni di trattamento, in modo da trovare il giusto equilibrio rischio/beneficio.

Alcuni elementi che prenderemo in considerazione sono:

- Costi ed efficacia: I controlli che andremmo ad effettuare saranno efficaci per il costo, che dovrà essere minore del rischio. Andremo a applicare i controlli più facili che ridurranno il rischio ad un livelli accettabile
- Contesto organizzativo: Abbiamo valutato che i controlli che useremo rientrano nel budget in termini di risorse, altresì importante è l'influenza che la struttura ha sul trattamento.
- Governance: Abbiamo controllato i requisiti legali e normativi, andando ad implementare dei controlli tollerati dalla nostra governance.
- Cultura: Abbiamo anche valutato l'influenza che la cultura aziendale ha sul trattamento, appurando che non ci sono resistenze nell'introduzione dei nuovi controlli.

3 - Controlli

I controlli che andremo ad implementare ci serviranno a proteggere le risorse dell'organizzazione, ridurre il rischio ed assicurare la conformità.

3.1 - Funzioni di controllo

Ora andremmo ad applicare 5 controlli, con 5 funzioni diverse , al rischio appena individuato, appoggiandoci alle pubblicazione ufficiale NIST SP 800-53 Rev. 5

Controllo deterrente - **PL-4** (Rules of behaviour)

- **Descrizione**: Stabilisce le regole comportamentali per gli utenti del sistema, specificando le responsabilità e le conseguenze in caso di mancato rispetto.
- **Applicazione**: Implementare e comunicare chiaramente politiche che specifichino le conseguenze severe per i tentativi di sfruttamento dei sistemi, inclusi gli attacchi di SQL Injection. Questo può includere penalità disciplinari, terminazione dell'accesso al sistema, e azioni legali contro gli individui responsabili di tali attività non autorizzate.

Come Agisce il Controllo

Questo tipo di controllo deterrente agisce influenzando il comportamento degli utenti attraverso la consapevolezza delle severe conseguenze legali e disciplinari che derivano dal tentativo di compromettere la sicurezza del sistema. L'obiettivo è prevenire atti deliberati di abuso o sperimentazione non autorizzata che potrebbero portare a una violazione di sicurezza tramite SQL Injection.

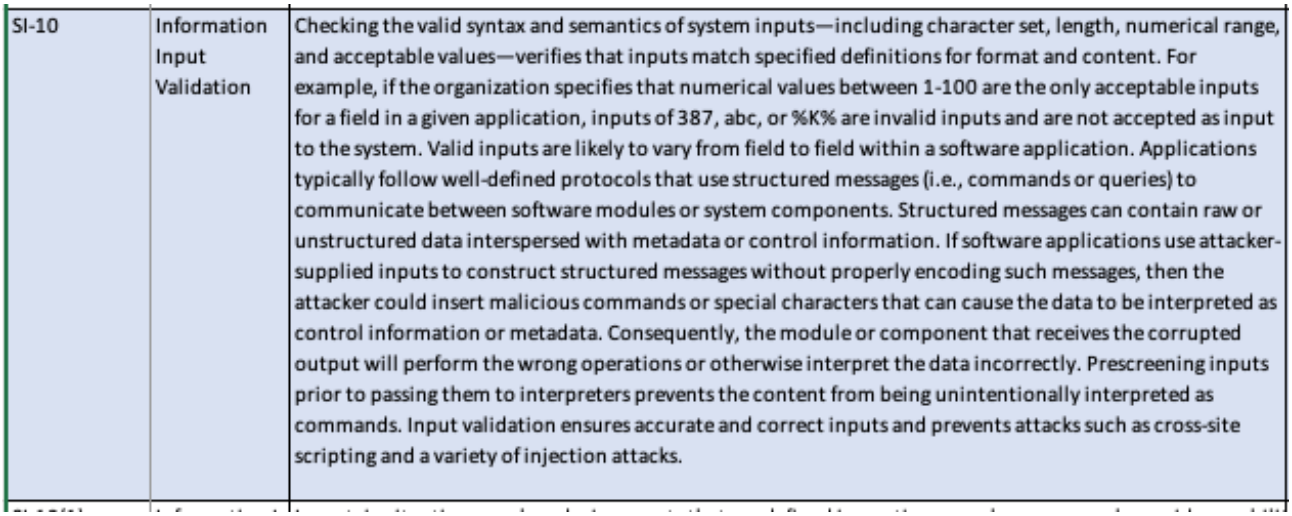
PL-4	Rules of Behavior	a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy; b. Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system; c. Review and update the rules of behavior [Assignment: organization-defined frequency]; and d. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge [Selection (one or more): [Assignment: organization-defined frequency]; when the rules are revised or updated].

Controllo preventivo - **SI-10** (Information Input Validation)

- **Descrizione**: Stabilisce che il sistema deve validare l'input dell'informazione da parte degli utenti per garantire che sia conforme ai criteri specificati prima di essere elaborato.
- **Applicazione**: Assicurarsi che tutte le entrate di dati provenienti dagli utenti siano sottoposte a controlli rigorosi di validazione. Questo include l'uso di liste di controllo (whitelists) per i caratteri permessi nelle stringhe di input, la verifica che gli input non contengano comandi SQL o parti di essi, e l'impiego di prepared statements o query parametrizzate per interagire con il database. Questo approccio impedisce l'esecuzione di parti dell'input come codice SQL, bloccando così le iniezioni SQL prima che possano causare danni.

Come Agisce il Controllo

Il controllo SI-10 agisce creando una barriera tra gli input dell'utente e il sistema di elaborazione del database. Attraverso la validazione rigorosa degli input, il sistema previene l'interpretazione di parti dell'input come codice eseguibile, eliminando la possibilità che un attaccante possa modificare la logica delle query SQL. Questo non solo impedisce gli attacchi di SQL Injection ma migliora anche la stabilità e l'affidabilità dell'applicazione, assicurando che solo dati appropriati siano processati e immagazzinati.



SI-10	Information Input Validation	Checking the valid syntax and semantics of system inputs—including character set, length, numerical range, and acceptable values—verifies that inputs match specified definitions for format and content. For example, if the organization specifies that numerical values between 1-100 are the only acceptable inputs for a field in a given application, inputs of 387, abc, or %K% are invalid inputs and are not accepted as input to the system. Valid inputs are likely to vary from field to field within a software application. Applications typically follow well-defined protocols that use structured messages (i.e., commands or queries) to communicate between software modules or system components. Structured messages can contain raw or unstructured data interspersed with metadata or control information. If software applications use attacker-supplied inputs to construct structured messages without properly encoding such messages, then the attacker could insert malicious commands or special characters that can cause the data to be interpreted as control information or metadata. Consequently, the module or component that receives the corrupted output will perform the wrong operations or otherwise interpret the data incorrectly. Prescreening inputs prior to passing them to interpreters prevents the content from being unintentionally interpreted as commands. Input validation ensures accurate and correct inputs and prevents attacks such as cross-site scripting and a variety of injection attacks.

Controllo detective - **SI-4** (Information System)

- **Descrizione**: Richiede il monitoraggio continuo del sistema informativo per rilevare attività non autorizzate o anomale.
- **Applicazione**: Implementare sistemi di monitoraggio che tracciano e analizzano continuamente le query e le transazioni del database per individuare schemi insoliti o comandi SQL che potrebbero indicare un tentativo di SQL Injection. Questo può includere l'uso di strumenti di analisi dei log, intrusion detection systems (IDS), o security information and event management (SIEM) systems che generano allarmi in tempo reale quando vengono rilevate attività sospette.

Come Agisce il Controllo

Il controllo SI-4 agisce raccogliendo e analizzando i dati generati dalle interazioni degli utenti con il sistema. Monitorando attivamente questi dati, è possibile rilevare deviazioni dai comportamenti normali, come l'inserimento di sequenze di caratteri che sono comuni nelle iniezioni SQL. Una volta rilevato un tentativo, il sistema può avvisare gli amministratori di sicurezza, che possono quindi intervenire per indagare e mitigare ulteriormente l'incidente. Questo tipo di controllo non solo aiuta a identificare gli attacchi in corso, ma può anche fornire informazioni preziose per prevenire futuri tentativi di violazione.

SI-4	System Monitoring	System monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at external interfaces to the system. Internal monitoring includes the observation of events occurring within the system. Organizations monitor systems by observing audit activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives guide and inform the determination of the events. System monitoring capabilities are achieved through a variety of tools and techniques, including intrusion detection and prevention systems, malicious code protection software, scanning tools, audit record monitoring software, and network monitoring software. Depending on the security architecture, the distribution and configuration of monitoring devices may impact throughput at key internal and external boundaries as well as at other locations across a network due to the introduction of network throughput latency. If throughput management is needed, such devices are strategically located and deployed as part of an established organization-wide security architecture. Strategic locations for monitoring devices include selected perimeter locations and near key servers and server farms that support critical applications. Monitoring devices are typically employed at the managed interfaces associated with controls SC-7 and AC-17. The information collected is a function of the organizational monitoring objectives and the capability of systems to support such objectives. Specific types of transactions of interest include Hypertext Transfer Protocol (HTTP) traffic that bypasses HTTP proxies. System monitoring is an integral part of organizational continuous monitoring and incident response programs, and output from system monitoring serves as input to those programs. System monitoring requirements, including the need for specific types of system monitoring, may be referenced in other controls (e.g., AC-2g, AC-2(7), AC-2(12)(a), AC-17(1), AU-13, AU-13(1), AU-13(2), CM-3f, CM-6d, MA-3a, MA-4a, SC-5(3)(b), SC-7a, SC-7(24)(b), SC-18b, SC-43b). Adjustments to levels of system monitoring are based on law enforcement information, intelligence information, or other sources of information. The legality of system monitoring activities is based on applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Controllo correttivo - **IR-4** (Incident Handling)

- **Descrizione**: Stabilisce politiche e procedure per la gestione degli incidenti di sicurezza che impattano le informazioni o i sistemi informativi.
- **Applicazione**: Definire procedure specifiche per la risposta agli incidenti di SQL Injection, che includono l'isolamento delle aree del sistema interessate, la rimozione dell'accesso all'attaccante, l'analisi delle tecniche di attacco utilizzate, e la correzione delle vulnerabilità sfruttate. Questo può anche coinvolgere la reversibilità delle modifiche non autorizzate e la notifica agli stakeholder interessati.

Come Agisce il Controllo

Il controllo IR-4 agisce fornendo un framework strutturato per affrontare e risolvere gli incidenti di sicurezza dopo che sono stati rilevati. Nel contesto di un attacco di SQL Injection, questo controllo aiuta a minimizzare l'impatto dell'attacco attraverso un intervento rapido e mirato. Le azioni correttive possono includere la revoca delle modifiche dannose, la riparazione delle vulnerabilità che hanno permesso l'attacco, e la restaurazione dei dati compromessi. Inoltre, le lezioni apprese durante la gestione dell'incidente possono contribuire a rafforzare le misure di sicurezza e prevenire incidenti futuri.

IR-4	Incident Handling	Organizations recognize that incident response capabilities are dependent on the capabilities of organizational systems and the mission and business processes being supported by those systems. Organizations consider incident response as part of the definition, design, and development of mission and business processes and systems. Incident-related information can be obtained from a variety of sources, including audit monitoring, physical access monitoring, and network monitoring; user or administrator reports; and reported supply chain events. An effective incident handling capability includes coordination among many organizational entities (e.g., mission or business owners, system owners, authorizing officials, human resources offices, physical security offices, personnel security offices, legal departments, risk executive [function], operations personnel, procurement offices). Suspected security incidents include the receipt of suspicious email communications that can contain malicious code. Suspected supply chain incidents include the insertion of counterfeit hardware or malicious code into organizational systems or system components. For federal agencies, an incident that involves personally identifiable information is considered a breach. A breach results in unauthorized disclosure, the loss of control, unauthorized acquisition, compromise, or a similar occurrence where a person other than an authorized user accesses or potentially accesses personally identifiable information or an authorized user accesses or potentially accesses such information for other than authorized purposes.

Controllo di compensazione - **CP-2** (Contingency Plan)

- **Descrizione**: Prevede la preparazione e il mantenimento di piani di contingenza per garantire la continuità delle operazioni in caso di interruzione del servizio o di incidenti di sicurezza.
- **Applicazione**: Nel contesto di un attacco di SQL Injection, un piano di contingenza ben preparato può prevedere misure specifiche per il ripristino rapido dei servizi critici del database, minimizzando l'interruzione delle operazioni di business.

Come agisce il controllo

Il controllo CP-2 è vitale per garantire che l'organizzazione possa continuare a operare o riprendere rapidamente le operazioni dopo un'interruzione. Facendo ciò, minimizza il rischio finanziario, legale, e di reputazione che può derivare da un'interruzione prolungata dei servizi. Questo controllo non solo protegge le risorse e i dati, ma garantisce anche che l'organizzazione sia resiliente e preparata a gestire le emergenze in modo efficace.

CP-2	Contingency Plan	Contingency planning for systems is part of an overall program for achieving continuity of operations for organizational mission and business functions. Contingency planning addresses system restoration and implementation of alternative mission or business processes when systems are compromised or breached. Contingency planning is considered throughout the system development life cycle and is a fundamental part of the system design. Systems can be designed for redundancy, to provide backup capabilities, and for resilience. Contingency plans reflect the degree of restoration required for organizational systems since not all systems need to fully recover to achieve the level of continuity of operations desired. System recovery objectives reflect applicable laws, executive orders, directives, regulations, policies, standards, guidelines, organizational risk tolerance, and system impact level. Actions addressed in contingency plans include orderly system degradation, system shutdown, fallback to a manual mode, alternate information flows, and operating in modes reserved for when systems are under attack. By coordinating contingency planning with incident handling activities, organizations ensure that the necessary planning activities are in place and activated in the event of an incident. Organizations consider whether continuity of operations during an incident conflicts with the capability to automatically disable the system, as specified in IR-4(5). Incident response planning is part of contingency planning for organizations and is addressed in the IR (Incident Response) family.