Occorre esaminare i meccanismi di gestione degli errori cercando una corrispondenza tra le seguenti vulnerabilità di carattere comune:

- Non è possibile convalidare tutti i parametri di ingresso;
- Vengono rivelate troppe informazioni al client.

Audit and Gestione dei Log:

- Sono state individuate delle attività chiave per l'audit?
- L'attività di audit copre tutti i livelli e i server dell'applicazione?
- Come vengono protetti i file di log?

Occorre esaminare i meccanismi di logging cercando una corrispondenza tra le seguenti vulnerabilità di carattere comune:

- Mancata revisione e registrazione (audit) dei tentativi d'accesso falliti;
- Mancata protezione dei file di log;
- Mancata revisione e registrazione (audit) nei vari livelli del server dell'applicazione.

Indicazioni aggiuntive. Dopo aver completato l'attività di modellazione delle minacce, si procede come segue:

- Se si vuole descrivere il modello delle minacce in un documento, mantenere il documento di facile lettura in modo da potere essere consultato frequentemente. Tale documentazione dovrebbe includere gli obiettivi di sicurezza, gli scenari chiave, le risorse protette, un elenco di minacce e un elenco di vulnerabilità.
- Analizzare le vulnerabilità per contribuire a predisporre la progettazione e l'implementazione della sicurezza.
- Analizzare le vulnerabilità per pianificare e implementare il test di sicurezza del sistema.
- Tracciare e aggiornare l'elenco delle vulnerabilità riscontrate utilizzando un sistema di tracciamento.
- Se sono state identificate delle minacce a cui è stata attribuita una priorità molto alta, ma per le quali non sono state individuate le corrispettive vulnerabilità, è necessario decidere se indagare ulteriormente o meno con il rischio di essere esposti a possibili attacchi, oppure di continuare l'analisi alla ricerca di una possibile vulnerabilità.
- Comunicare le informazioni acquisite ai membri del team di lavoro.

6.2 Identificazione del Processo di Sviluppo del Software Sicuro

L'applicazione di un processo di gestione del rischio[58] nello sviluppo di un sistema abilita le organizzazioni a bilanciare i requisiti per la protezione delle informazioni e degli asset proprietari con il solo costo di implementare le strategie di controllo della sicurezza e di mitigazione attraverso l'SDLC.
Il processo di gestione del rischio, identifica le attività e gli asset critici, nonché le vulnerabilità sistemiche a cui è esposta l'organizzazione. I rischi sono spesso condivisi in tutta l'organizzazione e non sono specifici per sole determinate architetture di sistema.
In questo contesto la metodologia ed il tool sviluppato da AGID a tale scopo (https://www.sicurezzait.gov.it) sono strategici per la gestione strutturata del rischio. Per ulteriori dettagli si rinvia all' Allegato 1- Linee Guida per l'adozione di un ciclo di sviluppo di software sicuro.
Alcuni dei vantaggi apportati con l'integrazione degli aspetti di sicurezza nel ciclo di vita di sviluppo del software, sono:

[58] Fare riferimento alla metodologia e al tool sviluppato da AGID a tale scopo (**Cyber Risk Management** - **https://www.sicurezzait.gov.it/Home**). Per ulteriori dettagli si rinvia all' *Allegato 1- Linee Guida per l'adozione di un ciclo di sviluppo di software sicuro.*

- L’individuazione preventiva e la mitigazione delle vulnerabilità e dei problemi di sicurezza presenti nella configurazione dei sistemi, con conseguente riduzione dei costi per l'implementazione dei controlli di sicurezza e delle tecniche di mitigazione delle vulnerabilità;
- La consapevolezza delle potenziali sfide ingegneristiche dovute ai controlli di sicurezza obbligatori;
- L’identificazione dei servizi di sicurezza condivisi e riutilizzo delle strategie e degli strumenti di sicurezza che riducono i costi di sviluppo e migliorano la condizione di sicurezza complessiva del sistema, attraverso l'applicazione di metodi e tecniche collaudate;
- La facilitazione nell'attuazione delle decisioni prese da parte dei dirigenti, attraverso l'applicazione tempestiva di un processo completo di gestione del rischio;
- La documentazione di importanti decisioni di sicurezza prese durante il processo di sviluppo, per informare la direzione sulle considerazioni di sicurezza intraprese durante tutte le fasi dello sviluppo;
- Il miglioramento dell'organizzazione e della fiducia degli utenti nel promuovere l'adozione e l'uso dei propri sistemi;
- Una migliore interoperabilità e integrazione dei sistemi che sarebbe difficile raggiungere se la sicurezza fosse considerata separatamente ai vari livelli.

Uno studio della Forrester Consulting sullo stato della sicurezza applicativa ha riportato che le organizzazioni che implementano un processo MS-SDL hanno mostrato risultati di ROI migliori rispetto agli altri approcci metodologici. Anche, la Aberdeen Group ha dimostrato come l'adozione di un processo MS-SDL aumenti la sicurezza e riduca la gravità e il costo degli incidenti dovuti alla presenza di vulnerabilità nel software, generando al contempo un ritorno sugli investimenti (quattro volte maggiore) rispetto ad altri approcci di sicurezza adottati nello sviluppo di software.
MS-SDL è supportato da una rilevante quantità di risorse, tra cui documentazione, tutorial e strumenti software. Tale ricchezza di informazioni e strumenti rende sicuramente MS-SDL un'opzione interessante per le organizzazioni che intendono adottare nuove iniziative di sicurezza del software.
La modellazione delle minacce è un approccio per analizzare la sicurezza di un'applicazione. Si tratta di un approccio strutturato che consente di identificare, quantificare e affrontare i rischi di sicurezza associati ad una applicazione. La modellazione delle minacce non è un approccio orientato alla revisione del codice, ma integra il processo di revisione del codice da un punto di vista della sicurezza. L'inclusione della modellazione delle minacce nell'SDLC può contribuire a garantire che le applicazioni vengano sviluppate con la sicurezza integrata fin dall'inizio (Secure by Design/ Secure by Default).
Questo, in combinazione con la documentazione prodotta nell'ambito del processo di modellazione delle minacce, può fornire al revisore una maggiore comprensione del sistema. Consente inoltre al revisore di vedere dove si trovano i punti di accesso all'applicazione e quali sono le potenziali minacce associabili a ciascun punto di accesso.
Il concetto di modellazione delle minacce non è nuovo, ma negli ultimi anni si è verificato un chiaro cambiamento di mentalità. La modellazione delle minacce, oggi guarda ad un sistema dal punto di vista di un potenziale attaccante, piuttosto che dal punto di vista della difesa. Microsoft è stata forte sostenitrice di tale processo negli ultimi anni, facendo della modellazione delle minacce una componente fondamentale del proprio SDLC, che sostiene essere una delle principali ragioni di maggiore sicurezza riscontrabile nei suoi prodotti.
Quando l'analisi del codice sorgente, ad esempio di applicazioni esistenti, viene eseguita al di fuori dell'SDLC (in quanto già realizzate), i risultati della modellazione delle minacce, aiutano a ridurre la complessità dell'analisi del codice sorgente, promuovendo un approccio maggiormente circoscritto. Invece di rivedere tutto il codice sorgente con uguale attenzione, è possibile assegnare una priorità alla revisione di sicurezza del codice, basandosi sul risultato ottenuto dal processo di modellazione che individua le minacce a più alto rischio facendo sì che la revisione del codice possa essere indirizzata in modo più puntuale.

Questi i vantaggi introdotti dal processo di modellazione delle minacce:

- la conferma dell'idoneità degli elementi di sicurezza individuati da attuare;
- l'individuazione di eventuali lacune nelle caratteristiche di sicurezza da attuare;
- l'identificazione di eventuali ulteriori elementi di sicurezza;
- l'identificazione dei requisiti di policy e di processo;
- l'identificazione dei requisiti da inserire nelle operazioni di sicurezza;
- l'identificazione dei requisiti in materia di tracciamento e monitoraggio;
- arrivare ai casi di abuso, se utilizzati, secondo la metodologia Agile;
- la comprensione dei requisiti di business continuity;
- la comprensione dei requisiti in materia di capacità e disponibilità.

L' esecuzione del processo di modellazione delle minacce, in fase di progettazione, aiuta nella:

- identificazione delle vulnerabilità che devono essere risolte a livello di progettazione e di implementazione;
- identificazione dei beni informativi che necessitano di controlli di sicurezza;
- mappatura dei controlli di sicurezza, identificati in controlli tecnico/amministrativi/fisici a seconda dei casi (questa attività può essere svolta anche a livello di architettura, ma farlo a livello di progettazione aiuta ad essere più precisi);
- identificazione dei casi di "test di sicurezza"/"scenari di test di sicurezza" nella verifica dei requisiti di sicurezza implementati.

La modellazione delle minacce è il processo di valutazione e documentazione dei rischi associati alla sicurezza di un particolare sistema e/o applicazione software. Mediante l'adozione di opportune tecniche già discusse in precedenza nel documento, è possibile identificare strategie di mitigazione efficaci per contrastare potenziali minacce a cui potrebbe essere soggetta l'applicazione. La modellazione delle minacce consente inoltre, di giustificare l'introduzione o l'eliminazione di eventuali feature all'interno dell'applicazione oltre che governare, al fine di proteggere gli asset dell'applicazione, l'introduzione di nuove policy o pratiche di sicurezza all'interno del sistema. La categorizzazione delle minacce di sicurezza può essere ottenuta mediante l'adozione di un modello denominato STRIDE che è l'acronimo che riunisce la gamma dei rischi a cui può essere soggetta l'applicazione e per i quali deve essere protetta.
Nell'ambito della fase progettuale dell'SDL, nel processo di definizione dei requisiti di sicurezza, un modello come STRIDE può essere di aiuto nel definire i pattern di attacco, tra cui estrarre il modello di attacco (ovvero il sottoinsieme dei possibili attacchi) per il sistema applicativo oggetto di analisi. Lo STRIDE ha l'indubbio vantaggio di non essere eccessivamente astratto ma è piuttosto facilmente riconducibile a situazioni reali. In gran parte della letteratura il modello STRIDE viene definito come un sistema per modellare le minacce. Ma in realtà (in accordo con Gary McGraw) si ritiene più opportuno pensare che STRIDE sia un modello relativo ai possibili attacchi, legando la "minaccia" agli attori (umani e non) che sono invece gli artefici degli attacchi stessi. Le sei categorie di rischi a cui la STRIDE afferisce (Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, and Elevation of privilege) consentono di identificare le vulnerabilità ed i possibili vettori di attacco nelle applicazioni software.

Le linee guida per la modellazione delle minacce ispirata a MS-SDL si suddivide nelle seguenti fasi:

- Identificazione degli asset. Cosa il sistema dovrebbe proteggere?
- Creazione di una panoramica dell'architettura. Concentrandosi sui confini di fiducia, ovvero sui flussi di dati scambiati tra componenti appartenenti ad un'entità e componenti appartenenti ad un'altra entità.
- Scomposizione del sistema in sotto-componenti fino al livello più basso possibile.