5.3 Threat Intelligence e Threat Modeling

Se l'obiettivo che ci si prefigge è quello di individuare gli attacchi a cui il software è correntemente esposto, allora il possesso di informazioni sulle minacce possono favorire nel porre l'attenzione sulle precise azioni necessarie che potrebbero essere intraprese nell'immediato. Diversamente, se l'obiettivo è ridurre la superficie di attacco e indirizzare gli investimenti in modo proattivo, allora la modellazione delle minacce può essere sicuramente di maggiore supporto. Quest'ultima non è in grado di fornire una risposta rapida al singolo problema di sicurezza che invece può essere data dalla Threat Intelligence, ma può sicuramente essere di aiuto nel guidare un programma maggiormente strategico che ha come obiettivo quello di elevare il livello di resilienza del software.

	Threat Modeling	**Threat Intelligence**
Finestra temporale	Proattivo	Reattivo
Estensione	Individuazione delle problematiche di sicurezza	Individuazione degli attaccanti
Supporto dal mercato	Consulenza e formazione	Feeds & Tools

Table 1 – Differenze tra Threat Modeling e Threat Intelligence

5.4 Threat Modeling e Threat Assessment

L'attività di Threat Assessment si concentra sull'identificazione delle minacce nelle applicazioni. Tale pratica è orientata all'individuazione e alla accurata comprensione di potenziali attacchi al software per recepire meglio i rischi e facilitarne la gestione. Difatti, la "software assurance" consiste nell'identificare i rischi presenti nelle applicazioni trattandoli quindi di conseguenza.
I rischi per un'applicazione possono essere relativi al business dell'applicazione (si pensi agli attacchi alla logica di business) o alla configurazione tecnica dell'applicazione. Lo stream del profilo di rischio dell'applicazione si occupa del primo, mentre il Threat Modeling si concentra sul secondo. Di seguito una sintesi dei livelli di maturità di un'organizzazione riguardo la valutazione delle minacce in relazione al profilo di rischio applicativo e all'attività di Threat modeling:

	Profilo di rischio applicativo	**Threat Modeling**
Livello di maturità 1 – Identificazione del Best-effort delle minacce di alto livello per l'organizzazione e per i singoli progetti.	Valutazione base del rischio applicativo	Modellazione delle minacce ad hoc del Best-effort
Livello di maturità 2 - Standardizzazione e analisi a livello aziendale delle minacce legate al software all'interno dell'organizzazione.	Comprensione del rischio per tutte le applicazioni dell'organizzazione	Modellazione delle minacce standardizzata
Livello di maturità 3 - Miglioramento proattivo della copertura delle minacce in tutta l'organizzazione	Revisione periodica dei profili di rischio dell'applicazione	Miglioramento della qualità grazie all'automazione del processo di analisi

Table 2 - Threat Assessment Overview

A seguire si descrivono in modo maggiormente dettagliato i singoli livelli di maturità sopra indicati, considerando che il tool di Risk Management di AGID può essere utilizzato per gestire questa tematica a tutti e tre i livelli, in base alla completezza delle informazioni gestite:

1) Profilo di rischio applicativo

- Livello di maturità 1
  - Benefici: capacità di classificare le applicazioni in base al rischio
  - Attività: come organizzazione, si vuole spendere il proprio budget nella sicurezza lì dove necessario. Il rischio applicativo è un valido strumento per guidare la spesa per la sicurezza. Una classificazione dei rischi aiuta a identificare quali applicazioni possono rappresentare una seria minaccia per l'organizzazione se queste venissero attaccate o violate. Adottare un metodo semplice per valutare il rischio applicativo per applicazione, stimando il potenziale impatto aziendale che essa rappresenta per l'organizzazione in caso di attacco. A tal fine, valutare l'impatto di una violazione della riservatezza, dell'integrità e della disponibilità dei dati o del servizio. Considerare l'utilizzo di un questionario di 5-10 domande per comprendere le caratteristiche importanti dell'applicazione, come ad esempio se l'applicazione tratta dati finanziari, se esposta a Internet o se sono coinvolti dati relativi alla privacy. Il profilo di rischio dell'applicazione indica se questi fattori sono applicabili e se possono avere un impatto significativo sull'organizzazione. Successivamente, utilizzare uno schema per classificare le applicazioni in base a tale rischio. Uno semplice schema qualitativo (ad es. alto/medio/basso) che traduce queste caratteristiche in un valore risulta essere spesso efficace. E' importante utilizzare tali valori per rappresentare e confrontare il rischio di applicazioni diverse l'una rispetto all'altra. Organizzazioni mature altamente orientate al rischio potrebbero utilizzare schemi di rischio maggiormente quantitativi. Non inventare un nuovo schema di rischio se l'organizzazione ne ha già uno e questo funziona bene. Valutate il rischio in base alla serie di domande e assegnare un livello di rischio ad ciascuna applicazione.
- Livello di maturità 2
  - Benefici: conoscenza solida del livello di rischio di un'applicazione
  - Attività: l'obiettivo di questa attività è quello di comprendere a fondo il livello di rischio di tutte le applicazioni presenti all'interno delle organizzazioni per concentrare gli sforzi dove è veramente importante. Dal punto di vista della valutazione del rischio, il questionario di base non è sufficiente per valutare a fondo il rischio di tutte le applicazioni. E' opportuno creare un modo ampio e standardizzato per valutare il rischio dell'applicazione, tra l'altro attraverso il loro impatto sulla sicurezza dell'informazione (riservatezza, integrità e disponibilità dei dati). Oltre alla sicurezza, si vuole anche valutare il rischio per la privacy dell'applicazione. Comprendere i dati che l'applicazione elabora e quali potenziali violazioni della privacy sono rilevanti. Infine, valutare l'impatto che l'applicazione ha su le altre applicazioni presenti all'interno dell'organizzazione (ad esempio, l'applicazione potrebbe modificare dati che sono stati considerati di sola lettura in un altro contesto). Valutare tutte le applicazioni all'interno dell'organizzazione, comprese quelle legacy. Considerare l'uso di schemi quantitativi per classificare il rischio applicativo. Un semplice schema qualitativo (ad esempio alto/medio/basso) non è sufficiente per gestire e confrontare efficacemente le applicazioni su scala Enterprise. Sulla base di tale input, costruire un inventario centralizzato dei profili di rischio che utilizza i risultati delle valutazioni del rischio per definire il profilo. Questo inventario fornisce a tutte le parti interessate una visione allineata del livello di rischio di un'applicazione per assegnare un'adeguata priorità alle attività legate alla sicurezza.
- Livello di maturità 3
  - Benefici: aggiornamento tempestivo della classificazione dell'applicazione in caso di modifiche

- Attività: Il portafoglio di applicazioni di un'organizzazione cambia, così come le condizioni e i vincoli in cui opera un'applicazione (ad esempio, guidato dalla strategia aziendale). Eseguire una revisione periodica dell'inventario dei rischi per garantire la correttezza delle valutazioni dei rischi delle diverse applicazioni. Operare tale revisione a livello aziendale. Inoltre, via via che l'organizzazione evolve e matura nella garantire la sicurezza del software, è importante incoraggiare i team a chiedersi continuamente quali cambiamenti nelle condizioni potrebbero avere un impatto sul profilo di rischio. Per esempio, un'applicazione interna potrebbe essere esposta a Internet a seguito di una decisione aziendale. Ciò dovrebbe indurre i team a ripetere la valutazione del rischio e ad aggiornare di conseguenza il profilo di rischio dell'applicazione. In un'implementazione matura di questa pratica, è altrettanto importante formare e aggiornare continuamente i team sulle esperienze e sulle migliori pratiche derivanti da queste valutazioni del rischio. Ciò porta ad una migliore esecuzione e ad una rappresentazione più accurata del profilo di rischio dell'applicazione.

2) Threat modeling
   - Livello di maturità 1
     - Benefici: comprensione di base delle potenziali minacce
     - Attività: lo scopo del Threat Modeling è quello di identificare in modo proattivo le potenziali problematiche presenti nella progettazione tecnica dell'applicazione. Una configurazione imprudente potrebbe dar luogo a importanti vettori di attacco in un'applicazione che può essere sfruttata per colpire l'organizzazione da cui viene realizzata o utilizzata. L'esperienza dimostra che la progettazione dell'architettura può essere una fonte rilevante di problemi di sicurezza e le conseguenze possono essere significative. La pratica della modellazione delle minacce include sia la raccolta che la gestione delle minacce. Per individuare le minacce e buona norma adottare quelle che sono riconosciute come buone pratiche di sicurezza o un approccio maggiormente strutturato come STRIDE. La modellizzazione delle minacce è spesso più efficace se eseguita da un gruppo di persone, prevedendo un brainstorming. Una delle sfide principali nella modellizzazione delle minacce è quella di riuscire ad ottenere, attraverso un esercizio di efficienza, un elenco contenuto di minacce rilevanti, evitando processi lunghi ed elenchi eccessivamente dettagliati di minacce di scarsa rilevanza. L'esperienza come sempre, aiuta a trovare il giusto equilibrio. Eseguire la modellazione delle minacce in modo iterativo per allinearsi ai paradigmi di sviluppo maggiormente iterativi. Se si aggiungono nuove funzionalità ad un'applicazione esistente, esaminare solo le nuove funzioni aggiunte piuttosto di cercare di coprire l'intero ambito. Eseguire la modellazione delle minacce su progetti importanti (vedi sopra: Application Risk Profile) in modalità best effort per identificare le minacce più importanti per l'applicazione. Ad esempio, un buon punto di partenza potrebbe essere quello di prendere nota degli schemi di rete esistenti descritti durante i vari workshop.
   - Livello di maturità 2
     - Benefici: miglioramento della raccolta e gestione delle minacce
     - Attività: stabilire un approccio standard per eseguire in modo strutturato la modellazione delle minacce e aumentare la qualità e l'efficienza di tale attività all'interno dell'organizzazione facendo sì che lo sforzo investito sia utile e ben speso. Una modellazione strutturata delle minacce tiene conto dei diversi attori, risorse e flussi per identificare un ampio spettro di potenziali minacce all'applicazione. Questa definisce gli input necessari per avviare l'attività (ad esempio, una descrizione di massima dell'architettura tecnica e un diagramma di flusso dei dati), i diversi passaggi per identificare le minacce e i formalismi per descrivere o annotare le