5 PROGETTAZIONE DEL SOFTWARE SECURE/PRIVACY BY DESIGN

5.1 Processi di sviluppo del software sicuro

Questo capitolo illustra alcuni framework di processo di riferimento nello sviluppo sicuro delle applicazioni software, quali: il framework BSA for Secure Software (BSA), il Software Assurance Maturity Model (SAMMM), il Building Security in Maturity Model (BSIMM), il Comprehensive and Lightweight Application Security Process (CLASP) e il ciclo di vita di sviluppo sicuro (SDL) di Microsoft (MS-SDL).
Lo scopo nel presentare diversi framework di sviluppo è quello di ottenere una migliore comprensione delle tecniche di Threat Modeling e di come questo si integra in un ciclo di sviluppo sicuro del software. Indipendentemente dalla metodologia di sviluppo adottata, la definizione dei controlli di sicurezza nelle applicazioni inizia con, o precede, la fase di progettazione e continua per tutto il ciclo di vita dell'applicazione in risposta alle mutevoli esigenze organizzative, in un ambiente costantemente a rischio e in continua evoluzione.

5.1.1 BSA Framework for Secure Software (BSA)

BSA[3] è un framework di sviluppo sicuro del software sviluppato dalla statunitense Software Alliance BSA[4], che riunisce e consolida in un unico quadro, le migliori pratiche di sicurezza da attuare durante tutto il ciclo di sviluppo del software, in modo tale da poter essere efficacemente misurato, indipendentemente dall'ambiente di sviluppo e dallo scopo del software stesso. Il Framework si concentra sul prodotto software (includendo il Software-as-a-Service) considerando sia i processi adottati nello sviluppo e nella gestione del prodotto, sia la resilienza del prodotto stesso. L'obiettivo del framework è quello di integrare, piuttosto che sostituire, le linee guida per i processi di gestione del rischio organizzativo. Per quanto possibile, cerca l'allineamento con gli standard internazionali riconosciuti e nel contempo di rimanere flessibile, adattabile, focalizzato sui risultati e basato sul rischio.

5.1.2 Open Software Assurance Maturity Model (SAMM)

OpenSAMM[5] è un framework supportato da OWASP[6] (Open Web Application Security Project) che si basa su un insieme di procedure di sicurezza legate a quattro importanti funzioni di business critiche, coinvolte nello sviluppo del software, vale a dire Governance, Costruzione, Verifica e Distribuzione. Ciascuna funzione di business adotta tre pratiche di sicurezza e ciascuna di esse è suddivisa in tre livelli di maturità. La valutazione delle minacce è la prima pratica di sicurezza adottata durante la funzione di business "Costruzione". Questa utilizza il Threat modeling per identificare i potenziali rischi. Successore diretto di questo framework è l'OWASP SAMM[7] rilasciato per consentire alle organizzazioni di misurare e migliorare la postura di sicurezza del software prodotto. OpenSAMM non si lega ad alcun approccio di modellazione delle minacce e raccomanda l'uso di STRIDE della Microsoft o TRIKE come possibili opzioni.

3 https://ww2.bsa.org/~/media/Files/Policy/BSA_2019SoftwareSecurityFramework.pdf

4 https://ww2.bsa.org/

5 http://www.opensamm.org/

6 https://www.owasp.org/images/6/6f/SAMM_Core_V1-5_FINAL.pdf

7 https://owaspsamm.org/