dovrebbero essere distribuite solo dopo il completamento degli appropriati test e della relativa documentazione. (Vedi CWE 439).

- Definire gli opportuni requisiti di sicurezza.
  - Descrizione: Incaricare il business owner per la definizione dei requisiti di sicurezza del software. Ciò include gli aspetti che vanno dalle regole di convalida basate su whitelist fino ai requisiti non funzionali, come le prestazioni di una funzione specifica del sistema. La definizione anticipata di tali requisiti garantisce che la sicurezza sia integrata nel sistema sin dall'inizio.
- Condurre una Design Review.
  - Descrizione: L'integrazione delle pratiche di sicurezza nella fase di progettazione consente di risparmiare tempo e denaro. Condurre un'analisi dei rischi con i professionisti della sicurezza (ad esempio attraverso il tool di Risk Management fornito da AGID) e modellare l'applicazione per identificare i rischi maggiormente rilevanti. Ciò consente di integrare le appropriate contromisure nella progettazione e nell'architettura dell'applicazione software. (Vedi CWE 701, 656).
- Eseguire una Code Review.
  - Descrizione: La revisione del codice incentrata sugli aspetti di sicurezza possono rappresentare uno dei mezzi più efficaci per individuare i bug di sicurezza. E' importante revisionare regolarmente il codice alla ricerca di problematiche comuni di sicurezza come SQL Injection e Cross-Site Scripting. Avvalersi degli strumenti automatizzati per massimizzare l'ampiezza della copertura e la coerenza dei findings. (Vedi CWE 702).
- Eseguire gli opportuni test di sicurezza.
  - Descrizione: Condurre dei test di sicurezza sia durante che dopo lo sviluppo al fine di garantire che l'applicazione soddisfi gli standard di sicurezza imposti. Tali test dovrebbero essere condotti anche dopo le major release per garantire che eventuali vulnerabilità non siano state introdotte durante il processo di aggiornamento. Avvalersi dell'automazione includendo i test di sicurezza nella pipeline CI/CD.
- Hardenizzare l'infrastruttura.
  - Descrizione: Tutti i componenti dell'infrastruttura a supporto dell'applicazione devono essere configurati secondo le migliori pratiche di sicurezza e le linee guida di hardening. In una tipica applicazione web ciò può includere router, firewall, switch di rete, sistemi operativi, server web, application server, database e framework applicativi. (Vedi CWE 15, 656).
- Definire un piano di gestione degli incidenti.
  - Descrizione: E' opportuno elaborare e regolarmente verificare un piano di gestione degli incidenti. Si deve ben definire e mantenere aggiornato, l'elenco delle persone da coinvolgere in un incidente di sicurezza che riguarda l'applicazione software.
- Formare il team sugli aspetti della sicurezza.
  - Descrizione: La formazione aiuta a definire un linguaggio comune che il team può utilizzare per migliorare la sicurezza dell'applicazione software. La formazione non dovrebbe essere limitata esclusivamente agli sviluppatori di software, tester e architetti. Chiunque sia coinvolto nel processo di sviluppo, come gli analisti funzionali e i project manager, dovrebbe essere soggetto a formazione periodica sulla sicurezza del software.

5.2.2.2 Best practice di secure design per il cloud

In questo paragrafo, vengono sinteticamente descritte alcune delle migliori pratiche da adottare in fase di design, per fronteggiare le vulnerabilità e i rischi che potrebbero nascere a seguito dello spostamento di applicazioni e dati verso il cloud.

Tali pratiche si rivolgono a tutte le organizzazioni, indipendentemente dalle dimensioni, che intendono migliorare la sicurezza dei propri servizi in cloud. Si fa notare che queste best practice non sono da intendersi esaustive e che devono essere integrate con le linee guida rilasciate dai fornitori di servizi cloud (CSP), con le best practice generali di sicurezza informatica, con i requisiti di conformità normativa e con le pratiche definite dalle associazioni di categoria del cloud (ad esempio, la Cloud Security Alliance).

- Utilizzo non sicuro delle credenziali di sviluppo
  - Le credenziali dello sviluppatore consentono al team e ad eventuali integrazioni di accedere all'account cloud. Queste dovrebbero essere conservate e utilizzate in modo sicuro per garantire che solo le persone e i casi d'uso autorizzati ne abbiano accesso. Se possibile, prevedere un monitoraggio adeguato e una scadenza automatica dopo un determinato periodo di tempo o di inattività delle credenziali.
- Storage pubblicamente accessibili
  - I provider cloud normalmente prevedono diversi metodi di memorizzazione di oggetti e dati. E' importante revisionare regolarmente le relative configurazioni al fine di garantire che solo i componenti previsti siano pubblicamente accessibili.
- Uso improprio della configurazione di default
  - I provider cloud di solito pre-configurano i criteri di default di controllo degli accessi. Tale impostazione a volte può essere utile, ma spesso introduce dei rischi in quanto le offerte di servizi del fornitore spesso sono soggette a cambiamento. Quindi, le regole preconfigurate spesso vengono modificate per consentire l'accesso ai nuovi servizi che sono fuori del contesto di ciò che è di fatto necessario o in uso.
- Compromissione delle regole di controllo accesso
  - Quando si progetta l'accesso ad un servizio in cloud è buona norma seguire sempre il principio del minimo privilegio. E' necessario considerare la granularità dell'accesso ai servizi, ai sistemi e alla rete. Pertanto è opportuno revisionare regolarmente o automaticamente tali tipologie di accesso al fine di garantire che il principio del minimo privilegio venga rispettato.
- Costrutti di rete non configurati correttamente
  - La maggior parte dei provider cloud dispone di metodi per controllare l'accesso alla rete che vanno al di là delle semplici regole basate sugli indirizzi IP. Considerare l'utilizzo di tali costrutti per controllare l'accesso a livello granulare. Considerare l'utilizzo di componenti di rete basti su provider cloud per segmentare il traffico in modo ponderato.
- Monitoraggio e Logging inadeguato
  - Attivare e monitorare regolarmente la registrazione su log degli accessi attraverso API. Adottare una strategia di logging basata sul rischio per quei servizi che non vengono loggati attraverso i core logging services.
- Mancanza di un Inventory Management
  - L'accesso basato su API risolve molti problemi di inventory management. Adottare le opportune strategie al fine di arricchire l'ambiente con informazioni aggiuntive su proprietà, casi d'uso e sensibilità.
- Dirottamento del dominio
  - Spesso esiste un rapporto di fiducia transitoria tra i servizi cloud e le entries DNS. Revisionare regolarmente le configurazioni DNS e cloud per prevenire situazioni di acquisizione di controllo fraudolento.
- Mancanza di un piano di Disaster Recovery
  - Gli ambienti cloud non risolvono automaticamente i problemi di Disaster Recovery. Considerare l'appropriato livello di investimento per gli eventi catastrofici che avvengono all'interno dell'ambiente cloud. Progettare un programma di Disaster Recovery per il ripristino abilitato da account esterni, provider o da locale.
- Configurazione manuale degli account