5 PROGETTAZIONE E SVILUPPO DELL'APPLICAZIONE: DIRETTIVE STANDARD

5.1 Progettazione dell'applicazione

L'architettura dell'applicazione deve essere progettata e sviluppata secondo i paradigmi standard dell'industria del software, quali: Architettura monolitica (mainframe), Client server, Service Oriented Architecture (SOA), ecc.
Nel corso della fase di progettazione è necessario garantire un adeguato livello di sicurezza applicativa e infrastrutturale attraverso l'analisi e la modellazione delle minacce relative agli applicativi coinvolti, delle interfacce e degli agenti che potrebbero minacciare il sistema. Per l'analisi della sicurezza applicativa di un'architettura di sistema si adotta un approccio differente a seconda che si tratti di progettazione di applicazioni ex-novo (approccio Secure by Design) piuttosto che di reingegnerizzazione di applicazioni esistenti (approccio Security Control). Nel dettaglio:

- **PROGETTAZIONE SICURA BY DESIGN** - Durante le fasi di analisi della sicurezza applicativa di una architettura di sistema (da definire o in fase di rivisitazione) è necessaria l'attuazione di pratiche di progettazione sicura attraverso l'individuazione di requisiti di sicurezza e contromisure secondo i Security by Design Principles. Le pratiche di progettazione sicura realizzano la sicurezza delle informazioni attraverso un approccio di "Defense in Depth" del layer applicativo. La "difesa in profondità" ha come scopo limitare al minimo i danni in caso di attacco riuscito. In pratica, nell'ipotesi che un attaccante riesca a oltrepassare il primo livello di difesa (ad esempio aggirando il controllo di autenticazione), ulteriori misure più restrittive devono intervenire per ostacolarne l'avanzata (ad esempio, restringendo al minimo i privilegi d'accesso alle risorse o applicando la compartimentazione dell'applicazione al fine di ostacolare bloccare la propagazione dell'attacco all'intero sistema).
- **SECURITY CONTROL** (su applicazione esistente) – È necessario: 1) Identificare, quantificare e risolvere i rischi di sicurezza associati ad un'interfaccia, un'applicazione e/o un sistema esistenti. 2) Validare dal punto di vista della sicurezza applicativa gli sviluppi realizzati da terze parti (sicurezza della supply chain). 3) Tutelare il proprio patrimonio informativo e i dati.

Le tecniche di modellazione delle minacce e d'identificazione delle relative contromisure, finalizzate a indirizzare i requisiti di sicurezza applicativa di un'architettura di sistema, insieme alle pratiche di progettazione sicura, sono trattate in dettaglio nell'*Allegato 4* - ***Linee Guida per la modellazione delle minacce ed individuazione delle azioni di mitigazione conformi ai principi del Secure/Privacy by Design.***

5.2 Sviluppo dell'applicazione – Criteri Generali

Nel corso della fase di sviluppo di un'applicazione, si raccomanda l'adozione dei criteri generali riportati nei paragrafi successivi.

5.2.1 Performance

Le soluzioni di programmazione impiegate devono ridurre al minimo l'impatto sulle risorse di sistema.
È necessario:

- non ottimizzare mai manualmente ciò che può essere ottimizzato dai compilatori;
- per i linguaggi che accedono direttamente alla memoria del sistema, evitare di avere puntatori multipli ad una determinata risorsa;
- utilizzare i data-types appropriati (es: non utilizzare long quando int è sufficiente);
- utilizzare switch/case al posto di strutture nidificate di if;
- porre le risorse più frequentemente utilizzate le une vicine alle altre;
- allocare la memoria il più tardi possibile (costruzione degli oggetti);