L'approccio migliore per proteggere un sistema informativo, è garantire che ogni sua componente abbia un proprio meccanismo di protezione. La costruzione di strati multipli di controlli di sicurezza posti lungo un sistema è definita ***Defence in Depth***.

La Defense-in-Depth è l'approccio alla sicurezza delle informazioni che prevede il raggiungimento di una adeguato livello di sicurezza attraverso l'utilizzo coordinato e combinato di molteplici contromisure.

Questa strategia difensiva si fonda sull'integrazione di differenti categorie di elementi: persone, tecnologie e modalità operative. La ridondanza e la distribuzione delle contromisure possono essere sintetizzate in una "difesa a differenti livelli" ("Layered Defenses"). Il concetto, di derivazione militare, si basa sull'assunto che nel caso in cui un attacco abbia successo, a causa del fallimento di un meccanismo di sicurezza, altri meccanismi di sicurezza possono intervenire per consentire un'adeguata protezione dell'intero Sistema.

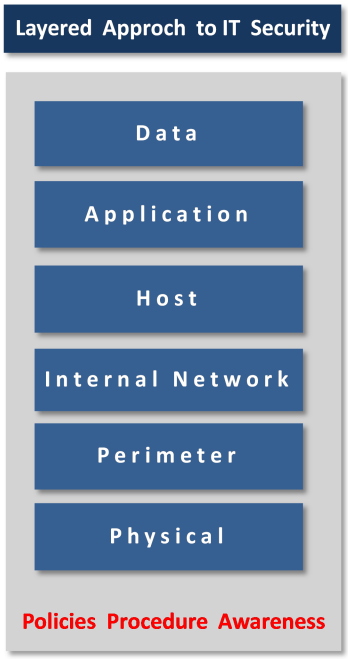


*Figura 3 - Defence-in-Depth model for IT*

Diverse sono le iniziative che si sono incentrate sulle problematiche Secure Development promuovendo azioni di sensibilizzazione (indirizzate ad aziende e community di sviluppatori) quali:

- la diffusione delle fondamentali best practices in materia di sicurezza applicativa (le prime tra tutte riconducibili a una buona ingegnerizzazione del software);
- una piena comprensione delle minacce più comuni (compresi i difetti propri dei linguaggi di programmazione);
- ancora più importante, una considerazione della problematica fin dalle prime fasi del ciclo di sviluppo.

L'OWASP traccia periodicamente la lista delle vulnerabilità più critiche delle applicazioni web. L'obiettivo è appunto, quello di educare e sensibilizzare sulle conseguenze che possono scaturire da implementazioni errate e facilmente vulnerabili. L'ultimo rapporto OWASP è stato rilasciato nel novembre del 2017 (OWASP Top 10 – 2017). La maggior parte delle problematiche identificate nella OWASP Top 10 – 2017 sono le stesse (o comunque molto simili) a quelle identificate nel rapporto precedente (OWASP Top 10 – 2013) con qualche novità, come si evince dalla figura che segue: