5 BEST PRACTICES PER ADEGUARE E MANTENERE LA SICUREZZA DEL SOFTWARE DI BASE

L'apertura delle applicazioni verso fornitori, clienti, utenti remoti e mobili ha comportato la scomparsa di un perimetro aziendale definito e un'estrema diversificazione delle minacce. In questo nuovo scenario, le applicazioni sono diventate il **principale vettore di attacco** ed è sempre più difficile proteggerle. Lo studio presentato nel ***Rapporto OAD***[1] ***2017*** sugli attacchi applicativi in Italia, evidenzia come **principale causa degli attacchi** applicativi, sono le **vulnerabilità** delle infrastrutture ICT, del software di base e dei middleware usati dalle applicazioni (circa il 37%). Seguono poi le **vulnerabilità intrinseche all'applicativo** stesso quali, ad esempio, quelle dei sistemi di identificazione, autenticazione e controllo degli accessi. Nell'ultimo Rapporto Clusit del 2019[2] si evidenzia un trend di crescita degli attacchi sia in termini quantitativi che in termini di gravità dei danni prodotti. Il suddetto rapporto riporta quanto segue "Nell'ultimo biennio il tasso di crescita del numero di attacchi gravi è aumentato di 10 volte rispetto al precedente. Non solo, la Severity media di questi attacchi è contestualmente peggiorata, agendo da moltiplicatore dei danni.".

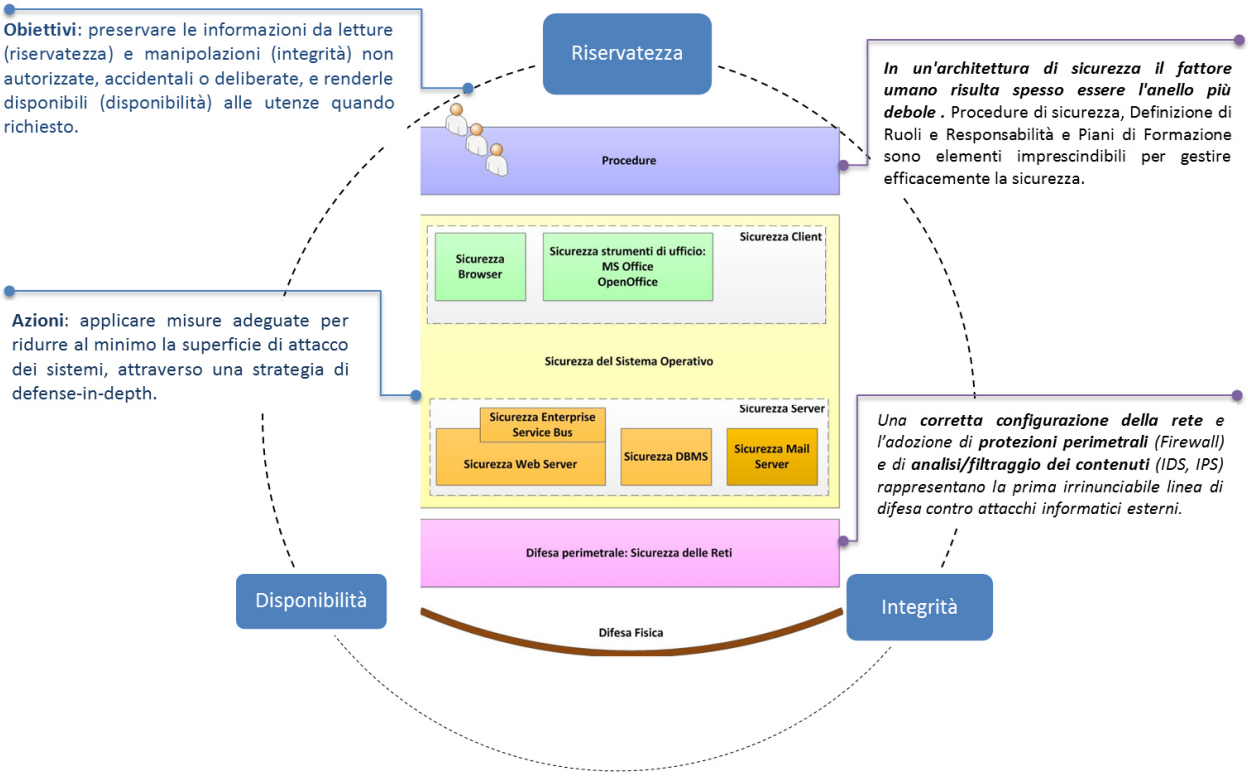

Figura 1 - Scenario - Sicurezza ad ogni livello (fisico, logico e organizzativo)

[1] Osservatorio Attacchi Digitali – https://www.malaboadvisoring.it/index.php?option=com_content&view=article&id=126:rapporto-2017-oad-attacchi-agli-applicativi-in-italia-&catid=13:oci-ed-oai-&Itemid=127

[2] https://clusit.it/rapporto-clusit/