	dalle fasi di seguito elencate: - Rilevamento, avvalersi di strumenti che verifichino l'eventuale mancanza di patch di protezione. Il rilevamento deve avvenire in modo automatico ed attivare il processo di gestione delle patch; - Valutazione, qualora sia riscontrata la mancanza di aggiornamenti utili, valutare la gravità delle problematiche risolvibili con l'applicazione delle patch; - Acquisizione, nel caso le misure di protezione applicate risultino insufficienti all'eliminazione della vulnerabilità, procedere con lo scaricamento della patch per sottoporla ad un'approfondita analisi; - Verifica, procedere con l'installazione della patch su un sistema di prova al fine di verificare l'impatto delle conseguenze dell'aggiornamento sulla configurazione dell'ambiente di produzione; - Gestione, eseguire la registrazione al servizio di notifica per segnalare eventuali vulnerabilità quando individuate; - Distribuzione, distribuire la patch sulle macchine interessate; prevedere, inoltre, l'adozione di un piano di ripristino o di backup. In presenza di "Zero-day exploit", per i quali non è ancora disponibile la patch, massimizzare la difesa perimetrale ed eseguire il patching appena disponibile e testato.

Secure testing

Vulnerability Assessment	
Minaccia	- Accesso non autorizzato ai sistemi (risorse di sistema, configurazioni, interfacce amministrative, ecc.). - Accesso non autorizzato alle informazioni; - Compromissione delle comunicazioni. - Divulgazione di informazioni riservate. - Negazione dei servizi. - Cancellazione o furto di informazioni. - Attacchi all'integrità dei sistemi (software e configurazioni). - Attacchi all'integrità delle informazioni. - Uso non autorizzato di privilegi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione. - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	Effettuare almeno una volta l'anno un'attività di Vulnerability Assessment (VA) in modo da identificare le eventuali vulnerabilità che possono costituire un canale di accesso non autorizzato ad informazioni. Il VA deve verificare la corretta configurazione delle porte logiche affinché siano attive solo quelle strettamente necessarie. Inoltre, l'attività di VA deve essere condotta avendo come riferimento le ultime vulnerabilità note, pubblicate nelle banche dati di riferimento in tema di sicurezza informatica come, ad esempio, Open Source Vulnerability DataBase (OSVDB) e Common Vulnerabilities Exposures (CVE). In seguito all'attività di VA, per mitigare il rischio associato alle vulnerabilità identificate è necessario: - definire i ruoli e le responsabilità per la gestione delle vulnerabilità tecniche; - identificare le azioni da intraprendere (es. disabilitare le funzionalità non utilizzate, inclusi protocolli e servizi; rendere più sicure le impostazioni di configurazione predefinite, ridurre al minimo il numero delle interfacce di amministrazione, ecc.); - revisionare le funzionalità di failover del sistema.

Penetration Test