PENETRATION TESTING [PT]

ASSESSMENT TOOLS AND TECHNIQUES TO IDENTIFY SYSTEM WEAKNESSES

AND

ONGOING ASSESSMENT AND AUTOMATION

Autore: Aldo Pedico –Cybersecurity & Privacy Consultant
Contatto: pedicoaldo@gmail.com

INTRODUZIONE

In questo documento, ho voluto fornire delle indicazioni generali e molto semplici che permettono:

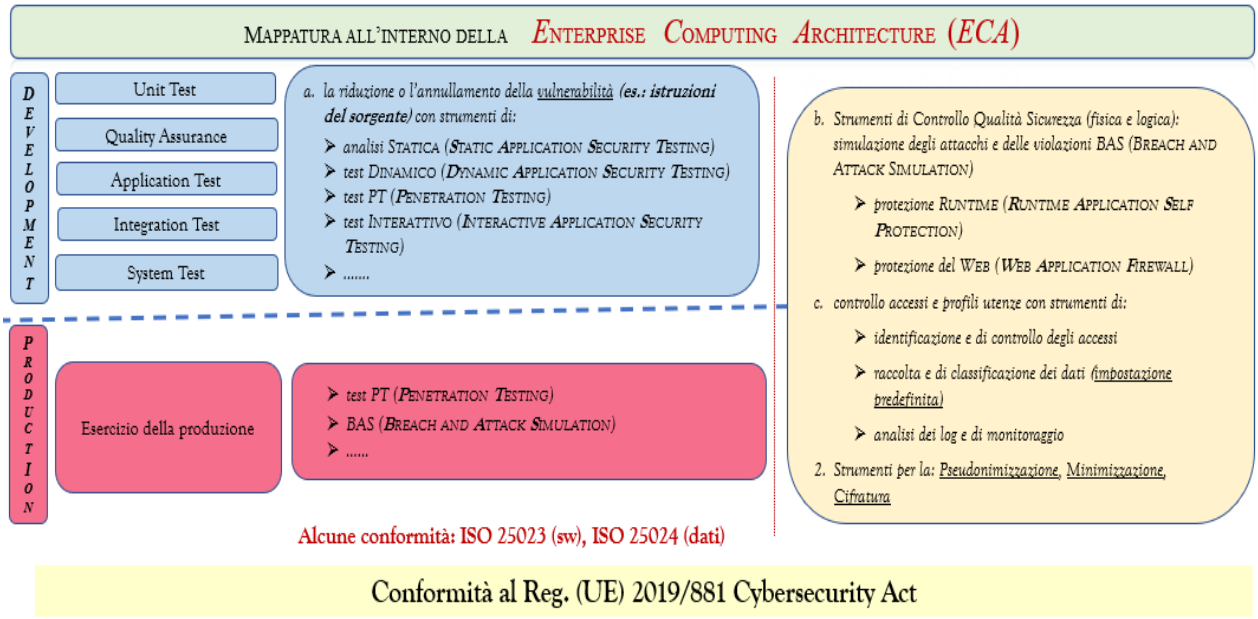
1. *di inquadrare il significato della tecnica di* PENETRATION TEST *attraverso le sue caratteristiche,*
2. *di capire il perché debba essere utilizzata la tecnica di PT,*
3. *di individuare il momento in cui adottare il PT,*
4. *di decidere dove tale tecnica debba essere inserita nei processi organizzativi (*ONGOING PROCESS*).*

La tecnica di PT *è una delle diverse tecniche che devono essere adottate all'interno del* CHANGE MANAGEMENT PROCESS *del* SOFTWARE AND HARDWARE LIFE CYCLE *e nell'*ONGOING ASSESSMENT AND AUTOMATION PROCESSES.

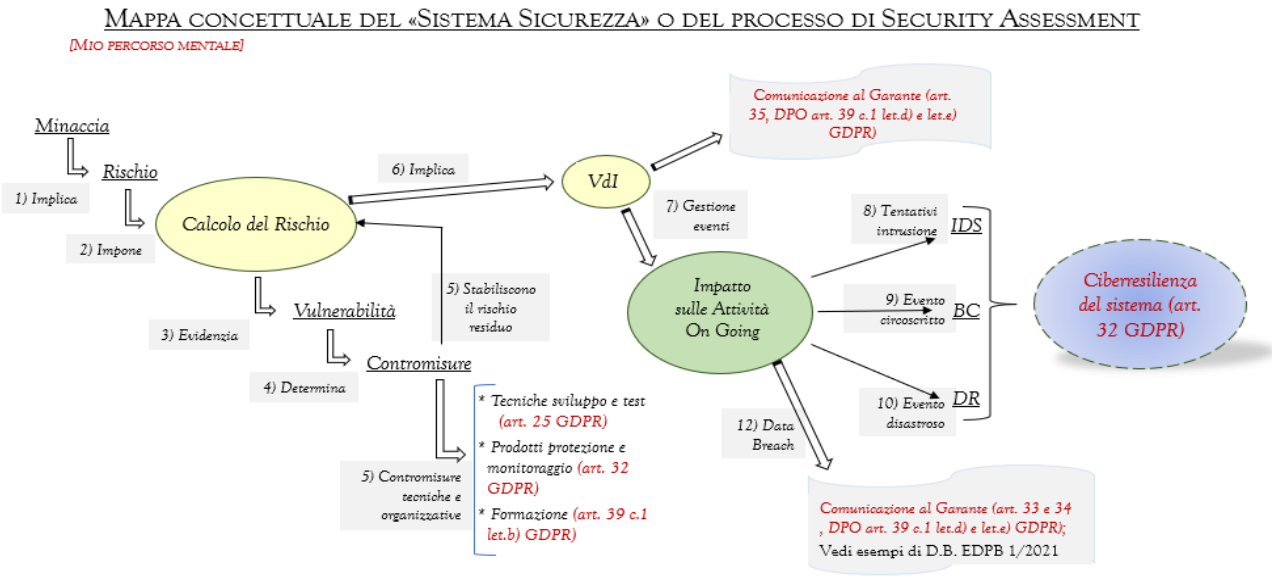
Tali processi si collocano in un contesto più ampio e per meglio comprendere dove si posizionano vi presento lo schema di seguito.

*In questo mio schema ho rappresentato l'architettura di un'organizzazione (*ECA*) che ha al suo interno anche le fasi di sviluppo (*Development*) del software (parte in azzurro).*

Per l'ambiente di Development *e di* Production *ho indicato le tecniche di* SECURITY MANAGEMENT *sia in fase di attività di* ASSESSMENT *asincrona sia durante le attività* ONGOING.



Nella figura seguente, ho evidenziato il mio processo mentale che utilizzo per affrontare con metodo l'intero processo di SECURITY ASSESSMENT.



È di fondamentale importanza la COMPRESENZA *di tecniche diverse (*BAS, SAST, IAST, DAST, *ecc.) per ottenere una maggiore garanzia di sicurezza;* SOLO IL PT NON È SUFFICIENTE PERCHÉ LE SIMULAZIONI POTREBBERO NON ESSERE ESAUSTIVE (COPERTURA) E INEFFICACI (DEBOLEZZA).

Occorre prendere in considerazione alcune caratteristiche che determinano l'efficacia delle simulazioni a seconda che queste siano eseguite o meno in modo automatico.

In particolare:

- Simulazioni NON eseguite automaticamente:

  1. ABILITÀ*: dipende molto dall'esperienza del tecnico che esegue il* PENETRATION TEST*;*
  2. COPERTURA*: l'efficacia del test è in funzione della capacità del tecnico di eseguire tutta la casistica necessaria a garantire una copertura del contesto stabilito;*
  3. OBSOLESCENZA*: è necessario un continuo aggiornamento della casistica delle tecniche di* ATTACCO *e, quindi, il tecnico potrebbe essere* NON *aggiornato;*
  4. FREQUENZA*: l'efficacia dei risultati è anche in relazione alla continuità dei test, perché esiste la consapevolezza che un cambiamento infrastrutturale o del software potrebbe presentare una lacuna o debolezza con conseguenze dannose.*

- Simulazioni eseguite automaticamente da un programma di PT inserito in modo sistematico all'interno del processo Security Management:

  1. ABILITÀ*: è molto probabile che il programma abbia al suo interno tutte le tecniche necessarie a svolgere il test;*
  2. COPERTURA*: l'efficacia del test è in funzione dell'esecuzione di tutta la casistica necessaria a garantire una copertura del contesto stabilito;*
  3. OBSOLESCENZA*: è necessario un continuo aggiornamento della casistica delle tecniche di* ATTACCO *e, quindi, il software potrebbe essere* NON *aggiornato;*
  4. FREQUENZA*: l'efficacia dei risultati è anche in relazione alla continuità dei test, perché esiste la consapevolezza che un cambiamento infrastrutturale o del software potrebbe presentare una lacuna o debolezza con conseguenze dannose, quindi è necessario inserire il programma/i all'interno sia del* CHANGE MANAGEMENT *del* SOFTWARE AND HARDWARE LIFE CYCLE *sia dell'*ASSESSMENT AND AUTOMATION PROCESS.

INDICE DEGLI ARGOMENTI

Titolo **Pag.**

PENETRATION TESTING GENERAL DESCRIPTION

Le organizzazioni possono considerare l'aggiunta di test di penetrazione controllata al loro arsenale di strumenti e tecniche utilizzate per valutare i controlli di sicurezza e privacy nei sistemi organizzativi.

Il test di penetrazione ha le seguenti caratteristiche:

1. *È un tipo specifico di valutazione in cui i valutatori simulano le azioni di una determinata classe di aggressori utilizzando un insieme definito di documentazione (ad esempio, documentazione rappresentativa di ciò che è probabile che quella classe di aggressori possieda) e lavorando sotto altri vincoli specifici per tentare di aggirare le caratteristiche di sicurezza o privacy di un sistema.*
2. *Viene condotto come tentativo controllato di violare i controlli di sicurezza e privacy impiegati all'interno del sistema utilizzando le tecniche dell'attaccante e gli strumenti hardware e software appropriati.*
3. *Rappresenta i risultati di un valutatore specifico o di un gruppo di valutatori in un momento specifico utilizzando regole di ingaggio concordate.*

Considerando la complessità delle tecnologie informatiche comunemente impiegate dalle organizzazioni oggi, i PT possono essere visti ***non come un mezzo per verificare le caratteristiche di sicurezza e privacy di un sistema, ma piuttosto:***

1. ***come un mezzo per migliorare la comprensione del sistema da parte dell'organizzazione,***
2. ***scoprire punti deboli o carenze nel sistema e***
3. ***indicare il livello di sforzo richiesto dagli avversari per violare le tutele del sistema.***

Gli esercizi di PT possono essere programmati e/o casuali in accordo con la politica organizzativa e le valutazioni organizzative del rischio.

Si può prendere in considerazione l'esecuzione di PT:

1. *su qualsiasi sistema di nuova concezione (o sistema legacy sottoposto a un importante aggiornamento) prima che il sistema sia autorizzato al funzionamento,*
2. *dopo che sono state apportate modifiche importanti all'ambiente in cui opera il sistema e*
3. *quando un nuovo tipo di viene rilevato un attacco che potrebbe avere un impatto sul sistema.*

Le organizzazioni monitorano attivamente l'ambiente di sistema e il panorama delle minacce (ad esempio, nuove vulnerabilità, tecniche di attacco, implementazioni di nuove tecnologie, sicurezza degli utenti e

sensibilizzazione e formazione sulla privacy) per identificare i cambiamenti che richiedono test di penetrazione fuori ciclo.

Le organizzazioni specificano quali componenti all'interno del sistema sono soggetti a test di penetrazione, nonché il profilo dell'attaccante da adottare durante gli esercizi di PT e addestrano il personale selezionato all'uso e alla manutenzione degli strumenti e delle tecniche dei test di penetrazione.

Strumenti efficaci per i test di penetrazione hanno la capacità di aggiornare prontamente l'elenco delle tecniche di attacco e delle vulnerabilità sfruttabili utilizzate durante gli esercizi.

Le organizzazioni aggiornano l'elenco delle tecniche di attacco e delle vulnerabilità sfruttabili utilizzate nei PT sulla base di una valutazione organizzativa del rischio o quando vengono identificate e segnalate nuove vulnerabilità o minacce significative.

Quando possibile, le organizzazioni utilizzano strumenti e tecniche di attacco che includono la capacità di eseguire PT sui sistemi e controlli di sicurezza e privacy in modo automatizzato.

Le informazioni ottenute dal processo di PT possono essere condivise con il personale appropriato in tutta l'organizzazione per aiutare a stabilire la priorità delle vulnerabilità nel sistema che sono dimostrabilmente soggette a compromissione da parte di aggressori di un profilo equivalente a quelli utilizzati negli esercizi di PT.

La definizione delle priorità aiuta a determinare strategie efficaci per eliminare le vulnerabilità identificate e mitigare i rischi associati alle operazioni e alle risorse dell'organizzazione, agli individui, alle altre organizzazioni e alla nazione risultanti dal funzionamento e dall'uso del sistema.

Il PT può essere integrato nel NETWORK SECURITY TESTING PROCESS *e nel* PATCH AND VULNERABILITY MANAGEMENT PROCESS.

PENETRATION TESTING CONSIDERATIONS

Le organizzazioni considerano i seguenti criteri quando sviluppano e implementano un programma PT controllato.

Un efficace PT:

1. *Va oltre la scansione delle vulnerabilità per fornire una prova esplicita dei rischi della missione e un indicatore del livello di sforzo che un avversario dovrebbe spendere per causare danni alle operazioni e alle risorse dell'organizzazione, agli individui, ad altre organizzazioni o alla Nazione.*
2. *Si avvicina al sistema come farebbe l'avversario, considerando le vulnerabilità, le configurazioni di sistema errate, le relazioni di fiducia tra le organizzazioni ei punti deboli dell'architettura nell'ambiente in fase di test.*
3. *Ha un ambito chiaramente definito e contiene come minimo una definizione:*
   a) *dell'ambiente soggetto a test (ad es. strutture, utenti, gruppi organizzativi);*

b) della superficie di attacco da testare (ad es. server, sistemi desktop, reti wireless, applicazioni Web, sistemi di rilevamento e prevenzione delle intrusioni, firewall, account e-mail, sicurezza degli utenti e sensibilizzazione alla privacy e comportamento di formazione e comportamento di risposta agli incidenti, comprese le violazioni delle informazioni di identificazione personale);

c) delle fonti di minaccia da simulare (ad esempio, un'enumerazione dei profili degli aggressori da utilizzare, come un aggressore interno, un aggressore occasionale, uno o un gruppo di aggressori esterni mirati, un attore nazionale/stato o un'organizzazione criminale);

d) degli obiettivi per l'attaccante simulato (ad esempio, ottenere l'accesso come amministratore di dominio sulla struttura LDAP [LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL] *dell'organizzazione e accedere e modificare le informazioni nel sistema finanziario dell'organizzazione);*

e) del livello di impegno (es. tempo e risorse) da impiegare;

f) delle regole di ingaggio.

4. *Documenta accuratamente tutte le attività eseguite durante il test, comprese tutte le vulnerabilità sfruttate e come le vulnerabilità sono state combinate negli attacchi.*
5. *Produce risultati che indicano una probabilità che si verifichi un determinato attacco utilizzando il livello di sforzo che la squadra ha dovuto impiegare per penetrare nel sistema come indicatore della resistenza alla penetrazione del sistema.*
6. *Convalida i controlli di sicurezza e privacy esistenti (compresi i meccanismi di mitigazione del rischio, come firewall e sistemi di rilevamento e prevenzione delle intrusioni).*
7. *Fornisce un registro verificabile e riproducibile di tutte le attività svolte durante il test.*
8. *Fornisce risultati attuabili con informazioni sulle possibili misure di riparazione per gli attacchi eseguiti con successo.*

ONGOING ASSESSMENT AND AUTOMATION

USING AUTOMATED TECHNIQUES TO ACHIEVE MORE EFFICIENT ASSESSMENT

La ONGOING ASSESSMENT (OA) *della sicurezza e della privacy è la valutazione continua dell'efficacia dell'implementazione del controllo della sicurezza e della privacy.*

La OA *è un sottoinsieme essenziale delle attività di monitoraggio continuo della sicurezza delle informazioni (*INFORMATION SECURITY CONTINUOUS MONITORING [ISCM]*).*

Nella OA le informazioni relative alla sicurezza sono correlate, analizzate e segnalate ai Responsabili, utilizzando strumenti automatizzati nella misura in cui sia possibile e pratico farlo. In tal modo è possibile prendere decisioni sulla base oggettiva dei rischi evidenziati.

L'evoluzione delle minacce e le modifiche nell'elaborazione delle PII creano una sfida per le organizzazioni che progettano, implementano e gestiscono sistemi complessi compromessi di molti componenti hardware, firmware e software.

La capacità di valutare tutti i controlli di sicurezza e privacy implementati con la frequenza necessaria utilizzando metodi manuali o procedurali è diventata impraticabile per la maggior parte delle organizzazioni a causa delle dimensioni, della complessità e della portata delle proprie infrastrutture informatiche.

Una strategia per aumentare il numero di controlli di sicurezza e privacy, per i quali la valutazione e il monitoraggio possono essere automatizzati, dipende dalla definizione di una specifica dello stato desiderato e dall'espressione dello stato desiderato in una forma che possa essere confrontata automaticamente (cioè nei dati) con lo stato attuale.

Lo stato desiderato è un valore definito o una specifica con cui è possibile confrontare il valore dello stato effettivo.

Una mancata corrispondenza dei due valori indica che è presente un difetto nell'efficacia di uno o più controlli.

Ad esempio, un criterio dell'organizzazione può indicare che gli account utente verranno bloccati dopo 3 tentativi di accesso non riusciti.

La specifica dello stato desiderato sarebbe che i dispositivi applicabili siano configurati per bloccare gli account dopo tre tentativi di accesso non riusciti.

Se durante la valutazione automatizzata, le informazioni relative alla sicurezza raccolte indicano che un dispositivo specifico è configurato in modo tale che gli account siano bloccati dopo 5 tentativi di accesso non riusciti, si rileva una mancata corrispondenza tra lo stato desiderato (3 tentativi consentiti prima del blocco) e lo stato effettivo (5 tentativi consentiti prima del blocco).

La mancata corrispondenza può riflettere un problema con l'efficacia del controllo SP 800-53 AC-7 (tentativi di accesso non riusciti).

Per automatizzare in modo efficace le valutazioni di sicurezza e controllo della privacy utilizzando la strategia di specifica dello stato desiderata, è importante soddisfare i seguenti prerequisiti:

1. *sono definite le specifiche automatiche dello stato effettivo e del comportamento;*
2. *sono definite le specifiche dello stato desiderato basate sui dati (paragonabili allo stato attuale); e*
3. *è definito un metodo per calcolare o identificare i difetti (cioè le differenze tra lo stato e il comportamento desiderati ed effettivi).*

Quando i prerequisiti sono soddisfatti, il sistema di valutazione può calcolare automaticamente dove si verificano differenze tra lo stato desiderato e lo stato effettivo (difetti), utilizzare tali informazioni per creare rapporti di valutazione della sicurezza e della privacy e consegnarli al personale designato tramite una gestione della sicurezza e della privacy.

SUGGERIMENTI

1. *Per aiutare ad automatizzare la* OA, *il* NIST *e il* DEPARTMENT OF HOMELAND SECURITY CYBERSECURITY INFRASTRUCTURE SECURITY AGENCY (CISA) *hanno collaborato allo sviluppo di un processo che sfrutta il metodo di valutazione del test ed è coerente con il* RISK MANAGEMENT FRAMEWORK, *come descritto in* SP 800-37 *e la guida* ISCM *in* SP 800-137.

2. *Il processo di automazione è descritto in* NIST INTERAGENCY/INTERNAL REPORT (NISTIR) 8011, AUTOMATION SUPPORT FOR SECURITY CONTROL ASSESSMENTS: VOL. 1: OVERVIEW [IR 8011-1] *che definisce le capacità di sicurezza specifiche e descrive* OVERALL AUTOMATED ASSESSMENT PROCESS.

3. *Metodi specifici per automatizzare la valutazione di ciascuna capacità di sicurezza definita sono forniti nei successivi volumi* NISTIR 8011.

4. *L'automazione del metodo di prova per le* SECURITY ASSESSMENT *è facilitata dal programma* CISA CONTINUOUS DIAGNOSTICS AND MITIGATION (CDM).

RIFERIMENTI

1) Appendici D e F del NIST SP 800-53A – Assessing Security and Privacy Controls in Information Systems and Organizations

2) Cybersecurity – Manuale (Autore: Pedico Aldo)

3) GDPR – Manuale Adeguamento (Autore: Pedico Aldo)