Regolamentazione attivita' di VAPT

Il cliente non deve effettuare autonomamente o tramite propri fornitori VAPT o portscan dalla propria infrastruttura di virtualizzazione o verso di essa, a causa dei possibili impatti sulla infrastruttura fisica sottostante (ad es. per eccessivo utilizzo delle risorse condivise). Attività di questo tipo verranno recepite come attacchi infrastrutturali e potrebbero scatenare azioni di trattamento degli incidenti o reattive, con conseguenze anche di tipo legale. Pertanto:

- **Il cliente deve richiedere l'autorizzazione per qualsiasi test di intrusione.**
- **Per richiedere l'autorizzazione, è necessario aver eseguito l'accesso al customerportal** utilizzando le credenziali dell'amministratore del tenant e allegare alla richiesta (coda SDGPIAS) l'apposito modulo ("Cineca Vulnerability Assessment / Penetration Testing Request Form") compilato con tutte le informazioni ed attendere l'autorizzazione a procedere; se il testing deve essere condotto da una terza parte incaricata appositamente, è necessario compilare e inviare il modulo e avvisare la terza parte quando Cineca concede l'autorizzazione. Cineca non concederà alcuna autorizzazione direttamente a terzi.
- Cineca si riserva il diritto di richiedere lo stop dell'azione di VAPT al manifestarsi di problemi sul carico dei sistemi che danneggino le performance di altri tenant.
- Non possono essere oggetto di test o portscan le interfacce di accesso alla gestione dei sistemi Cloud, al logging/monitoring e le API del sistema, che sono elementi di controllo dell'infrastruttura sotto la proprietà e responsabilità di Cineca.

Modulo CINECA Vulnerability Assessment / Penetration Testing Request Form