Bieteranfragen- 001-04

	Vergabenummer	Letzte Änderung
	EU LÖ 025/26	03.03.2026
Gesamtmaßnahme		
Modellprojekt „StraWiMa“ Landkreis Harz		
Leistung		
Durchführung eines IT-Sicherheits- und Penetrationstests		

Laufende Nummer	Frage	Antwort/Datum
1	Nach Durchsicht der Unterlagen haben sich folgende Fragen ergeben: 1. interner Penetrationstest: Anzahl Server (physisch, virtuell) / Anzahl Endpunkte (Anzahl Clients, Netzwerkgeräte). Ein circa Mengengerüst für die Einordnung und benötigter Zeitaufwand der Prüfung.	Ca. 230 virtuelle Server, dediziert physische sind nicht im Einsatz, die gesamte Umgebung läuft auf einem VSphere Cluster, 1150 Clients, davon 84 im Gesundheitsamt
	2. Es sollen iPhone/iPad Geräte geprüft werden. Für welche Anwendungen werden diese genutzt? Desweiteren wird unter Fachanwendungen beschrieben, dass Surface Pro Geräte eingesetzt werden. Diese Geräte sollen aber nicht geprüft werden ? Wie werden diese Geräte verwaltet?	iPhone/ iPad: Zugriff auf E-Mails (Postfach des jeweiligen Benutzers und zugewiesene OE-Postfächer), Terminkalender, NextCloud, Intranet LK, MS Office-Anwendungen (nur lesen), NINA-Warn-App, WebEx (Video-Konferenz-Tool), Apple-Standard-Apps (Browser Safari, Adressbuch, Rechner, Fotos, …) Surface Pro Geräte: werden über SCCM verwaltet, mit Ausnahme einer Anwendung werden alle Fachanwendungen über eine VDI Umgebung (CITRIX) bereitgestellt.
	3. Es wird beschrieben, dass die Fachanwendungen in der VDI-Umgebung verfügbar sind. Können Sie bestätigen, dass alle insgesamt aufgelisteten Fachanwendungen in der VDI-(Test)-Umgebung verfügbar sind und von remote geprüft werden können?	Alle Fachanwendungen des Gesundheits-amts sind in der VDI-Umgebung verfügbar, Ausnahme: mpMobile. mpMobile wird im Außendienst genutzt und ist nur auf Surfaces installiert. Die Anwendung mpMobile und der Zugriff auf die Mikado-Datenbank sollen auf ihre Sicherheit geprüft werden.
2	Im Bereich der Zertifizierungen wird von der ISO27001 oder BSI Zertifizierungen gesprochen, sind auch Personenzertifizierungen wie	Ja, Personenzertifizierungen sind zugelassen.

	beispielsweise eine OSCP Zertifizierung akzeptabel?	
3	Zu Ihrer Ausschreibung haben wir folgende Rückfrage. Als Leistungskriterium schreiben Sie: "Der Anbieter muss als Prüfstelle zertifiziert sein (nach ISO/IEC 27001), oder über von BSI-Auditoren erteilte Zertifikate nach BSI IT-Grundschutz oder äquivalente (z.B. „Certified Ethical Hacker“) für die eingesetzten Tester verfügen." Neben dem „Certified Ethical Hacker“ Zertifikat verfügen unsere Mitarbeitenden über folgende äquivalente Zertifikate: - ISACA Cyber Security Expert (CSE) - ISACA Cyber Security Practitioner (CSP) - ISTQB CT-SEC (Security Tester) - Skytale® Web Security Expert Welche dieser Zertifikate werden durch Sie als gleichwertig anerkannt?	Ja, die genannten Zertifizierungen werden anerkannt. Skytale® Web Security Expert alleine wäre nicht ausreichend, da es sich nur auf Webanwendungen bezieht.
4	In den Vergabeunterlagen ist im Dokument „FBH_Hinweise im Vergabeverfahren_Formulare“ das Formblatt 444 – Referenzbescheinigung enthalten. Dieses Formular bezieht sich jedoch eindeutig auf Bauvorhaben, einschließlich spezifischer Angaben zu Gewerken, Bauausführungen, Baubeginn/Fertigstellung und VOB Bezug. Da die ausgeschriebene Leistung jedoch keine Bauleistung, sondern eine Dienstleistung im Bereich IT Sicherheit/Penetrationstest betrifft, bitten wir um folgende Klärung: 1. Ist das Formblatt 444 für dieses Verfahren überhaupt anzuwenden? 2. Falls nein, bitten wir um Bereitstellung eines geeigneten Referenzformulars für Dienstleistungen bzw. um Klarstellung, welche Angaben Sie alternativ als Nachweis der technischen Leistungsfähigkeit akzeptieren.	Das Formblatt 444 ist für diese Ausschreibung nicht relevant. Als Referenz wird ein Nachweis über die erfolgreiche Durchführung von Pentests akzeptiert (was wurde wann geprüft, in welchem Unternehmen, in welchem Umfang)? Ein Nachweis kann eine schriftliche Bestätigung, eine Referenzliste oder Kontaktangaben von Ansprechpartnern sein.