Bieteranfragen- 13

	Vergabenummer	Letzte Änderung
	EU LÖ 025/26	16.03.2026
Gesamtmaßnahme		
Modellprojekt „StraWiMa“ Landkreis Harz		
Leistung		
Durchführung eines IT-Sicherheits- und Penetrationstests		

Laufende Nummer	Frage	Antwort/Datum
1.1	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
1.2	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.
1.3	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	Ja, Personenzertifizierungen sind zugelassen.

	Personenzertifizierungen wie 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.
5.1	Zu Ihrem Verfahren haben wir folgende Fragen:	Referenzen sind in diesem Verfahren bereits mit dem Angebot einzureichen.

	1. In der "Eigenerklärung zur Eignung" steht "Falls mein/unser Teilnahmeantrag/Angebot in die engere Wahl kommt, werde ich/werden wir drei Referenzen aus den letzten drei Jahren mit mindestens folgenden Angaben benennen:" Bedeutet dies, dass die Referenzen erst auf explizites Verlangen des AG vorzulegen sind	
5.2	2. Laut Formblatt 216 - Punkt 2.4 (sonstige Unterlagen) ist eine Urkalkulation einzureichen. Welche Angaben sollen aus der Urkalkulation hervorgehen? Ist ein bestimmtes Format gewünscht?	Die Urkalkulation ist gemäß FB 216 Pkt. 2 erst auf gesondertes Verlangen der Vergabestellen einzureichen.
6	Wir sind ein kleines Team, welches im aktuellen Unternehmen gerade das Thema Offensive Security aufbaut. Wir haben mit 3 Personen ca. 30 Jahre Erfahrung im IT-Security Bereich, was nachgewiesen werden kann, inklusive diverser Zertifizierungen, unter anderem den OSCP, welcher auch vom BSI anerkannt wird. Nun sind wir aber neu in diesem Unternehmen und dürfen keine Referenzen nennen, bei denen wir in den letzten Jahren Pentests und Red Teaming durchgeführt haben, da diese aus unserem alten Unternehmen stammen. Sind fehlende Referenzen in diesem Fall ein hartes Ausschlusskriterium?	Ja, fehlende Referenzen sind ein hartes Ausschlusskriterium.
7	Im Leistungsverzeichnis steht, dass die persönliche Eignung durch entsprechende Referenzen nachgewiesen werden soll, allerdings ist keine Anzahl an geforderten Referenzen angegeben. Sollte pro Person aus dem Team eine Referenz angegeben werden oder gibt es keine konkret geforderte Anzahl? Wir bitten um Klärung, da dies bei der Bearbeitung entsprechend mit berücksichtigt werden muss.	Pro Prüfer sollte mindestens eine Referenz nachgewiesen werden, insgesamt mindestens 2 Referenzen.
8.1	Bitte bestätigen Sie, ob die Anforderung „Konzept (5–10 Seiten)“ ausschließlich ein einziges, zusammenhängendes Konzept zur Durchführung des Penetrationstests	Das gesamte Konzept (alle Arbeitspakete) soll 5 – 10 Seiten (ohne Deckblatt, Inhaltsverzeichnis, Literaturverzeichnis o.ä.) umfassen.

	umfasst oder ob zusätzlich/alternativ je Arbeitspaket (Penetrationstest, Schwachstellenscan, Social-Engineering-Test) ein separates Konzept erwartet wird. Optional (falls ihr Seitenbegrenzung absichern wollt): Gilt die Seitenbegrenzung (5–10 Seiten) pro Konzeptdokument oder als Gesamtumfang über alle einzureichenden Konzeptdokumente?	
8.2	Sollen die auf Seite 4 aufgeführten Prüfobjekte separat oder in ihrer Gesamtheit getestet werden?	Die Prüfobjekte sollen generell separat betrachtet werden, Clusterungen sind mit Absprache des Auftraggebers möglich.
8.3	Wer stellt die technische Umgebung zum Betrieb der auf Seite 4 gelisteten Fachanwendungen zur Verfügung? Handelt es sich um eine on-premise Lösung oder um eine cloud-basierte Lösung?	Es handelt sich um on-premise-Lösungen im Rechenzentrum des Landkreises.
8.4	Sind für Penetrationstests/Vulnerability Scans an Fachanwendungen oder angebundenen Systemen mit Drittanbieter-/SaaS-Anteilen (z. B. SurvNet RKI, Hersteller Mikroprojekt, ggf. TEVIS/Starc medical) vorab Herstellerfreigaben erforderlich, und werden diese Freigaben durch den Auftraggeber eingeholt und bereitgestellt?	Alle Fachanwendungen sind on-premise-Lösungen ohne SaaS-Anteil. Herstellerfreigaben sind nicht erforderlich.
8.5	Bitte geben Sie je Fachanwendung die technischen Anwendungstypen an (Webanwendung, Client/Server, fat client in VDI, mobile App, API/Schnittstelle) sowie ob Schnittstellen/Integrationen (z. B. DEMIS bei SurvNet, Mikado-DB-Anbindung, Blue-Prism-VM/Schnittstellen) in den Scope fallen.	Siehe Anhang 1, Schnittstellen und virtuelle Maschinen fallen mit in den Scope.
8.6	Der Penetrationstest soll vor Ort durchgeführt werden. Bitte bestätigen Sie, ob für Vor-/Nachbereitung, Schwachstellenscans, Retests oder Dokumentation auch Remote-Zugänge (z. B. VPN) zulässig sind. Falls ja: für	Ja, Remote ist zulässig für Vor- und Nachbereitung, Dokumentation. Die Tests sind vor Ort durchzuführen. Remote-Zugänge sind per VPN und RSA-Token (2-FA) möglich.

	welche Arbeitspakete/Phasen und unter welchen Rahmenbedingungen (Zeitfenster, MFA, Jump Host)?	
8.7	Bitte erläutern Sie, ob in der Test-VDI/Testumgebung ausschließlich synthetische/anononymisierte Testdaten vorliegen oder ob (alte) Realdaten enthalten sind. Falls Realdaten vorhanden sein können: welche Schutzmaßnahmen/Regeln gelten für Testmethoden, Protokollierung und Nachweise (z. B. Screenshot-/Export-Regeln)?	In der Test-Umgebung einiger Fachanwendungen liegen veraltete Real-Daten vor. Protokollierung zwecks Nachweisführung ist erlaubt, Rücksprache und Abstimmung mit dem Auftraggeber und falls erforderlich Anonymisierung der Nachweise. AV-Vereinbarung nach DSG-VO ist abzuschließen.
9	In den Vergabeunterlagen wird keine gesonderte Regelung zur Haftung und zur Haftungsbegrenzung getroffen. Die VOL/B begrenzen die Haftung nur in besonderen Fällen, so dass die Haftung im Grundsatz unbegrenzt ist und für die Bieter ein unkalkulierbares Risiko darstellt. Branchenüblich sind hingegen beispielhaft die Regelungen der gängigen EVB-IT Verträge oder eine Beschränkung der Haftung auf den 1,5-fachen Brutto-Gesamtauftragswert. Gehen wir daher recht in der Annahme, dass Sie einer Begrenzung der Haftung auf den 1,5-fachen Brutto-Gesamtauftragswert oder nach EVB-IT zustimmen?	Zwischen Landkreis Harz und dem Auftragnehmer wird ein EBV-IT Dienstleistungsvertrag abgeschlossen, es gelten die EVB-IT Dienstleistungs-AGBs.
10.1	Unter Punkt 3.1.2 wird ein umfassender Schwachstellenscan der IT-Systeme gefordert , während unter Punkt 3.1.1 ein Penetrationstest der Fachanwendungen spezifiziert wird. Der besondere Schwerpunkt soll auf den Mikroprojekt-Anwendungen liegen. Dürfen wir zur strukturierten Aufwandsabschätzung davon ausgehen, dass die priorisierten Anwendungen einem tiefgehenden manuellen Applikations-Pentest (z.B. nach OWASP) unterzogen werden, während die restlichen Systeme (wie TEVIS, OctoWare) primär über den automatisierten Schwachstellenscan abgedeckt werden?	Die Mikroprojekt-Anwendungen und die Fachverfahren Octoware und SurvNet sollen einem tiefgehenden manuellen Penetrationstest unterzogen werden.
10.2	In Punkt 3.1.1 wird die Überprüfung von verwalteten mobilen Geräten (iPad / iPhone) gefordert. Bezieht sich	EMM soll geprüft werden, auf den mobilen Geräten gibt es keine spezifischen Fachverfahren.

	diese Prüfung auf das Configuration Review des Mobile Device Managements (EMM) oder auf einen technischen Penetrationstest der darauf installierten Client-Applikationen?	
10.3	Im Rahmen des Social-Engineering-Tests werden u.a. Phishing-Kampagnen, Pretexting, Honeypots und physische Zugangstests gefordert. Um die Testdurchführung effizient zu bündeln: Ist es im Sinne des Auftraggebers, diese Maßnahmen in klar abgegrenzte Module (z.B. Modul A: Digitale Kampagne/Phishing, Modul B: Vor-Ort-Szenarien/Physischer Zugang) zu unterteilen, um den operativen Ablauf im Gesundheitsamt nicht unnötig zu stören?	Ja.
10.4	Bezüglich des physischen Zugangstests zu Rechenzentren und Büros: Ist hierfür ein fixes Zeitkontingent vorgesehen?	Physische Zugangstests sollen während der Dienstzeit, im Zeitfenster Montag – Donnerstag, von 8:00 bis 15:00 Uhr durchgeführt werden.
10.5	Unter Punkt 3.2 wird eine vorsichtige Vorgehensweise gefordert, um Beeinträchtigungen auszuschließen. Gleichzeitig ist eine Test-VDI-Umgebung vorhanden. Stehen für die im Fokus stehenden Fachanwendungen voll funktionsfähige Testinstanzen mit synthetischen Testdaten (ohne echte Gesundheitsdaten) zur Verfügung, auf denen auch destruktive Testpfade (z.B. SQL-Injection) risikofrei verifiziert werden können?	Die Anwendungen des Gesundheitsamts stehen in der Test-VDI-Umgebung zur Verfügung (außer die Anwendung SurvNet RKI). In der Test-Umgebung einiger Fachanwendungen liegen veraltete Real-Daten vor.
10.6	Für Systeme wie SurvNet RKI wird angemerkt, dass die Software vom RKI zur Verfügung gestellt wird. Liegt für fremdgehostete oder von Bundesbehörden bereitgestellte Anwendungen eine explizite Testfreigabe (Rules of Engagement/Permission to Attack) der jeweiligen Hersteller/Betreiber vor, oder beschränkt sich der Test hier rein auf die lokale Client-Sicherheit?	Die Anwendung SurvNet wird im LK Harz on-premise betrieben.
10.7	Unter Punkt 3.1.1 wird die Bewertung einer XDR-Integration hinsichtlich Vor- und Nachteilen für die IT-Infrastruktur gefordert. Da es sich hierbei um eine strategische Beratungsleistung	Ja.

	handelt, die sich oft erst aus den Gesamtergebnissen des Audits ableitet: Soll dieser Punkt als separates Arbeitspaket im Konzept ausgewiesen werden?	
11	Bitte erläutern Sie, auf welcher Vertragsgrundlage angeboten werden soll, da diese der Vergabe nicht beigefügt waren. Insbesondere regen wir an, die branchenüblichen EVB-IT Dienstleistung Vorlage und AGB zu verwenden, da diese die notwendige Haftungsbeschränkung enthält, die alle Unternehmen im Rahmen der allgemeinen Risikomanagementanforderungen vorweisen können müssen.	Zwischen Landkreis Harz und dem Auftragnehmer wird ein EBV-IT Dienstleistungsvertrag abgeschlossen, es gelten die EVB-IT Dienstleistungs-AGBs.
13.1	Im „Leistungsverzeichnis_LK Harz 24.02.26“ wird gefordert, dass der Anbieter „als Prüfstelle zertifiziert sein muss (nach ISO/IEC 27001)“. Nach unserem Verständnis beschreibt die Norm ISO/IEC 27001 primär Anforderungen an ein Informationssicherheits-Managementsystem (ISMS) von Organisationen. Eine Zertifizierung „als Prüfstelle“ im Sinne einer Stelle, die selbst Audits bzw. Zertifizierungen durchführen darf, erfolgt hingegen üblicherweise auf Grundlage akkreditierungsrelevanter Normen wie z. B. ISO/IEC 17021 in Verbindung mit ISO/IEC 27006. Vor diesem Hintergrund bitten wir um Klarstellung: 1. Ist mit der genannten Anforderung gemeint, dass der Anbieter selbst über eine gültige ISO/IEC 27001-Zertifizierung für sein Unternehmen bzw. sein ISMS verfügt?	Es wäre wünschenswert, wenn der Anbieter über eine gültige ISO/IEC 27001-Zertifizierung für sein Unternehmen bzw. sein ISMS verfügt.
13.2	2. Oder beabsichtigt der Auftraggeber tatsächlich, dass der Anbieter eine akkreditierte Zertifizierungs- bzw. Prüfstelle ist, die selbst ISO/IEC 27001-Audits bzw. Zertifizierungen durchführen darf? Sollte Letzteres gemeint sein, bitten wir zudem um kurze Begründung der Anforderung bzw. um Prüfung, ob alternativ auch Unternehmen mit eigener ISO/IEC 27001-Zertifizierung	Der Anbieter muss keine akkreditierte Zertifizierungs- bzw. Prüfstelle sein. Es wäre wünschenswert, wenn der Anbieter nachweisen kann, dass sein Unternehmen effektive Sicherheitskontrollen und -prozesse implementiert hat und über eine gültige ISO/IEC 27001-Zertifizierung für sein Unternehmen bzw. sein ISMS verfügt.

	als ausreichend angesehen werden können, da die Anforderung an eine akkreditierte Prüfstelle den potenziellen Bieterkreis erheblich einschränken könnte.	