Landkreis Harz
Der Landrat

Finanziert von der Europäischen Union
NextGenerationEU

Vergabeverfahren

Leistungsbeschreibung: Penetrationstest im Rahmen des ÖGD-Projekts

Inhalt:

Sitz der Verwaltung:
Friedrich-Ebert-Str. 42
38820 Halberstadt
Telefon: (0 39 41) 59 70 - 0
Telefax: (0 39 41) 59 70 - 43 33
Internet: www.kreis-hz.de
E-Mail: info@kreis-hz.de

Öffnungszeiten:
Montag: 8:00 – 12:00 und 13:00 – 16:00 Uhr
Dienstag: 8:00 – 12:00 und 13:00 – 16:00 Uhr
Mittwoch: 8:00 – 12:00 und 13:00 – 16:00 Uhr
Donnerstag: 8:00 – 12:00 und 13:00 – 16:00 Uhr

Bankverbindung:
Harzsparkasse
IBAN: DE33 8105 2000 0370 0831 05
BIC: NOLADE21HRZ

1. Ausgangssituation

Der Landkreis Harz beteiligt sich mit dem Modellprojekt „SePro Harz- Aufbau Serverlandschaft und Ausweitung Prozessdigitalisierung im Gesundheitsamt des Landkreises Harz“ am Förderprogramm zur Digitalisierung der Gesundheitsämter durch die Steigerung und Weiterentwicklung des digitalen Reifegrades des öffentlichen Gesundheitsdienstes.

Im Rahmen der Förderung aus dem Pakt für den ÖGD sind den Erfordernissen u.a. der Interoperabilität, der IT-Sicherheit, der Informationssicherheit und des Datenschutzes nach dem Stand der Technik Rechnung zu tragen. Daher hat das Gesundheitsamt bei der Erarbeitung des Modellprojektes „SePro Harz“ ein Unterprojekt „IT-Sicherheit“ mit eingeplant. Ein Bestandteil dieses Projekts ist die Durchführung umfassender Sicherheitstests (Penetrationstest).

2. Zielsetzung

Die IT-Systeme, Anwendungen, Netzwerke sowie personelle und organisatorische Maßnahmen des Landkreises Harz sollen auf ihre Sicherheit geprüft werden. Im Mittelpunkt des Projekts steht das Gesundheitsamt des Landkreises Harz, hier sollen insbesondere Fachanwendungen berücksichtigt werden. Um Sicherheitslücken aufzuspüren, bevor diese durch reale Angreifer ausgenutzt werden, soll ein Penetrationstest durchgeführt werden. Mittels Durchführung realistischer Simulationen in Form von Angriffsszenarien sollen im Gesundheitsamt potentielle Risiken frühzeitig erkannt und durch geeignete Maßnahmen vermindert werden.

Zur Identifikation, Analyse und Minimierung von Sicherheitsrisiken soll ein Penetrationstest in Form eines „Grey box“- Tests durchgeführt werden.

Das Projekt zum Penetrationstest soll **05/2026** beginnen und muss am **31.07.2026** abgeschlossen sein. Aufgrund von bewilligten Fördermitteln und der damit verbundenen Fristen, muss eine Abrechnung der Leistungen so erfolgen, dass die Projektabschlussrechnung zum **31.07.2026** dem Gesundheitsamt Harz vorliegt.

Um Interessenskonflikte zu vermeiden, ist der Penetrationstest durch einen externen Dienstleister durchzuführen, der nicht bei der Konzeption, am Aufbau und Betrieb der IT-Systeme am LK Harz beteiligt war bzw. ist.

3. Leistung

Technische und organisatorische Fragen zum Test und zum Vorgehen sollen in einer gemeinsamen **Kick-Off-Veranstaltung** (Auftragnehmer und Auftraggeber) entwickelt und ein Testkonzept erstellt werden. Zusammen mit dem Auftraggeber sollen das Ziel, die Auswahl von Werkzeugen und Methoden, die Durchführung sowie Dokumentation des Penetrationstests abgestimmt werden. Projektbegleitend werden Besprechungen zur Planung/ Durchführung (z.B. vereinbaren von Zeitfenstern, Vorstellung der geplanten Maßnahmen und Werkzeuge) der einzelnen Leistungen/ Aufgabenpakete (Penetrationstest, Schwachstellenscan, Social-Engineering-Test) mit dem Auftraggeber durchgeführt, diese Abstimmungen können online (in Form von Videokonferenzen) stattfinden.

Der Penetrationstest soll vor Ort durchgeführt werden.

Der Auftragnehmer übernimmt im Rahmen seiner Tätigkeit die Bereitstellung aller notwendigen technischen Tools und Programme zur Überprüfung, Modellierung und Dokumentation, so dass für den Auftraggeber keine zusätzlichen Software- bzw. Lizenzkosten entstehen. Entsprechende Zugänge auf die zu prüfenden Systeme werden vom Auftraggeber zur Verfügung gestellt.

Für die Angebotsauswertung muss zwingend ein Konzept zur Durchführung des Penetrationstests eingereicht werden. Das Konzept soll technische als auch organisatorische Aspekte berücksichtigten. Anzugeben sind insbesondere die durchzuführenden Methoden und zu nutzenden Werkzeuge und die dazugehörige Art der Dokumentation für den Auftraggeber.
Es ist im Rahmen dieses Konzeptes eine Aufwandschätzung abzugeben, die die Anzahl der durchführenden Personen und die Anzahl der benötigten Tage beinhaltet, um den Penetrationstest innerhalb der Vertragslaufzeit durchzuführen und abzuschließen.
Planung und Umsetzung des Penetrationstests sollen im Konzept plausibel und für den Auftraggeber nachvollziehbar sein. Das Konzept beinhaltet den organisatorischen Aufbau des Penetrationstests (Projektplan), den zeitlichen Ablauf (Meilensteinplanung / Zeitachse) und die technische Projektumsetzung (Auflistung der eingesetzten Hard- und Software). Das Konzept umfasst mind. 5, max. 10 Seiten.

3.1. Umfang

Die ausgeschriebene Leistung beinhaltet die folgende Arbeitspakete:

3.1.1. Penetrationstest

Der Penetrationstest soll durch realistische Simulation von Angriffsszenarien interne und externe IT-Komponenten und die Fachanwendungen des Gesundheitsamts auf Sicherheitsrisiken prüfen sowie die damit vernetzten Systeme bzw. Plattformen im IT-Informationsverbund des Landkreises Harz.

Im Landkreis Harz werden mobile Geräte (iPad / iPhone) verwendet, die per EMM-Plattform verwaltet werden. Diese Lösung bzw. die verwalteten Geräte sollen ebenfalls im Rahmen des Penetrationstests auf ihre Sicherheit geprüft werden.

Nach Abschluss des Penetrationstests soll die Wirksamkeit der aktuellen Sicherheitsmaßnahmen bewertet, Schwachstellen aufgedeckt und konkrete Verbesserungsmaßnahmen vorgeschlagen werden. Des Weiteren soll eine XDR-Integration und dessen Nutzung für den Landkreis in Bezug auf seine Vor- und Nachteile in der jetzigen vorhandenen IT-Infrastruktur bewertet werden.

3.1.2. Schwachstellenscan

Die IT-Systeme, (interne und externe) Netzwerke und Anwendungen sollen einem umfassenden Schwachstellen-Scan unterzogen werden. Dabei sollen (evt.) unsichere Dienste, fehlerhafte Konfigurationen und Sicherheitslücken identifiziert werden. Server, Workstations, mobile Geräte und Web-Anwendungen sollen überprüft werden. Die erkannten Schwachstellen sollen in einem Bericht dargestellt und bewertet werden und Handlungsempfehlungen inkl. Priorisierung zwecks Behebung der Schwachstellen aufgezeigt werden.

3.1.3. Social-Engineering-Tests

Im Landkreis Harz wurden 2024, 2025 und 2026 alle Mitarbeiter in Security Awareness-Schulungen im Umgang mit Social-Engineering-Angriffen geschult. In einem Social-Engineering-Test sollen auch die „menschlichen Sicherheitsbarrieren“ und die organisatorischen Abläufe, mit Fokus auf das Gesundheitsamt getestet werden. Es soll vor allem eine Phishing-Kampagne durchgeführt werden. Weitere Maßnahmen wie z.B. Pretexting, Installation eines „Honeypot“ mit dem Angebot für kostenloses WLAN, physische Zugangstests (Überprüfung der Zugangskontrollen durch unbefugtes Betreten von Gebäuden oder Büros) sind in das Social-Engineering Konzept mit einzubeziehen.

Dokumentationen zu den Prüfobjekten (IT-Strukturpläne, Netzwerk- und Raumpläne, Inventarlisten) werden vom Auftraggeber vorgehalten.

Prüfobjekte:

- Intern:	zentrale IT-Infrastruktur: Betriebssysteme Server, VDI (virtuelle Umgebung des Gesundheitsamts), Netzwerke, Dateiserver, DMS (Dokumentenmanagementsystem) - generelle Prüfung der Umgebung an einem Arbeitsplatz des Gesundheitsamts - Portnutzung WAN LK Harz (mit einem Gerät des Testers) - Virenschutz-Software
Extern:	Test Angriffsoberfläche DMZ, Firewalls, Server, Dienste (VPN, E-Mail, Behördenpostfach usw.), Voice (stationäre Telefonie), Online-Terminvergabe, Mobile Device Management (EMM)
- Physische Zugänge:	zu Büros / Arbeitsplatz, zum Rechenzentrum, Serverräume / IT-Technikräume, Gebäude
- mobile Geräte:	zentral konfiguriert durch EMM (Enterprise Mobility Management)

Die Fachanwendungen des Gesundheitsamts sollen im Fokus stehen:

SurvNet RKI:	Software zur Erfassung, Auswertung und Weiterleitung von Meldedaten gemäß IfSG, Übermittlung der Daten von Gesundheitsämtern an die zuständigen Landesbehörden per DEMIS-Schnittstelle, weitere Übermittlung an das RKI, Software wird vom RKI zur Verfügung gestellt Personenbezogene Daten/ Gesundheitsdaten werden verarbeitet
MikroProjekt-Software (Averso, Health, WHealth)	
- Averso:	Dokumentation der Erstuntersuchung von Asylbewerbern Export von Daten ins Ausländerzentralregister Personenbezogene Daten/ Gesundheitsdaten werden verarbeitet
- Health:	Dokumentation von Meldungen nach IfSG Personenbezogene Daten/ Gesundheitsdaten werden verarbeitet
- WHealth:	Verwalten aller Wasserarten - Trinkwasser, Badewasser, EG-Badewasser, Wasser aus Schwimmbädern und Hallenbädern, sonstige Wasserarten - Anwendung auf mobilen Geräten im Außendienst, Synchronisation der Daten Erfassen, bearbeiten, überwachen und auswerten aller Informationen zu Adressen, Objekten, Objekt-Zusatzdaten, Terminen, Proben, Besichtigungen, Auffälligkeiten, dem kompletten Schriftverkehr, eingehenden Informationen, Gebühren, Zeitplänen etc.
OctoWare:	Software unterstützt Arbeitsabläufe im Gesundheitsamt - Organisation und Dokumentation von bspw. Untersuchungen im ärztlichen, zahnärztlichen und sozialpsychiatrischen Dienst, gruppenprophylaktischen Maßnahmen in Schulen, Begutachtungen, Auswertungen, Fallstatistiken Personenbezogene Daten/ Gesundheitsdaten werden verarbeitet

TEVIS:	Online Terminkalender für den gesamten Landkreis Im Gesundheitsamt: Termine für Belehrungen, Schulerstuntersuchungen Weboberfläche für Bürger Personenbezogene Daten
Starc medical:	Röntgenuntersuchungen mit externer Befundung im AMEOS-Klinikum Personenbezogene Daten/ Gesundheitsdaten werden verarbeitet
Blue Prism:	Prozess-Automatisierung (RPA) Simulation der Tätigkeiten von Anwendern Personenbezogene Daten/ Gesundheitsdaten werden verarbeitet Diverse virtuelle Maschinen und Schnittstellen zu Fachanwendungen bestehen

Besonderer Schwerpunkt des IT-Sicherheitstests liegt auf den Anwendungen „Mikado Health“, „Mikado WHealth“ und „Averso“ der Firma Mikroprojekt GmbH.
Die Mitarbeiter des Gesundheitsamts im Außendienst arbeiten mit Geräten Surface Pro 7+. Auf den Surfaces wird eine Anwendung (mpMobile) für die Bearbeitung von Probenbegleitscheinen im Außendienst genutzt, dafür werden Daten der Mikado-Datenbank ausgetauscht.
Im Rahmen des Penetrationstests soll die Sicherheit des Zugriffs auf die Mikado- Datenbank getestet werden.

Die Fachanwendungen des Gesundheitsamts sind in der VDI-Umgebung des Landkreises verfügbar. Eine Test-VDI-Umgebung (analog zur Produktiv-Umgebung) ist vorhanden.

3.2. Aggressivität

Es soll ein vorsichtiger Penetrationstest durchgeführt werden, gefundene Schwachstellen nur dann ausgenutzt, wenn nach bestem Wissen eine Beeinträchtigung des untersuchten Systems ausgeschlossen werden kann.
Intern bekannte Systeme mit Sicherheitslücken werden im Vorfeld als Einstieg ausgeschlossen.

4. Ergebnis

Zum Penetrationstest soll eine Dokumentation durch den Auftragnehmer erstellt werden. Inhalt der Dokumentation sollen die Angriffe selbst, die Angriffsszenarien, die Beweisführung für das Aufdecken von Sicherheitslücken sein.
Die Ergebnisse des Penetrationstests sollen auf verständliche Art und Weise / für den Auftraggeber nachvollziehbar im Bericht dargestellt und Risiken bewertet werden. Automatisierte Berichte, z.B. Ergebnisberichte von Prüfwerkzeugen sind lediglich im Anhang des Ergebnisberichts zu finden. Der Bericht soll Empfehlungen enthalten, wie die im Penetrationstest erkannten Sicherheitslücken geschlossen werden können. Welche kurzfristigen Maßnahmen sollten durchgeführt und langfristige Strategien aufgezeigt werden.
Die Ergebnisse des Penetrationstests müssen in einer Präsentation dem Landkreis Harz vorgestellt und in Form **eines abschließenden Workshops** diskutiert werden.

5. Persönliche Eignung

Alle zur Leistungserbringung eingesetzten Personen müssen die deutsche Sprache in Wort und Schrift sehr gut beherrschen. Die deutsche Sprache ist verbindlich für alle Dokumentationen, Berichte und in allen Besprechungen.

Das Testteam sollte aus mindestens zwei Personen bestehen. Während der gesamten Projektlaufzeit hat der Auftragnehmer dem Auftraggeber aussagekräftige Ansprechpersonen in allen Bereichen zur Verfügung zu stellen. Der Auftragnehmer hat eine Projektleitung und eine stellvertretende Projektleitung zu benennen. Die genauen Kontaktdaten sind bei Projektstart dem Auftraggeber zu benennen.

Das Testteam muss über spezielle technische, methodische und fachliche Fähigkeiten sowie persönliche Kompetenzen verfügen.
Die eingesetzten Prüfer besitzen Erfahrungen in System- und Netzwerk-Administration, IT-Sicherheitsprodukten, Informationssicherheit, haben eine technische Ausbildung absolviert und besitzen Berufserfahrung im Bereich Systemadministration o.ä. Nachweise über die Qualifikation von mindestens zwei Mitarbeitern sind dem Auftraggeber vorzulegen. Die Prüfer müssen über Erfahrungen bei der Durchführung von Penetrationstests verfügen, idealerweise im öffentlichen Sektor. Referenzen sind dem Auftraggeber vorzulegen. 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. Nachweise (Zertifikate, fachliche Qualifikationen) sind dem Auftraggeber vorzulegen.

Die eingesetzten Tester des Auftragnehmers besitzen zur erfolgreichen Umsetzung der Leistungen folgende Fach- und Methoden Kompetenzen:

- Mehrjährige Kenntnisse zu Angriffstechniken und Schwachstellenanalyse (z.B. Zero-Day-Schwachstellen, SQL-Injection)
- Erfahrung mit OWASP Top 10, MITRE ATT&CK-Framework oder weiteren gleichwertigen Standards zur Identifikation und Klassifikation von Sicherheitsrisiken
- Kenntnisse der Penetrationstest-Methodik (z.B. Black-Box-, White-Box- und Grey-Box-Tests)
- Sicherer Umgang mit Tools für Penetrationstests (u.a. Netzwerk-Scanner, Schwachstellenscanner, Sicherheitsanalyse-Tools)
- Kenntnisse über Sicherheitsstandards und regulatorische Anforderungen, insbesondere ISO 27001 und BSI IT-Grundschutz

Anlagen:
- Preisblatt für Bieter Durchführung Pentest