

Maßnahme	Tool zum automatisierten Pentesting
Vergabenummer	F017-26-001

## Leistungsbeschreibung

### 1. Allgemeine und projektbezogenen Informationen

#### 1.1. Auftraggeber und Rahmenbedingungen

Das Krankenhaus Barmherzige Brüder Regensburg ist mit 985 Betten das größte katholische Krankenhaus Deutschlands sowie Lehrkrankenhaus der Universität Regensburg. An den beiden Häusern Prüfeninger Straße (Prüfeninger Straße 86, 93049 Regensburg) und Klinik St. Hedwig (Steinmetzstraße 1-3, 93049 Regensburg) kümmern sich rund 3.800 Mitarbeitende in 30 Kliniken und Instituten sowie in 34 Zentren um die Versorgung von jährlich etwa 46.000 stationären und 150.000 ambulanten Patienten. Seit 2021 hat das Krankenhaus Barmherzige Brüder Regensburg den Auftrag eines Maximalversorgers übertragen bekommen.

Allgemeine Informationen zum Auftraggeber	
Rechtsträger/ Auftraggeber	Barmherzige Brüder gemeinnützige Krankenhaus GmbH
Standort	Krankenhaus Barmherzige Brüder Regensburg
Straße und Hausnummer	Prüfeninger Straße 86
PLZ und Ort	93049 Regensburg

#### 1.2. Ausgangslage und bestehende Systemlandschaft

Mit der vorliegenden Beschaffung nach § 16 DVBayKrG, orientiert an einer öffentlichen Ausschreibung nach § 9 UVgO, möchte der Auftraggeber Barmherzige Brüder gemeinnützige Krankenhaus GmbH, Krankenhaus Barmherzige Brüder Regensburg (nachfolgend auch „Auftraggeber“) ein Tool für automatisiertes Pentesting, das kontinuierlich die Sicherheitslage einer IT-Infrastruktur durch simulierte Cyberangriffe überprüft, einführen.

#### Bestehende Systemlandschaft des Auftraggebers

##### Infrastruktur intern:

- Windows-Server: ca. 1.500
- Linux-Server: ca. 450
- Windows-Arbeitsplätze: ca. 5.000
- Windows-Benutzer: ca. 12.000
- Appliances: ca. 50
- Interner Microsoft-Mail-Server mit ca. 15 Maildomänen
- 7 verbundene Domänen mit Active-Directory
- 100 IP-Adressen / Domänen, die durch den Auftraggeber verwaltet werden und teilweise Verbindung nach intern haben und teilweise über das Internet erreichbar sind.
- Keycloak als Identity- und Access-Management-Lösung

##### Cloud-Schnittstelle:

- Anbindung von Entra-ID an ein internes zentrales Active-Directory

**Cloud:**

- 30 extern gehostete Web-Auftritte die keine Verbindung zur internen Infrastruktur haben

### **1.3. Zielsetzung der Beschaffung**

Kritische Infrastrukturen müssen gemäß NIS2-Umsetzungsgesetz und KRITIS-Dachgesetz die Wirksamkeit ihrer Cybersicherheitsmaßnahmen durch regelmäßige, risikobasierte Tests nachweisen. Dazu gehören insbesondere Penetrationstests. Die zu beschaffende Lösung dient dazu, das einzuhaltende Sicherheitsniveau nachzuweisen und aufrecht zu erhalten. Die Lösung soll automatisiert Schwachstellen und Angriffspfade identifizieren, bevor echte Angreifer diese ausnutzen können.

Mit dieser Lösung soll sichergestellt werden, dass die IT-Sicherheitsstrategie jederzeit dem aktuellen Bedrohungsniveau entspricht und die Vertraulichkeit, Integrität und Verfügbarkeit von Patientendaten nachhaltig geschützt sind.

Das Verfahren und die Ergebnisse müssen als Nachweise für Audits und Compliance-Anforderungen (insbesondere ISO 27001, NIS2, KRITIS) genutzt werden können.

## **2. Anforderungen an den Leistungsgegenstand (*Musskriterien*)**

Die Lösung muss zwingend für die interne Validierung als selbstverwaltete Software On-Premise verfügbar sein, für die externe Validierung ist der Einsatz einer SaaS Anwendung gestattet.

Alle sensiblen Daten verbleiben vollständig im Rechenzentrum des Auftraggebers. Die Lösung gewährleistet vollständige Datenhoheit und -kontrolle.

Die Lösung benötigt für die Durchführung interner Testszenarien keine Internetverbindung. Der Einsatz in isolierten (air-gapped) Umgebungen muss dafür unterstützt werden.

Die Lösung arbeitet agentenlos, d. h. ohne Installation von Software-Agenten auf den Zielsystemen.

Die Lösung deckt internes Pentesting, Pentesting von Cloud-Anwendungen sowie das Pentesting von Cloud-Schnittstellen ab.

Alle Tests erfolgen unter realen Bedingungen – es handelt sich um keine Simulation. Die tatsächliche Wirksamkeit der Sicherheitsmechanismen wird geprüft, ohne Datenverlust oder Betriebsunterbrechungen zu verursachen. Dies gilt ausdrücklich auch für kritische Szenarien wie Ransomware-Angriffe oder den Missbrauch kompromittierter Zugangsdaten, ohne die Geschäftskontinuität oder die Verfügbarkeit medizinischer Systeme zu gefährden.

Die Lösung unterstützt dynamische Angriffsketten umfassend, einschließlich Remote Code Execution (RCE), Lateral Movement, Privilege Escalation und Post-Exploitation. Erlangte oder bereitgestellte Zugangsdaten werden für laterale Bewegungen und Privilegienerweiterungen über mehrere Systeme hinweg identifiziert und nachverfolgt.

Unterstützt werden vollautomatisierte Tests ohne manuelle Eingriffe sowie benutzerdefinierte Testszenarien in den Modi Black-Box, Grey-Box und Targeted.

Die Lösung emuliert bekannte Ransomware-Familien, mindestens: REvil, Maze, Conti, LockBit und Qilin.

Die Lösung umfasst eine Command-and-Control-Server-Emulation (C2/C&C) zur Durchführung von Tests auf Datenabfluss.

Die Lösung verfügt über eine AD-Passwort-Cracking-Engine, die Dark-Web-Daten sowie integrierte und benutzerdefinierte Wörterbücher nutzt. Darüber hinaus prüft die Lösung, ob bestehende Zugangsdaten im Open, Deep oder Dark Web kompromittiert wurden.

Die Lösung führt simulierte Angriffe nach dem MITRE ATT&CK-Framework gegen Cloud-Infrastrukturen durch, konkret gegen: Identitäten (z. B. IAM-Rollen, Dienstkonto, Benutzerrechte), Workloads (z. B. VMs, Container, Serverless Functions) und Daten- und Speicherressourcen (z. B. S3-Buckets, Blob Storage, Datenbanken)

Die Lösung stellt folgende Funktionsbereiche in einer integrierten Plattform bereit: externe Angriffssimulation, interne Angriffssimulation, Schwachstellenmanagement sowie automatisiertes Pentesting.

Die Lösung ermöglicht eine einfache und flexible Konfiguration der oben genannten Testszenarien

Die Lösung identifiziert Schwachstellen und priorisiert diese anhand ihrer Ausnutzbarkeit und der potenziellen geschäftlichen Auswirkungen. Die Ergebnisse bilden die Grundlage für eine effektive Risikobewertung und Maßnahmenplanung.

Die Lösung liefert umfassende, aussagekräftige Berichte – beispielsweise Resilience Score und Trendanalysen – mit konkreten Handlungsempfehlungen zur Verbesserung der Cyber-Resilienz.

### **3. Implementierung, Abnahme**

Der Auftragnehmer implementiert seine Software-Lösung beim Auftraggeber. Dabei begleitet und berät er den Auftraggeber vor und während der gesamten Implementierung. Im Preisblatt ist ein Pauschalpreis für die Implementierungsleistungen anzugeben. Die Implementierung schließt eine Onboarding-Architekturberatung durch Experten des Auftragnehmers ein.

Die Abnahme der Implementierungsleistung erfolgt in zwei Stufen: einer technischen Abnahme sowie einer fachlichen Abnahme. Beide Stufen sind vom Auftraggeber schriftlich zu bestätigen.

#### **Stufe 1 – Technische Abnahme**

Die technische Abnahme erfolgt, wenn folgende Kriterien vollständig erfüllt sind:

- Die Lösung ist vollständig installiert und in der definierten On-Premise-Umgebung des Auftraggebers lauffähig.
- Die Lösung ist in den definierten Netzsegmenten erreichbar und agentenlos funktionsfähig.
- Die Benutzer- und Rollenverwaltung ist eingerichtet.
- Der Betrieb in der air-gapped Umgebung wurde erfolgreich verifiziert.
- Alle Testergebnisse eines initialen Referenztests (Proof-of-Function) wurden durch den Auftragnehmer dokumentiert und dem Auftraggeber übergeben.

#### **Stufe 2 – Fachliche Abnahme**

Die fachliche Abnahme erfolgt, wenn folgende Kriterien vollständig erfüllt sind:

- Alle vertraglich vereinbarten Schulungen (Administration, Reporting, Anwendung) wurden durchgeführt.
- Die Dokumentation (Betriebsanleitung, Administrationshandbuch) liegt vollständig in deutscher Sprache vor.
- Ein vollständiger Testlauf mit mindestens einem internen und einem externen Angriffsszenario wurde erfolgreich durchgeführt und dokumentiert.
- Die erzeugten Berichte (Executive Summary, Management Summary, Aktionsbericht) wurden auf Vollständigkeit und inhaltliche Korrektheit geprüft.
- Der Remediation-Lifecycle ist für mindestens einen Testbefund vollständig abgebildet und nachvollziehbar dokumentiert.

## Service und Support

Der Auftragnehmer gewährleistet Support über die gesamte Vertragslaufzeit von drei Jahren. Der Support ist werktags (Montag bis Freitag, 8:00 bis 17:00 Uhr) per Hotline erreichbar.

## Schulungen

Der Auftragnehmer führt folgende Schulungen durch:

- 1 x 1 Tag (à 8 Std.) Schulung der Administratoren, max. 5 Teilnehmer  
Systemkonfiguration, Basisparameter, Berechtigungskonzepte
- 2 x 1 Tag (à 8 Std.) Schulung Reporting, max. 5 Teilnehmer  
Meldungen und Reports erstellen und konfigurieren. Individuelle Anpassungen direkt an den Reports im System durchführen.
- 2 x 1 Tag (à 8 Std.) Schulung der Anwendung, ca. 10 Teilnehmer  
Einführen und erklären der Software, der Dashboards und der möglichen Test-Szenarien.  
Erstellen von Testszenerarien, Interpretation der Ergebnisse, Umsetzen von Mitigationsmaßnahmen.

Die Schulungen können nach Wahlrecht des Auftragnehmers online oder beim Auftraggeber durchgeführt werden. Soweit technisch möglich, erfolgen alle Schulungen an der installierten Software des Auftraggebers.

## 4. Anforderungen an den Auftragnehmer und das einzusetzende Personal (Eignung)

### 4.1 Anforderungen an das Unternehmen

Der Auftragnehmer ist nach ISO 27001 zertifiziert.

Der Auftragnehmer hält den höchsten Partnerstatus beim Hersteller der angebotenen Lösung. Dieser Partnerstatus besteht seit mindestens 2024.

### 4.2 Anforderungen an das Personal

Für die gesamte Implementierungsphase muss der Bieter Mitarbeiterinnen und Mitarbeiter einsetzen, deren fachliches Knowhow sich nicht nur auf die Kenntnis der Software fokussiert, sondern bei denen auch fundierte Kenntnisse der betroffenen Prozesse (Angriffsszenarien, Schwachstellen) vorhanden sind.

Da die Beratungskompetenz der Mitarbeitenden des Auftragnehmers entscheidend für den Projekterfolg ist, haben die Bieter mit dem Angebot Mitarbeiterprofile für die auf dem Projekt einzusetzende Projektleitung und für weitere im Unternehmen vorhandene fachliche Mitarbeitende mit namentlicher Benennung beizufügen. Die Mitarbeiterprofile sollen dabei sowohl die Kompetenzen der Projektleitung als auch die der fachlichen Mitarbeitenden hinsichtlich vergleichbarer Projekte darstellen.

Mindestanforderungen an das Personal des Auftragnehmers sind:

#### Erstes Profil: Projektleitung

- Mindestens 5 Jahre Berufserfahrung als Projektleitung; dabei ist es wichtig, dass Erfahrungen in der Integration der angebotenen Lösung vorhanden sind.
- Mindestens zwei absolvierte Projekte in einer ähnlichen Größenordnung im Kontext der Umsetzung der angebotenen Lösung bei Kunden in der Rolle des Projektleiters, optimalerweise im Krankenhauskontext.

## Zweites Profil: Fachliche Mitarbeitende

Der Bieter hat mindestens einen und maximal drei fachliche Mitarbeitende zu benennen, die die nachfolgenden Anforderungen in der Summe erfüllen. Sofern ein fachlicher Mitarbeiter oder eine fachliche Mitarbeiterin die Anforderungen aus mehreren Kategorien für fachliche Mitarbeitende erfüllt, muss für die erfüllten Kategorien kein zusätzlicher fachlicher Mitarbeiter oder fachliche Mitarbeiterin benannt werden. Maßgeblich ist, dass sämtliche Anforderungen erfüllt werden.

### Anforderungen an die fachlichen Mitarbeitenden bezüglich der angebotenen Lösung

- Nachweis der Fachkompetenz bezüglich der angebotenen Lösung durch entsprechende Zertifizierungen, wie z.B. aktuelle Herstellerzertifizierungen.
- Mindestens fünf absolvierte Implementierungen, optimalerweise im Krankenhauskontext.

### Anforderungen an die fachlichen Mitarbeitenden im Bereich Pentesting

- Nachweis der Fachkompetenz im Pentesting durch mindestens drei durchgeführte externe Pentests in den letzten 3 Jahren bei Unternehmen vergleichbar dem Auftraggeber.

Die vollständigen Eignungsanforderungen ergeben sich aus Dokument 10 (Eigenerklärung zur Eignung). Die in dieser Ziffer 4 beschriebenen Anforderungen werden durch das vom Bieter ausgefüllte Dokument 10 nachgewiesen.

## 5. Mengengerüst

Es wird folgende Software inkl. Wartungsleistungen beschafft:

Nr.	Leistungsgegenstand	Menge	Laufzeit
<b>Softwaremietmodell</b>			
1	Softwarelösung "Penetrationstest-Tool" inkl. Upgrades und Updates für 36 Monate	1 Stück	36 Monate

## 6. Anforderungen an die Leistungserbringung (Kann-Kriterien, die zu einer höheren Bewertung im Rahmen der Zuschlagsbewertung führen)

Weitere Anforderungen an die Leistungserbringung in Form von Kann-Kriterien, die im Rahmen der Zuschlagsprüfung gewertet werden, sind dem Wertungskriterienkatalog (Dokument 05b) zu entnehmen. Der vom Bieter ausgefüllte Wertungskriterienkatalog wird Bestandteil des Vertrags.

## 7. Mitwirkungsobliegenheiten und Beistellungen des Auftraggebers

Die Bereitstellung von maximal 5 virtuellen Servern (Größenordnung: 4 CPU Cores, 8-16 GB RAM, 100-200 GB System-Disk) und der Lizenzierung des Windows-Betriebssystems erfolgt durch den Auftraggeber in seiner bestehenden Infrastruktur.

Der Auftraggeber stellt für die Installation und den Support einen Online-Zugang zur notwendigen Infrastruktur zur Verfügung.

Der Auftraggeber stellt die Infrastruktur zur Installation der virtuelle Server zur Verfügung.

Falls über die hier genannten Mitwirkungsobliegenheiten und Beistellungen hinaus zusätzliche Anforderungen für die angebotene Lösung bestehen, sind diese extra im Angebot zu berücksichtigen und zu bepreisen (z.B. HW-Server, besondere Grafikkarten etc., DB-Lizenzen, Lizenzen für ein anderes Betriebssystem).