

[Stand: 05.06.2026]

Vergabeunterlagen, Teil 3

Leistungsbeschreibung

**GKV-Spitzenverband
Deutsche Verbindungsstelle
Krankenversicherung - Ausland (DVKA)
Pennefeldsweg 12c
53177 Bonn**

Öffentliches Verfahren gem. § 9 Abs. 1 UVgO

„Endpoint Security Lösung“

Az.: DVKA 003-2026

Ablauf der Angebotsfrist: Freitag, 26. Juni 2026, 14.00 Uhr
--

Diese Vergabeunterlagen sind urheberrechtlich geschützt und dürfen nur zur Erstellung eines Angebotes verwendet werden. Eine Weitergabe, Vervielfältigung oder anderweitige Nutzung der Unterlagen ist nur mit vorheriger Zustimmung der DVKA zulässig.

Inhaltsverzeichnis

1.	Einleitung.....	3
2.	Ausschreibungsgegenstand.....	3
2.1	Endpoint Security Lösung	3
2.2	Technische und Funktionale Anforderungen	3
2.2.1	Unterstützte Betriebssysteme	3
2.2.2	Installation und Betrieb	3
2.2.3	Zentrale Verwaltung und Benutzeroberfläche.....	5
2.2.4	Anbindung an Active Directory (on Premise) und Microsoft M365 (Cloud)	5
2.2.5	Bedrohungsanalyse	5
2.2.6	Reporting und Compliance	6
2.2.7	Skalierbarkeit	6
2.2.8	Support und SLA.....	6
2.3	Mengengerüst	6
2.3.1	Clients Windows	6
2.3.2	Server Linux und Windows	7
2.3.3	Exchange Server	7
2.4	Funktionale Erweiterbarkeit.....	7
2.4.1	MDR	7
3.	Projektunterstützung und Schulung	7
4.	Support.....	7
5.	Abgrenzung	8
6.	Zeitplanung.....	8



1. Einleitung

Die DVKA ist eine bundesunmittelbare Körperschaft des öffentlichen Rechts und Teil des GKV-Spitzenverbandes. Sie versteht sich als Dienstleister und zuverlässiger Partner der gesetzlichen Krankenkassen, von deren Versicherten und Verbänden, anderen Sozialversicherungsträgern sowie international agierenden Institutionen.

Die DVKA verarbeitet sowohl innerhalb verschiedener interner Geschäftsprozesse der DVKA, als auch im innereuropäischen bzw. nationalen Datenaustausch mit Sozialversicherungsträgern eine Vielzahl von Informationen in mehreren Fachanwendungen.

2. Ausschreibungsgegenstand

2.1 Endpoint Security Lösung

Die DVKA benötigt eine Antiviren- bzw. End Point Security-Lösung die eine Unterstützung für physikalische und virtualisierte Windows und Linux-Server und Clients bietet. Die Lösung muss zentral verwaltbar und XDR-fähig sein. Eine spätere Erweiterung um MDR-Services muss möglich sein.

2.2 Technische und Funktionale Anforderungen

2.2.1 Unterstützte Betriebssysteme

Die folgenden Betriebssysteme müssen von der angebotenen Lösung unterstützt werden, ebenso wie die künftigen Versionen.

- Windows Server 2016, 2022 und 2025
- Windows 10 und 11
- Red Hat Enterprise Linux (RHEL) 8, 9 und 10
- CentOS Stream 8, 9 und 10

2.2.2 Installation und Betrieb

Folgende Anforderung zur Installation und für den Betrieb müssen erfüllt werden.

- Deployment der Agenten über zentrale Verwaltungsoberfläche
- Unterstützung von virtualisierten Clients und Servern mit VMware vSphere
- Paketierbares Installationspaket zur Verteilung mittels Softwareverteilungswerkzeugen (z.B. SCCM)
- Anbindung an zentrale Protokollierungs- bzw. SIEM-Lösung (z.B. ProLog, Splunk)
- Der Agent lässt sich in ein (Golden-)Image integrieren
- Der Installer verfügt über einen Mechanismus zur Erkennung (und Deinstallation) von Drittanbieter-Lösungen



- Die Produktsprache wird anhand der konfigurierten Systemsprache des Betriebssystems festgelegt. Mindestens die beiden Sprachen Deutsch und Englisch müssen unterstützt werden.
- Die zu installierenden Produktbestandteile lassen sich einzeln auswählen
- Eine Installation ohne Benutzerinteraktion ist de-/aktivierbar
- Die Client-Installation kann aus einer lokalen Updatequelle (kein Nachladen von Software aus dem Internet) durchgeführt werden
- Die Zeitliche Steuerung von Produkt-Updates ist möglich
- Befindet sich ein System nicht im LAN oder ist kein Update-Server erreichbar, aktualisiert sich das System direkt über das Internet
- Systemkritische Dateien werden überwacht und Änderungen protokolliert
- Registrierungsschlüssel eines Windows-Systems werden überwacht und Änderungen protokolliert
- Überwachungsregeln auf Basis einzelner Dateien, Ordner, Registrierungsschlüssel und Registrierungswerte müssen möglich sein.
- Ausschlüsse auf Basis einzelner Dateien, Ordner, Registrierungsschlüssel und Registrierungswerte müssen möglich sein.
- Es muss einen Echtzeitschutz (On-Access) mit Unterstützung lokaler und Netzlaufwerke geben
- Erkennung und Blockierung von potentiell unerwünschten Anwendungen und Inhalten mit Black- und Whitelisting
- Erkennung von potentiell schädlichem Netzwerkverkehr
- Anti-Exploit Schutz muss vorhanden sein (Schutz vor gängigen Exploits wie z.B. Pufferüberläufen, nachladen von Bibliotheken über UNC-Pfade, ...)
- Der Schutz des Systems muss auch im abgesicherten Modus gewährleistet sein
- Schutz vor Ransomware durch verhaltensbasierte Erkennung von Dateiverschlüsselungsoperationen (Auch auf Windows Terminal Servern)
- Schutz vor Remote ausgeführter Ransomware
- Festplatten und Boot-Record Schutz (MBR)
- Ein Snapshot zur forensischen Analyse muss erstellt werden können
- Der Download riskanter Dateitypen kann per Konfiguration individuell je Dateityp eingeschränkt werden
- Der Zugriff auf bestimmte Web-Inhalte und Downloads kann eingeschränkt werden.
- Manipulationsschutz, der verhindert, dass Schutzeinstellungen durch Unberechtigte angepasst werden. z.B. durch Deaktivierung des Agenten
- Unterstützung für containerisierte Anwendungen und Kubernetes-Umgebungen (z. B. Tanzu)



- Möglichkeit zur Überwachung laufender Container (Runtime Security)
- Integration der entsprechenden Ereignisse in bestehende Logging- und Monitoring-Strukturen
- Schnittstelle zur Integration in Anwendungen, über die Dateien zur Prüfung auf Schadsoftware übergeben und ein Ergebnis synchron zurückgegeben werden kann (z. B. über eine REST-basierte API).

2.2.3 Zentrale Verwaltung und Benutzeroberfläche

Die Verwaltung aller geschützten Systeme muss über eine zentrale Komponente möglich sein.

- Sprachunterstützung Deutsch und Englisch
- Der Computernamen, mit dem das System in der Verwaltungsoberfläche identifizierbar ist, kann vorgegeben werden
- Bei Bedarf kann über die zentrale Verwaltung ein vollständiger Scan eines Systems initiiert werden
- Alle Ereignisse werden an die zentrale Verwaltung übermittelt
- In der zentralen Verwaltung werden pro System detailliert alle installierten Komponenten inkl. Versionsnummer angezeigt
- In der zentralen Verwaltung kann eine Aktualisierung des Endpoint Agenten initiiert werden
- Richtlinien können zentral verwaltet werden

2.2.4 Anbindung an Active Directory (on Premise) und Microsoft M365 (Cloud)

Die Anbindung an ein Microsoft-basiertes Active Directory System muss möglich sein.

- Unterstützung einer AD-Integration (Windows Server 2022 basierend)
- Unterstützung von LDAPs (LDAP over SSL)

2.2.5 Bedrohungsanalyse

Folgende Anforderungen an die Bedrohungsanalyse müssen erfüllt werden.

- Die Lösung verfügt über eine Bedrohungsanalyse, die bei einer Erkennung Daten in aufbereiteter Form anzeigt. Die angezeigten Daten umfassen die vollständige Angriffskette, vom Eintritt ins System bis hin zur Erkennung.
- Eine Historie der Bedrohungsanalysen der letzten 90 Tagen ist verfügbar.
- Eine Übersicht über die Gerätegefährdung ist verfügbar (welche Geräte sind veraltet und anfällig für Bedrohungen).
- Es werden durch die Bedrohungsanalyse detaillierte Informationen mindestens zu Gerät, angemeldetem Benutzer, laufenden Prozessen und Zeitpunkt der Erkennung bereitgestellt.



2.2.6 Reporting und Compliance

Nachstehende Anforderungen hinsichtlich Reporting und Compliance müssen erfüllt werden.

- Historische Informationen über z.B. Dateizugriffe, Netzwerkzugriffe etc. können bis zu 90 Tage abgefragt werden.
- Möglichkeit der Datenspeicherung über 365 Tage
- Ereignisse und sonstige allgemeine Status- und Fehlermeldung werden an das zentrale Management übermittelt.
- Alle relevanten Diagnosedaten eines Endgeräts können direkt über das Management angefordert werden.

2.2.7 Skalierbarkeit

Die Skalierbarkeit des Systems hinsichtlich der integrierten Server, Clients und E-Mail-Konten bis hin zum doppelten des unter Kapitel 2.3 dargestellten Mengengerüsts muss gewährleistet sein.

2.2.8 Support und SLA

Der Auftragnehmer erbringt Supportleistungen für die Antiviruslösung des Auftraggebers an Werktagen in NRW innerhalb der Servicezeiten von Montag bis Freitag, 08:00 bis 17:00 Uhr. Der Support erfolgt über E-Mail, Telefon sowie ein Ticket-System. Für Störungen gelten verbindliche Reaktionszeiten:

- bei kritischen Incidents innerhalb von 2 Stunden
- bei hoher Priorität innerhalb von 4 Stunden
- bei mittlerer Priorität innerhalb eines Werktags
- bei niedriger Priorität innerhalb von zwei Werktagen.

Die technische Unterstützung umfasst Remote-Support zur Fehleranalyse und -behebung sowie die Unterstützung bei der Installation des Antivirus-Clients und des Managementservers, bei Agent-Updates, Konfigurationsanpassungen in der Managementkonsole, dem Rollout und der Erstkonfiguration sowie bei der Behandlung von Detektionen und Fehlalarmen. Nicht lösbare Probleme werden durch den Auftragnehmer an den Hersteller eskaliert. Darüber hinaus stellt der Auftragnehmer den Zugriff auf das Softwareportal des Herstellers sicher und sorgt für die Bereitstellung aktueller Signatur-Updates, Major- und Minor-Releases sowie Hotfixes und Patches. Er bewertet geplante Updates, gibt Empfehlungen zur Nutzung verschiedener Update-Kanäle und überwacht, ob Clients veraltete Signaturen verwenden.

2.3 Mengengerüst

Das Produkt muss auf dem im Folgenden beschriebenen Mengengerüst nutzbar sein.

2.3.1 Clients Windows



Es kommen 200 Clients mit Windows 11 zum Einsatz.

2.3.2 Server Linux und Windows

Es kommen in Summe 110 Linux- und Windows Server zum Einsatz.

2.3.3 Exchange Server

Es kommt ein Microsoft Exchange Server mit ca. 200 Benutzerpostfächer und ca. 100 Shared Mailboxes zum Einsatz.

2.4 Funktionale Erweiterbarkeit

2.4.1 MDR

Das System muss als künftige mögliche Erweiterung an einen Manage Service (MDR) angebunden werden können. MDR ist allerdings nicht Bestandteil dieser Ausschreibung.

3. Projektunterstützung und Schulung

Für die erste Inbetriebnahme der Kernkomponenten der Software und dem Rollout auf die Client- und Server Systeme ist Projektunterstützung im Sinne einer Dienstleistung in Höhe von 5 PT anzubieten. Die Abrechnung soll nach tatsächlichem Aufwand erfolgen.

Außerdem muss eine administrative Schulung für das System mit angeboten werden. Ziel dieser Schulung ist es, dass der IT-Betrieb der DVKA das System warten und pflegen kann.

4. Support

Der Auftragnehmer stellt den laufenden Betrieb der Antivirus-Lösung sicher und unterstützt den Auftraggeber bei allen im Regelbetrieb anfallenden Aufgaben. Dazu gehört zunächst die Annahme, Priorisierung und Bearbeitung eingehender Supportanfragen über E-Mail, Telefon oder ein Ticket-System während der vereinbarten Servicezeiten. Der Auftragnehmer reagiert innerhalb der definierten SLA-Fristen, führt eine erste Fehleranalyse durch und beginnt unverzüglich mit der Störungsbehebung. Bei Bedarf erfolgt der Zugriff per Remote-Support, um Probleme schnell und effizient zu lösen.

Im technischen Betrieb übernimmt der Auftragnehmer typische Aufgaben wie die Unterstützung bei Installation und Aktualisierung des Antivirus-Clients, die Pflege und Anpassung von Richtlinien in der Management-Konsole sowie die Durchführung von Rollouts und Erstkonfigurationen. Er analysiert erkannte Bedrohungen, bewertet Detektionen und Fehlalarme und liefert Lösungsvorschläge oder Maßnahmenempfehlungen. Probleme, die nicht durch den Auftragnehmer selbst gelöst werden können, werden strukturiert und nachvollziehbar an den Hersteller eskaliert.

Zusätzlich stellt der Auftragnehmer sicher, dass der Auftraggeber Zugang zu allen relevanten Software-Downloads, Signatur-Updates, Patches und Versionsupgrades erhält. Er überwacht den



Updatestand der Endpunkte, informiert über notwendige Maßnahmen und empfiehlt geeignete Update- und Release-Kanäle.

5. Abgrenzung

Die Ausschreibung beinhaltet die Softwaremiete für das in Kapitel 1.3 beschriebene Mengengerüst. Außerdem müssen Softwareupdates und –upgrades während der gesamten Vertragslaufzeit kostenfrei bereitgestellt werden. Dies umfasst sowohl funktionale Erweiterungen als auch sicherheitsrelevante Aktualisierungen.

Nicht Bestandteil der Ausschreibung ist ein Managed Service zur Überwachung der Systeme. Die Pflege des Systems übernimmt nach der Inbetriebnahme die DVKA.

6. Zeitplanung

Ziel ist es, die Endpoint Security Lösung bis zum 30.09.2026 vollständig in Betrieb genommen zu haben.

Das bedeutet, dass die Lösung bis zu dem Zeitpunkt auf alle Clients, Windows- und Linux-Server sowie den Exchange Server ausgerollt sein muss.

