S i t z u n g s v o r l a g e	Nr. 179/2026

Federführendes Amt: Hauptamt			
Beratungsfolge	**Behandlung**		**Termin**
Verwaltungsausschuss	Beschlussfassung	Ö	14.07.2026

Betreff:
Beschaffung eines KI-gestützten Virenschutzes für die städtische Netzwerkumgebung

Beschlussvorschlag:

1. Der Verwaltungsausschuss stimmt der Durchführung einer Verhandlungsvergabe ohne Teilnahmewettbewerb zur Beschaffung einer Endpoint Detection and Response (EDR)-Lösung mit KI-gestütztem Virenschutz einschließlich eines 24-Stunden-Sicherheitsmonitorings (24/7 Security Operations Center – SOC) zu.

2. Das vom Gemeinderat am 21.11.2023 im Rahmen der Vergabe des KI-basierten Virenschutzes (XDR-Lösung) beschlossene mögliche Verlängerungsjahr (1. Februar 2027 bis 31. Januar 2028) wird aus wirtschaftlichen Gründen nicht in Anspruch genommen. Stattdessen erfolgt die Neuausschreibung für ein Jahr, mit der Option auf ein Verlängerungsjahr.

Begründung:

Die IT-Systeme der Stadt Winnenden sind täglich einer Vielzahl automatisierter Cyberangriffe ausgesetzt. Klassische Virenschutzprogramme erkennen hauptsächlich bereits bekannte Schadsoftware. Moderne Angriffe entwickeln sich jedoch ständig weiter und können daher herkömmliche Virenscanner umgehen. Aus diesem Grund soll die bisher eingesetzte Sicherheitslösung durch eine mindestens gleichwertige Endpoint Detection and Response (EDR)-Lösung ersetzt werden.

Ein EDR-System überwacht alle Computer, Notebooks und Server kontinuierlich auf verdächtige Aktivitäten. Dabei werden nicht nur bekannte Viren erkannt, sondern auch bislang unbekannte Angriffe anhand ihres Verhaltens identifiziert. Hierbei unterstützt künstliche Intelligenz (KI), indem sie ungewöhnliche Vorgänge automatisch analysiert und bewertet.

Zusätzlich beinhaltet die Lösung ein rund um die Uhr besetztes Security Operations Center (SOC). Dieses überwacht die Systeme 24 Stunden täglich an sieben Tagen der Woche. Bei sicherheitsrelevanten Ereignissen erfolgt eine sofortige Analyse durch IT-Sicherheitsspezialisten. Dadurch können Angriffe frühzeitig erkannt, bewertet und Gegenmaßnahmen eingeleitet werden, bevor größere Schäden entstehen. Durch diese Kombination aus moderner KI-Technologie und permanenter Überwachung bleibt das Sicherheitsniveau der gesamten IT-Infrastruktur der Stadtverwaltung sehr hoch.

Wirtschaftlichkeit:
Der Gemeinderat hat am 21.11. 2023 die Vergabe der bisherigen Sicherheitslösung (XDR-Lösung – KI basierter Virenschutz") für 3 Jahre mit der Option auf ein Verlängerungsjahr beschlossen. Die Kosten der bisher eingesetzten Sicherheitslösung beliefen sich auf rund 120.000 € pro Jahr. Hinzu kamen Kosten für sogenannte Incident-Response-Einsätze (2024: 25.000 € und 2025: 10.000€). Diese entstehen, wenn externe IT-Sicherheitsexperten bei Sicherheitsvorfällen kurzfristig hinzugezogen werden müssen.

Durch den inzwischen deutlich größeren Wettbewerb am Markt stehen heute mehrere leistungsfähige Anbieter zur Verfügung. Dies führt trotz eines erheblich erweiterten Leistungsumfangs zu einer Reduzierung der jährlichen Kosten gegenüber der bisherigen Lösung um 25 Prozent. Daher soll von der Verlängerungsoption um ein weiteres Jahr bewusst kein Gebrauch gemacht werden. Durch die vorzeitige Neuausschreibung können die aktuell günstigeren Marktpreise genutzt werden. Dadurch ergeben sich Einsparungen gegenüber einer Vertragsverlängerung bei gleichzeitig erweitertem Leistungsumfang.

Der neu abzuschließende Vertrag soll zunächst für ein Jahr abgeschlossen werden.
Zusätzlich soll bereits jetzt ein optionales Verlängerungsjahr genehmigt werden. Dadurch kann die Verwaltung – sofern sich die Zusammenarbeit bewährt und wirtschaftlich bleibt – den Vertrag ohne erneute Ausschreibung um ein weiteres Jahr verlängern.

Die neue Ausschreibung umfasst sämtliche für den sicheren Betrieb erforderlichen Leistungen zu einem jährlichen Preis von rund **100.000 €.** Geschätzt aus den durchgeführten Markterkundungen und erhaltenen Preisinformationen. 2023 waren wir eine der ersten Kommunen, die ein solches System einsetzten.

Im Leistungsumfang enthalten sind insbesondere:
- KI-gestützter Virenschutz,
- Endpoint Detection and Response (EDR),
- 24/7 Security Operations Center (SOC),
- permanente Sicherheitsüberwachung,
- Alarmierung und Erstreaktion bei Sicherheitsvorfällen,
- Software-Updates,
- Signatur- und Regelwerksaktualisierungen,
- Hersteller-Support,
- Wartung,
- Betrieb der Sicherheitsplattform,
- Migration und Außer-Betrieb-Name der bisherigen Lösung.

Vergabeverfahren:
Die Vergabe erfolgt als **Verhandlungsvergabe ohne Teilnahmewettbewerb**.
Hierfür werden acht geeignete und am Markt etablierte Anbieter zur Angebotsabgabe aufgefordert.
Durch die Verhandlungsgespräche können sowohl technische als auch wirtschaftliche Aspekte der Angebote optimiert werden.

Die Wertung der Angebote erfolgt anhand folgender Zuschlagskriterien:
- Preis: **60 %**
- Leistung und Qualität: **40 %**

Mehrfachangebote eines Unternehmens sind zulässig.
Sollte ein Unternehmen mit mehreren Angeboten zu den drei bestplatzierten Angeboten gehören, wird ausschließlich dessen wirtschaftlich bestes Angebot berücksichtigt. Die übrigen Plätze werden mit den nächstplatzierten Anbietern besetzt. Dadurch wird gewährleistet, dass die abschließenden Bietergespräche mit drei unterschiedlichen Unternehmen geführt werden und ein fairer Wettbewerb sichergestellt ist.

Finanzielle Auswirkungen:
Die jährlichen Kosten belaufen sich auf voraussichtlich rund **100.000 €.**
Mit dem Angebot sind sämtliche für den Betrieb erforderlichen Leistungen abgegolten. Zusätzliche Kosten für Überwachung und notwendige Angriffs-Analysen und - Abwehr entstehen nicht.
Durch den Wegfall separater Incident-Response-Leistungen sowie dem gesunkenen Marktpreis ist gegenüber der bisherigen Lösung eine wirtschaftlichere Gesamtlösung zu erwarten.

Weiteres Vorgehen:
Nach Zustimmung des Verwaltungsausschusses beginnt das Vergabeverfahren.
Im Anschluss werden die ausgewählten Unternehmen zur Angebotsabgabe aufgefordert. Nach Auswertung der Angebote und Durchführung der Verhandlungsgespräche erfolgt die Zuschlagserteilung an den wirtschaftlichsten Bieter.
Der Produktivbetrieb der neuen Sicherheitslösung soll rechtzeitig vor Ablauf des bestehenden Vertrags einschließlich einer geordneten Migration erfolgen, sodass ein unterbrechungsfreier Schutz der IT-Infrastruktur gewährleistet ist.

Freiwillige Aufgabe:	
Freiwillige Aufgabe	Ja ☐

S i t z u n g s v o r l a g e	Nr. 179/2026

CO_2-Relevanz:			
Auswirkung auf den Klimaschutz	**Nein** ☒	**Ja** positiv ☐ negativ ☐	geringfügig ☐ erheblich ☐

Begründung / Optimierung:

Verwaltungsaufwand:		
Auswirkung auf die Verwaltungsarbeit	**Nein** ☒	**Ja** Verwaltungsaufwand wird erhöht ☐ Verwaltungsaufwand wird reduziert ☐

Begründung:

Anlagen: