Stadt Leipzig

Leistungsbeschreibung
zur Lieferung, Inbetriebnahme, Pflege und Wartung eines Systems zur Angriffserkennung (SzA)

L-10.2-2024-00497

Inhaltsverzeichnis

0.Einleitung

Um den zunehmenden Gefahren durch Cyberattacken effektiv begegnen zu können, hat das Bundesministerium des Innern ein IT-Sicherheitsgesetz auf den Weg gebracht, das am 25. Juli 2015 in Kraft getreten ist. Hierin sind verbindliche Mindestanforderungen an die IT-Sicherheit für die Kritischen Infrastrukturen (KRITIS) und die Verpflichtung zur Meldung erheblicher IT-Sicherheitsvorfälle verankert.

Kritische Infrastrukturen (KRITIS) sind demnach Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung
- nachhaltig wirkende Versorgungsengpässe,
- erhebliche Störungen der öffentlichen Sicherheit
- oder andere dramatische Folgen einträten.

Mit dem Inkrafttreten der zweiten Kritis-Verordnung wurden die Sektoren der kritischen Infrastruktur erweitert. Einer der der Sektoren ist der Sektor Transport und Verkehr, der in dem §8 BSI-KritisV beschrieben wird. Die Zugehörigkeit des Mobilitäts- und Tiefbauamt (MTA) der Stadt Leipzig zu diesem Sektor begründet sich in den Schwellenwerten (mehr als 500.000 Einwohner) sowie dem Betreiben von Verkehrssteuerungssystem und Leitsystemen im kommunalen Straßenverkehr (Lichtsignalanlage, Parkleitsystem, LED-Tafeln).

Aus dieser Zugehörigkeit zum Sektor Transport und Verkehr ist ein Informations- und Managementsystem im MTA Leipzig seit der GAP-Analyse 2019 (IST-Soll Analyse) aufgesetzt wurden, dass nur im Geltungsbereich des MTA Leipzig gilt.

Aufgrund der steigenden Zahlen von Angriffen (z.B. Cyberangriffe, Informationsbeschaffung jeglicher Art etc.) auf Einrichtungen der kritischen Infrastruktur in den letzten Jahren ist zur Gewährleistung der Vermeidung von Störungen der Verfügbarkeit, Integrität und Authentizität sowie Vertraulichkeit eine gesetzliche Erweiterung zur Vermeidung dieser Störungen geschaffen wurden.

Um diesen Tatbestand Rechnung zu tragen, ist die Erweiterung von Kontrollmechanismen in den Sektoren geschaffen wurden - die Systeme zur Angriffserkennung (SzA).

Der Begriff „Systeme zur Angriffserkennung“ mit der Pflicht zum ordnungsgemäßen Einsatz ist dem BSIG im § 8a Absatz 1a eingefügt, sowie im §2 Absatz 9b Satz 1 BSIG legal definiert und in Satz 2 technisch weiter erläutert.

„Systeme zur Angriffserkennung im Sinne dieses Gesetzes sind durch technische Werkzeuge und organisatorische Einbindung unterstützte Prozesse zur Erkennung von Angriffen auf informationstechnische Systeme. Die Angriffserkennung erfolgt dabei durch Abgleich der in einem informationstechnischen System verarbeiteten Daten mit Informationen und technischen Mustern, die auf Angriffe hindeuten“
(§ 2 Absatz 9b BSIG)

Die Verpflichtung so ein System zur Angriffserkennung im MTA der Stadt Leipzig einzusetzen, ergibt sich aus § 8a Absatz 1a BSIG für Betreiber einer Kritischen Infrastruktur. Der Gesetzgeber schreibt dies seit dem 1. Mai 2023 verpflichtend vor. Dabei soll der Stand der Technik eingehalten und der ordnungsgemäße Einsatz der Angriffserkennungssysteme mit dem Nachweis nach § 8a Absatz 3 BSIG ebenfalls nachgewiesen werden.

„Die Verpflichtung nach Absatz 1 Satz 1, angemessene organisatorische und technische Vorkehrungen zu treffen, umfasst ab dem 1. Mai 2023 auch den Einsatz von Systemen zur Angriffserkennung. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete

Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen“
(§ 8a Absatz 1a Satz 1, 2 BSIG).

„Betreiber Kritischer Infrastrukturen haben die Erfüllung der Anforderungen nach den Absätzen 1 und 1a spätestens zwei Jahre nach dem in Absatz 1 genannten Zeitpunkt und anschließend alle zwei Jahre dem Bundesamt nachzuweisen“
(§ 8a Absatz 3 Satz 1 BSIG).

1. Beschreibung des Geltungsbereiches des MTA der Stadt Leipzig zum Einsatz von Systemen zur Angriffserkennung

Der vom Gesetzgeber verpflichtende Einsatz eines SzA für Betreiber einer Kritischen Infrastruktur betrifft im engeren Sinne das MTA der Stadt Leipzig im definierten Geltungsbereich der Abteilung Verkehrsmanagement und Beleuchtung (Abteilung 66.9).

Das MTA der Stadt Leipzig betreibt zwei Systeme (Verkehrssystemrechner, Verkehrssystem-management) zur Verkehrslenkung und Verkehrssteuerung. Von dem Sachgebiet Betrieb Beleuchtung und Verkehrstechnik (SG 66.93) werden dezentrale Straßenverkehrs-Signalanlagen mit den zugehörigen Peripheriekomponenten inklusive deren datentechnischer Anschluss betrieben. Weiterhin wird ein Parkleitsystem sowie ein Anzeigetafelsystem betrieben. Diese sind für den sicheren Verkehr im Stadtgebiet Leipzig entscheidend.

Nach der geänderten BSI-Kritisverordnung (Anhang 7, Teil 3, Nr.1.4.2) fällt der Betrieb eines Verkehrssteuerungs- und Leitsystems im kommunalen Straßenverkehr in der Stadt Leipzig mit über 500.000 Einwohnern unter die kritischen Infrastrukturen. Aus diesem Grunde wird nach dem Branchenspezifischen Sicherheitsstandard (B3S) für Verkehrssteuerungs- und Leitsysteme im kommunalen Straßenverkehr der Geltungsbereich betrachtet.

Der Geltungsbereich umfasst alle Komponenten und Anlagen des Bereichs der kritischen Dienstleistung nach BSI-Kritisverordnung. Die Schutzziele Verfügbarkeit, Vertraulichkeit und Integrität müssen/sollen in Bezug auf die Aufrechterhaltung der kritischen Dienstleistung gewährleistet werden. Dabei wurde insbesondere die Beeinträchtigung der Versorgungssicherheit durch Störungen der Schutzziele der zugrundeliegenden Systeme betrachtet.

Der Geltungsbereich kann wie folgt beschrieben werden:

1. den Kernprozess „Verkehrslenkung und Verkehrssteuerung“ mit den Subprozessen in den Sachgebieten:
    a. Sachgebiet Verkehrsmanagement Verkehrs- und Datenmanagement (SG 66.91)
    b. Sachgebiet Betrieb Beleuchtung und Verkehrstechnik (SG 66.92)
    c. Sachgebiet Betrieb Planung und Bau von Beleuchtung und LSA (SG.99.93)
    d. Sachgebiet Steuerzentrale Beleuchtung und Verkehr (SG 66.94)

2. weitere für die Informationssicherheit unterstützende Prozesse (Recht- und Vertragswesen, Planungs- und Rechnungswesen, IT-Koordination - Beschaffung von Hard- und Software, Personalrat und Personalamt, Gebäudesicherheit). Das Informationssicherheitsmanagementsystem (ISMS) des MTA Leipzig ist Bestandteil des (noch nicht zertifizierten) ISMS der Stadt Leipzig und verwendet daher Prozesse dieses übergeordneten ISMS mit, z.B. den Risikomanagementprozess.

3. organisatorische Teile des Verkehrs- und Tiefbauamts bei der Stadt Leipzig und der allgemeinen Verwaltung

4. geographisch den Standort der Rechentechnik Neues Rathaus Martin Luther-Ring 4-6 Schützenstraße, den Standort in der Wurzner Straße 93, den Standort Technisches Rathaus in der Prager Straße 118-136, wobei das Personal für die Bedienung der Rechentechnik im Neuen Rathaus nicht vor Ort eingesetzt ist.

Die Abteilung Generelle Planung ist nicht im Geltungsbereich beschrieben, da von der reinen Lehre des B3S (siehe Abbildung 1) ausgegangen wird.

2. Anforderungen an ein System zur Angriffserkennung

2.1 Allgemein

Die technische Funktionalität eines Systems zur Angriffserkennung (SzA) basiert im Wesentlichen auf Abläufen, die sich den Bereichen Protokollierung, Detektion und Reaktion zuordnen lassen. Um eine effektive Erkennung von Angriffen gewährleisten zu können, sind an die genannten Bereiche Anforderungen zu stellen, die in den nächsten Abschnitten benannt werden.

Damit eine optimale Planung und Umsetzung dieser Anforderungen für ein SzA für die vorhandenen Systeme und Prozesse erfolgen kann, ist das vorhandene ISMS mit einzubeziehen.

Die Anforderungen werden mit den in Versalien geschriebenen Modalverben MUSS, SOLLTE und KANN sowie den zugehörigen Verneinungen formuliert. Die Modalverben werden entsprechend den sprachlichen Erfordernissen konjugiert.

MUSS	:	Eine Anforderung die unbedingt erfüllt werden muss, um einen Umsetzungsgrad der Stufe 3 zu erreichen.
SOLLTE	:	Eine Anforderung die normalerweise getan werden sollte, es aber Gründe geben kann, dies doch nicht zu tun. Dies muss aber sorgfältig abgewogen und stichhaltig begründet werden, um einen Umsetzungsgrad der Stufe 4 zu erreichen.
KANN	:	wird für Anforderungen verwendet, deren Erfüllung nicht zwingend erforderlich, aber eine sinnvolle Ergänzung ist, wenn ein Umsetzungsgrad der Stufe 5 erreicht werden soll.

Grundsätzlich gilt für die Gesamtheit aller Bereiche (Protokollierung, Detektion und Reaktion) und Prozesse zur Angriffserkennung in diesem Dokument, dass

- die notwendigen technischen, organisatorischen und personellen Rahmenbedingungen geschaffen werden MÜSSEN,
- Informationen zu aktuellen Angriffsmustern für technische Vulnerabilitäten fortlaufend für die im Anwendungsbereich eingesetzten Systeme eingeholt werden MÜSSEN,
- durchgängig alle zur effektiven Angriffserkennung erforderliche Hard- und Software auf einem aktuellen Stand gehalten werden MUSS,
- die Signaturen von Detektionssystemen immer aktuell sein MÜSSEN,
- alle relevanten Systeme so konfiguriert sein MÜSSEN, dass Versuche, bekannte Schwachstellen auszunutzen, erkannt werden können, sofern keine schwerwiegenden Gründe dagegensprechen.

Weiterhin ist bei der Software darauf zu achten, dass diese in Deutsch ist und ein leichtes Handling über Maussteuerung ermöglicht.

Die Erfüllung der Anforderungen wird mit dem beiliegenden „Kriterienkatalog Fachliche Anforderungen.xlsx“ abgefragt, der ausgefüllt Bestandteil des Angebots wird.

2.2 Protokollierung

2.2.1 Planung der Protokollierung

Die Schritte für die Planungsphase MÜSSEN so gewählt werden, dass eine angemessene Sichtbarkeit innerhalb angemessener Zeit erzielt werden.
Der Betreiber MUSS alle zur wirksamen Angriffserkennung auf System- bzw. Netzebene notwendigen Protokoll- und Protokollierungsdaten (gemäß § 2 Absatz 8 und 8a BSIG) erheben, speichern und für die Auswertung bereitstellen, um sicherheitsrelevante Ereignisse (SRE) erkennen und bewerten zu können.

Hierzu KÖNNEN zusätzliche Systeme eingesetzt werden, sodass zur wirksamen Angriffserkennung nicht jedes einzelne Gerät Protokollierungsdaten aufzeichnen muss und damit die Verfügbarkeit der Produktivsysteme und damit der kritischen Dienstleistung gewährleistet werden kann.

Die zur Speicherung notwendigen Systeme und deren IT-Sicherheitsvorkehrungen MÜSSEN schon in der Planung bedacht werden. Im Rahmen der Planung MÜSSEN alle Systeme identifiziert werden, die zur Aufrechterhaltung der kritischen Dienstleistung maßgeblich sind, damit deren Protokoll- und Protokollierungsdaten später erfasst werden können.
Sind die bestehenden Systeme nicht in der Lage, auskömmliche Protokoll- und Protokollierungsdaten bereitzustellen, SOLLTE die Protokollierungsinfrastruktur so angepasst und/oder durch zusätzliche Maßnahmen, Software oder Systeme ergänzt werden, dass Detektion und Reaktion im entsprechend der Risikoanalyse notwendigen Rahmenmöglich sind.

Das anfallende Protokoll- und Protokollierungsdatenaufkommen KANN (und wird dringend empfohlen) anhand eines repräsentativen Systems pro Systemgruppe bestimmt werden.
Die Ergebnisse der Planungsphase MÜSSEN in einer geeigneten Formdokumentiert werden. Die Dokumentation MUSS alle Netzbereiche, die Protokoll- und Protokollierungsdatenquellen, deren Beziehungen untereinander und den Datenfluss der Protokoll- und Protokollierungsdaten im Anwendungsbereich umfassen.

Darüber hinaus MUSS für jedes System bzw. für jede Systemgruppe dokumentiert werden, welche Ereignisse dieses bzw. diese protokolliert.
Es MUSS ein Prozess eingerichtet werden, der sicherstellt, dass die Protokollierung bei Veränderungen im Anwendungsbereich (Changes) entsprechend angepasst wird.

2.2.2 Umsetzung der Protokollierung

Aufbau zentralisierter Protokollierungsinfrastrukturen:
Alle gesammelten sicherheitsrelevanten Protokoll- und Protokollierungsdaten MÜSSEN an für den jeweiligen Netzbereich an zentralen Stellen gespeichert werden. Die Zahl an zentralen Stellen zur Speicherung SOLLTE möglichst geringgehalten werden und sich mindestens an funktionalen Einheiten orientieren, sodass der Zugriff auf die gespeicherten Daten einfach erfolgen kann. Die Protokollierungsinfrastruktur MUSS dazu ausreichend dimensioniert sein.

Bereitstellung von Protokoll- und Protokollierungsdaten für die Auswertung:
Die gesammelten Protokoll- und Protokollierungsdaten MÜSSEN gefiltert, normalisiert, aggregiert und korreliert werden. Die so bearbeiteten Protokoll- und Protokollierungsdaten MÜSSEN geeignet verfügbar gemacht werden, damit sie ausgewertet werden können.
Eine zeitlich befristete Speicherung der unbearbeiteten Protokolldaten KANN den

Detektionsprozess zusätzlich unterstützen.

Für die Erzielung einer angemessenen Sichtbarkeit von Angriffen SOLLTEN die Protokollierungsdatenquellen auf Netzebene von außen (Netzgrenzen) nach innen (Netzbereiche) erschlossen werden.

Die Systemebene (kritische Anwendungen und Applikationen) SOLLTE ausgehend von den zentralen, kritischen Systemen, wie z. B. Prozessleit- und Automatisierungstechnik und Leitsystemen, erschlossen werden.

Die Priorisierung zur Auswahl der Protokollierungsdatenquellen SOLLTE ausgehend von der Kritikalität der Systeme abgeleitet werden. Nach erfolgreicher Umsetzung der Protokollierung MUSS geprüft werden, ob alle geplanten Protokollierungsdatenquellen gemäß der Planung umgesetzt wurden.

Sollten branchenspezifisch weitergehende gesetzliche oder regulatorische Anforderungen an die Protokollierung bestehen, so MÜSSEN diese ebenfalls entsprechend umgesetzt werden.

2.3 Detektion

2.3.1 Planung der Detektion

Bei der Auswahl und dem Einsatz von Detektionsmaßnahmen MUSS eine umfassende und effiziente Abdeckung der Bedrohungslandschaft erzielt werden. Dazu MÜSSEN die Ergebnisse der Risikoanalyse des MTA der Stadt Leipzig die Größe und Struktur des Geltungsbereiches der Stadt Leipzig einbezogen werden. Zur Bestimmung der Abdeckung KANN (Empfehlung) eine standardisierte Methode angewendet. In Abhängigkeit der Größe des Geltungsbereiches des MTA der Stadt Leipzig und der Bedrohungslandschaft KANN eine separate Betrachtung von Detektionsmaßnahmen für die IT- und OT-Umgebung erforderlich sein.

2.3.2 Umsetzung der Detektion

Als Mindestanforderung für die Detektion MÜSSEN alle Basisanforderungen von DER.1 (IT-Grundschutz) erfüllt werden:

- Kontinuierliche Überwachung und Auswertung von Protokoll- und Protokollierungsdaten
- Einsatz zusätzlicher Detektionssysteme
- Infrastruktur zur Auswertung von Protokoll- und Protokollierungsdaten und Prüfung sicherheitsrelevanter Ereignisse
- Auswertung von Informationen aus externen Quellen
- Auswertung der Protokoll- und Protokollierungsdaten durch spezialisiertes Personal
- Zentrale Detektion und Echtzeitüberprüfungen von Ereignismeldungen

2.4 Reaktion

Als Mindestanforderung für die Reaktion MÜSSEN alle Basisanforderungen von DER.2.1 (IT-Grundschutz) erfüllt werden. Es SOLLTEN zudem die Standardanforderungen aus DER.2.1 (IT-Grundschutz) umgesetzt werden.

Außerdem MUSS die *Automatische Reaktion auf sicherheitsrelevante Ereignisse als A*nforderung erfüllt werden.

Die eingesetzten SzA SOLLTEN auch eine nicht-automatisierte Qualifizierung und Behandlung von Ereignissen unterstützen.

3. Anforderungen an des SzA im MTA der Stadt Leipzig

Nach Punkt 2 zu ‚Anforderungen an ein System zur Angriffserkennung' muss das eingesetzte System alle MUSS – Anforderungen mit Tag der öffentlichen Bekanntgabe der Ausschreibung zum SzA erfüllen. Weiterhin sind in dem System alle aktuellen SOLLTE-Anforderungen mit aufzunehmen. Ziel ist es, den Umsetzungsgrad der Stufe 3 (Mindestanforderung BSI) oder wenn möglich auch Stufe 4 oder gar 5 mit dem Einsatz des SzA zu erreichen.

3.1 Eingliederung des SzA in die bestehende Netzstruktur

Für die Hauptkomponente des SzA wird ein neues Netzsegment an den Switchen im bestehenden Geltungsbereich des MTA eröffnet. Dies ist dringend erforderlich da VSM und VSR von unterschiedlichen Dienstleistern betrieben wird, um auch weiterhin eine Trennung von unterschiedlichen Anwendungssystemen zu gewährleisten.

In diesem neuen eigenständigen Netzwerksegment soll der Server in den Raum (Neues Rathaus) des Hauptswitches stehen. Die Anzahl der benötigten Ports am Hauptswitch, die zur Aufzeichnung der Transaktionen in den Netzwerken VSM/VSR gebraucht werden, muss der Auftragnehmer mitteilen. Es werden entsprechend der gebrauchten Anzahl von Ports mindestens noch zwei Ersatzports vom Auftraggeber zur Verfügung gestellt.

Neben dem integrierten Server ist in diesem eigenständigen Netzwerk eine Bedienstation sowie ein entsprechendes Speichermedium in örtlicher Trennung (Technisches Rathaus) vom Server vom Auftragnehmer mit zu betrachten.

Die unter Punkt 2.2.4 beschriebenen Anforderungen an die Detektion müssen entsprechend in den Netzwerken VSM und VSR umgesetzt werden. Dabei ist zu beachten, dass die Freigaben an der Firewall zu den einzelnen Netzwerken durchgeführt werden müssen.

Die entsprechenden Änderungen an den Netzwerkkomponenten (Switche, Hauptfirewall) mit Eigentum MTA der Stadt Leipzig bzw. LECOS GmbH werden durch den Dienstleister LECOS GmbH durchgeführt. Im VSR-Netzwerk muss eine Detektion mit der Firma Yunex genauer besprochen werden, da hinter der Hauptfirewall der LECOS GmbH das VSR-Netzwerk extra gesichert ist. Dabei dürfen nur Netzwerkkomponenten im VSR-Netzwerk am Standort Leipzig detektiert werden.

3.2. Allgemeine Beschreibung der Netzwerke VSM und VSR

Im MTA der Stadt Leipzig werden im KRITIS-Geltungsbereich dem Einsatzort des SzA, zwei durch eine Firewall getrennte Netzwerke betrieben. Diese zwei Netzwerke sind einerseits der Verkehrssystemrechner (VSR) mit den Lichtsignalanlagen und dem dynamischen Parkleitsystem sowie das Verkehrssystemmanagement (VSM) als Datensammler über softwareschnittstellen aus dem VSR und den Zählstellen sowie den Anzeigesystemen.

Dabei ist zu beachten das im VSM mindestens 5 Server (physisch) bzw. 4 Clients derzeit eingesetzt werden. Die Server (physisch) befinden sich räumlich getrennt von den abgesetzten Clients an unterschiedlichen Standorten. Ein Teil der Server ist auch

virtualisiert. Zukünftig soll die Anzahl der Server und Clients noch steigen. Hier ist davon auszugehen das die maximale Zahl Server (physisch) auf 12 steigt sowie der Clients auf 10.

Ähnlich verhält es sich beim VSR. In diesem Netz sind mindesten 8 Server (physisch), mehrere Switche bzw. Firewalls (physisch, virtualisiert) bzw. mindestens 18 Clients an unterschiedlichen Standorten. Auf den physisch vorhandenen Servern liegt teilweise eine Virtualisierung von Servern vor. In den nächsten Jahren ist davon auszugehen, dass die Anzahl der Server (physisch) weiter auf mindestens 15 bzw. die Clients auf 25 steigen.

Weiterhin befinden sich alle Server an einem Standort also räumlich getrennt von den Clients. Wie unter 3.1. beschrieben wird die Hauptfirewall bzw. der Hauptswitch von der LECOS GmbH betrieben.

3.3 Beschreibung der Hardware für das System zur Angriffserkennung

Die für das Netzsegment SzA benötigte Hardware wird an zwei Standorten eingesetzt. Es ist darauf zu achten, dass die Hardware entsprechend den Vorgaben in die Racks passt. Weiterhin ist die Hardware so zu dimensionieren, dass Sie für die nächsten 5 Jahre mindestens ausreichend ist. Bei der Installation der Hardware vor Ort ist eine entsprechende Verschlüsselung der Festplatten vorzunehmen.

3.3.1 Server

Der Server ist in das vorhandene Rack (Dell Rack 4210, 1999mm x 608mm x 999mm) im Neuen Rathaus einzubauen. Die Höhe des Servers darf dabei nur maximal zwei HE sein. Alle aufgeführten Anforderungen an die Server-Hardware sind als Mindestanforderungen zu verstehen:

· redundante Netzteile, 600W
- CPU Intel Xeon 24C/48T
· Microsoft Windows 2022 Standard, Desktop-Installation; oder gleichwertiges Betriebssystem (iX)
· Onboard 2x Gigabit Ethernet (RJ45), 1Gbit
· 2 USB-Anschlüsse
· RAID Hardware-Controller 2 GB Cache, batteriegepuffert
· 19 Zoll Einbauschienen für den Einbau in das vorhandene Rack
· Kabelmanagementarm
· IDRAC Enterprise
· Managementtool zur Überwachung von Festplatten, Netzteil u.a.
· Keine Wireless bzw. Infrarotschnittstellen
· Professional Support 5 Jahre, Next Business Day
· Optional: Verlängerung des Supports um 2 Jahre
- RAM 64 GB
- Festplatte1 480 GB SSD SATA Raid 1; Festplatte2 4 TB HD SATA Raid 1

3.3.2 Speichereinheit

Um den gesetzlichen Forderung einer lokalen getrennten Speicherung von Daten zu entsprechen, soll im Technischen Rathaus eine Speichereinheit in ein Rack (Dell Rack 4210, 1999mm x 608mm x 999mm) integriert werden. Die Daten müssen auf diesen Speicher mindestens zwei Jahr vorgehalten werden. Die Höhe der Speichereinheit darf dabei maximal zwei HE im Rack betragen. Es besteht aber auch die Möglichkeit einer externen Festplatte anstatt eines Rackservers, die den gleichen Anforderungen zur Speicherung von Daten wie ein Rackserver genügen muss.

Allgemeine Anforderungen an die Speichereinheit mit Einbau als Rackserver:

- redundante Netzteile, 600W
· Microsoft Windows 2022 Standard, Desktop-Installation; oder gleichwertiges Betriebssystem (iX)
· Onboard 2x Gigabit Ethernet (RJ45), 1Gbit
· 2 USB-Anschlüsse
· RAID Hardware-Controller 2 GB Cache, batteriegepuffert
· 19 Zoll Einbauschienen für den Einbau in das vorhandene Rack
· Kabelmanagementarm
· IDRAC Enterprise
· Managementtool zur Überwachung von Festplatten, Netzteil u.a.
· Keine Wireless bzw. Infrarotschnittstellen
· Professional Support 5 Jahre, Next Business Day
· Optional: Verlängerung des Supports um 2 Jahre

3.3.3 Thinclient

Der Thin-Client im SzA-Netz ist eine abgesetzte Bedienstation und wird im Technischen Rathaus eingesetzt, um das SzA zu bedienen. Dabei sollen folgende Mindestkriterien erfüllt werden:

- Betriebssystem Windows 10 Pro
- Intel Core i5-10500T
- 8 GB RAM
- 256GB SSD
- 5 Jahre HW-Support NBD

Das TFT sollte folgende Mindestanforderungen entsprechen:
- 27“ TFT
- Anschlüsse HDMI, VGA, DP
- Format 16:9
- Auflösung 1920x1080

Weiterhin muss der Thin-Client mit physischer Sicherung versehen sein und die systemspezifische Software, inclusive Konfiguration und Installation, vorhanden sein.

3.4 Anforderung an die Software System zur Angriffserkennung

Wie bereits unter 2.1 erwähnt muss die Ländersprache Deutsch für die Software SzA verwendet werden. Es muss eine Maussteuerung der Software möglich sein bzw. die Möglichkeit mit Kurzwahltasten wäre wünschenswert. Alle sinnvoll technisch realisierbaren Anforderungen unter dem gesamten Punkt 2 benannten Anforderungen eines SzA müssen erfüllt werden. Die Anforderungen für das SzA gelten mit dem Tag der öffentlichen Bekanntgabe der Ausschreibung (besonders MUSS-Anforderungen).

In der Anwendung selbst soll es möglich sein, mehrere gleich benannte eingegangene Vorgänge zu einem Vorgang zu erfassen. Es muss weiterhin eine Möglichkeit geben, den Relevanzbereich manuell einzustellen, damit keine Überflutung mit nicht relevanten Nachrichten stattfinden kann. Die für den definierten Relevanzbereich zugeordneten Vorgänge sollen dokumentiert werden und es muss eine entsprechende Auswertung über Reports visuell und tabellarisch möglich sein.

Wird für die weitere Bearbeitung von Protokollierungsdaten (Log-Dateien) noch andere Software mitverwendet, ist diese ebenfalls mit entsprechend der Vorgangsbearbeitung zu erläutern. Es muss jeder Zeit jeder Schritt nachvollziehbar sein.

4. Lizenzen

Es sind entsprechend alle Lizenzen für das SzA vom Betriebssystem bis hin zur Aufgabenerfüllung notwendigen Softwarepakete anzugeben. Entsprechend sind dabei Name des Softwarepaketes bzw. die Lizenznummern o.ä. in einer Anlage zum Angebot zu erfassen. Weiterhin ist bei den Lizenzen der entsprechende Lizenztyp anzugeben und entsprechend kurz zu erläutern.

5. Update, Sicherung und Image

Nach der erfolgten Installation des Gesamtsystems ist auf den entsprechenden Geräten ein Erst-Image zu erstellen. Dieses ist dann sicher vom Auftraggeber zu verwahren. Eine Imageerstellung soll einmal jährlich nach Terminabsprache zwischen Auftragnehmer und Auftraggeber stattfinden.

Die Sicherung der entsprechenden Dateien auf dem Server des SzA ist über das Raid 1 durch den Auftragnehmer entsprechend einzustellen. Weiterhin ist auf der örtlich getrennten Speichereinheit die Datensicherung vom Server zu spiegeln. Dieser Speichervorgang erfolgt unter Anleitung des Auftragnehmers durch den Auftraggeber. Dabei ist auf die Mindestspeicherung der Speichereinheit zu achten. Es sind die unter Punkt 2 getroffenen Anforderung zu Protokollierung, Detektion und Reaktion zu beachten.

Um auch die Hardware softwareseitig entsprechend auf den aktuellsten Stand zu halten, ist eine monatliche Prüfung des Ist-Standes (BIOS, Betriebssystem, Software) durch den Auftragnehmer durchzuführen und falls notwendig ein Update einzuspielen auch unter Anleitung des Auftraggebers. Dieser Sachverhalt ist monatlich zu protokollieren.

6. Test

Nach Abschluss des Aufbaues des SzA-Netzes ist ein Test für das Gesamtsystem SzA durchzuführen und zu protokollieren. Hierzu zählen zum Beispiel die Funktionsfähigkeit der Software, die Prüfung der Stimmigkeit der Firewallregeln der Zugriffe auf die zwei Netze, das Zugriffskonzept für die Nutzer (auch Token), Vorhandensein von Dokumentationen etc.

7. Wartung

Wie zum Teil unter Punkt 5 im dritten Absatz ist eine Prüfung der softwareseitigen Stände vorzunehmen und entsprechend auch zu protokollieren bzw. auch tätig zu werden. Die Wartung kann vom Auftragnehmer über Fernzugriff durchgeführt werden. Dabei ist zu beachten, dass ein personengebundener Token beim Auftraggeber beantragt wird, der für die Dauer des Vertragsverhältnisses bei der für die Wartung verantwortlichen Person verbleibt. Bei Verlust des Tokens ist der Auftraggeber sofort per Mail oder Telefon zu informieren. Ein Wartungsbuch ist entsprechend zu führen, entsprechend dem unter Punkt 5 genannten Rhythmus.

8. Schulung und Dokumentation

8.1 Dokumentationen

Für das System zur Angriffserkennung ist eine Systemdokumentation mit allen dazugehörigen Softwarekomponenten und der erforderlichen Netzwerkbeziehungen zu erstellen sowie das Datensicherungskonzept für die Backups des Servers und der Bedienstation zu übergeben. Weiterhin ist das Nutzerkonzept mit zu dokumentieren. Die Dokumentationen können elektronisch (pdf) übergeben werden. Bitte nicht die Form eines Wikis wählen.

8.2 Schulungen

Nach Einführung des SzA ist eine Schulung für eine Person (Administrator + Nutzer) am Echtzeitsystem vorzusehen. In der Folge sind noch zwei weitere Workshops, die über Videokonferenz möglich sind, mit einzuplanen.

9. Vergabekriterien

Der Zuschlag wird auf das unter Berücksichtigung aller Umstände wirtschaftlichste Angebot erteilt. Der niedrigste Angebotspreis allein ist nicht entscheidend. Insgesamt werden 100 Punkte vergeben. Die Bewertung erfolgt anhand folgender Zuschlagskriterien:

a. Gesamtpreis 60%

Berechnungsformel Preis:

$$P = \frac{\text{[Minimale Angebotssumme]}}{\text{(aktuelle Angebotssumme - minimale Angebotssumme) + [minimale Angebotssumme]}} \times 100 \times \frac{W_P}{100}$$

P = Ergebnis Preiswertung
W_P = Gewichtung des Wertungskriteriums Preis

Der Faktor [minimale Angebotssumme] steht für den positiven Betrag dieser Zahl. Daraus ergibt sich eine errechnete Punktezahl von maximal 100 Punkten. Die Angebotssummen werden vor der Berechnung kaufmännisch gerundet.

b. Bewertung Erfüllung im Kriterienkatalog Fachliche Anforderungen 40%

Berechnungsformel Kriterium b:

$$K = C \times \frac{W_C}{100}$$

K = Ergebnis Kriterium
C = Anzahl der erhaltenen Kriterienpunkte
W_C = Gewichtung des Wertungskriteriums

Die durch den führenden Bieter im Kriterienkatalog erzielten Höchstpunkte werden gleich 100 Punkte gesetzt. Entsprechend führen geringere Punktbewertungen zu prozentualen Abwertungen.

Beispiel:

Zuschlagskriterium	Bieter 1	Bieter 2	Bieter 2
Fachlicher Leistungsumfang	222,00	200,00	100,00
Punkte	**100,00**	**90,09**	**45,05**