1. Netzwerkstruktur/ -Sicherheit

IT-Anforderungen

Im Falle, dass die Geräte per Netzwerk verbunden werden können, müssen, aufgrund der sensiblen Infrastruktur des UKA, folgende Angaben und Informationen vom Anbieter, vor der Auftragsvergabe, mit Angebotsabgabe eingereicht werden.

Netzspannungsunterbrechung
Es ist zu beschreiben, wie sich die angebotenen Systeme bei einer plötzlichen Unterbrechung der Versorgungsspannung und/oder der Wasserversorgung verhalten.

Patch-Management

Der Auftragnehmer legt sein Konzept zum Patch-Management der auf seinen Geräten ablaufenden Software in Schriftform vor. Wird eine kritische OT-Sicherheitslücke in der Anwendung oder dem eingesetzten Betriebssystem bekannt, so hat der Auftragnehmer sicherzustellen, dass der verantwortliche Ansprechpartner des Auftraggebers binnen 48 Stunden vom Auftragnehmer informiert. Binnen zwei Wochen nach offiziellem Bekanntwerden des kritischen Sicherheitsproblems ist durch den Auftragnehmer die Sicherheitslücke geeignet zu schließen.

Kann diese Freigabe nicht erteilt werden, so ist dem verantwortlichen Ansprechpartner des Auftraggebers eine Risikoanalyse mit vorzuschlagenden Gegenmaßnahmen durch den Auftragnehmer zu überlassen. Sollte der Support für eingesetzte Betriebssysteme oder andere Softwarekomponenten von Drittherstellern enden und seitens des jeweiligen Herstellers keine Updates oder Patches für Sicherheitslücken mehr bereitgestellt werden, so ist die entsprechende Software kostenlos durch den Auftragnehmer gegen eine aktuelle supportete Version auszutauschen. Gegebenenfalls notwendige Änderungen/ Anpassungen des Gesamtsystems, um dies durchzuführen gehen auch zu Lasten des Auftragnehmers.

Fernwartung und Fernüberwachung
Der Zugriff zur Fernwartung wird vom Klinikum per Citrix-Netscaler ermöglicht. Wird dieser Zugang nicht vom Auftragnehmer unterstützt, so ist eine Alternative in Form einer Datenmatrix anzugeben. Wird eine Fernüberwachung angeboten muss diese beschreiben, welche Daten überwacht und gesteuert werden können.

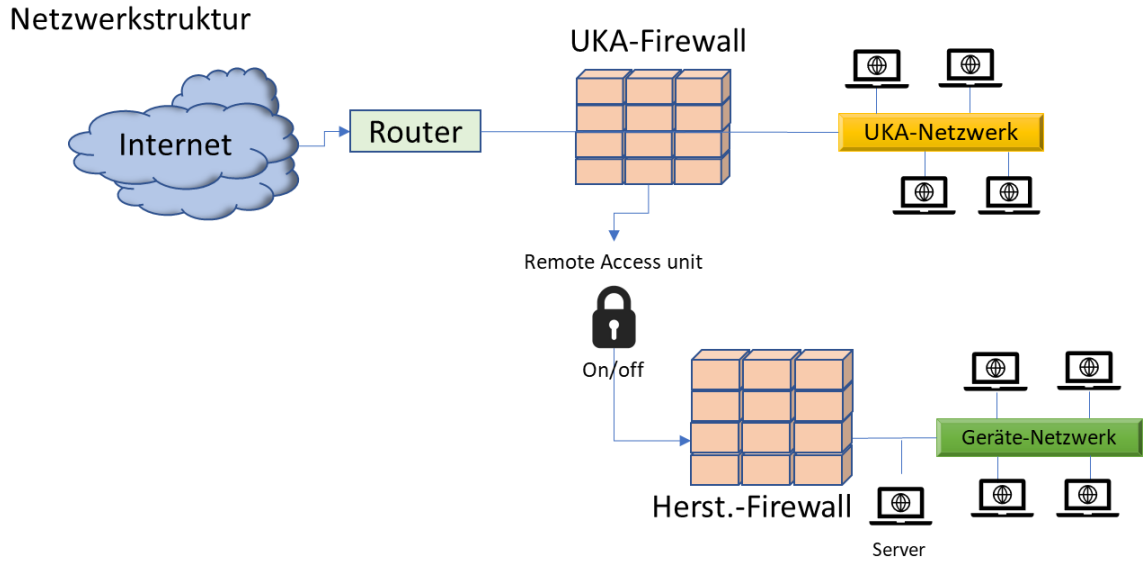
Netzwerk
Die vernetzbaren Geräte sind IPV4 fähig, unterstützen feste IP-Adressen (DHCP nicht gewünscht) und können über Netzwerksegmente hinweg kommunizieren. Anschuss Standard: 1000BASE-T (Gigabit Ethernet) / CAT 6A (oder besser) RJ45.

VPN:
Einwahl VPN (GlobalProtect Client2Side), sowie VPN Side2Side Tunnel sind ebenso konfigurierbar.

Software
Das UKA geht davon aus, dass nötige Software, die auf dem UKA-PC installiert werden muss, unter Windows 11 lauffähig ist.

Schnittstellen
Alle Schnittstellen, die zur Auswertung von Betriebsdaten dienen, müssen benannt und beschrieben werden.
Netzwerkstruktur

Die Systemanbindung ist grundsätzlich gemäß nachfolgender Struktur einzurichten:



Die Bieter sind aufgefordert die von Ihnen vorgesehene Netzwerkanbindung, basierend auf der o.a. Vorgabe mit eigenen Systemkomponenten grafisch darzustellen und dem Angebot beizufügen. Der Auftraggeber stellt bauseitig die Netzwerkinfrastruktur ab der Dose. Die Hersteller Firewall ist vom Auftragnehmer zu liefern.

Im Falle, dass für die Gerätevernetzung seitens des Anbieters zusätzliche Hardware (z.B. Server) erforderlich ist, wird diese vom Auftraggeber gestellt. In diesem Falle erfolgt die Gerätebetreuung durch den Auftraggeber. Der Anbieter ist aufgefordert die entsprechenden Hardwareanforderungen im Angebotskonzept zu benennen.

Anlage 10

Bitte Beantworten Sie nachfolgende Angaben zum System:

Nachfolgende Fragestellungen zur technischen Ausstattung Technischen sind über die freigegebenen Formularfelder zu beantworten:

Netzwerk:

Ist eine Netzwerkanbindung erforderlich? ..... (ja/nein)
Welche Netzwerkanbindung wird benötigt (höher) ..... ≤ 100 Mbit Angabe: .....
Spezielle Netzwerkanforderungen? (z.B. Glasfaserkabel, Firewall-Regeln)
Angabe: .....
Unterstützt das Gerät TCP/IP? ..... (ja/nein)

Verfügbarkeit/Einsatzbereich

Updates

Die Firma wird entsprechend dem Softwarepflegevertrag nach vorheriger Absprache mit den beiden Vertragspartnern GB-IT und Klinik einspielen.
..... (ja/nein)
Die Firma liefert im Vorfeld eine hinreichend detaillierte Beschreibung der Programm-Änderungen und deren Auswirkungen auf den Betrieb. Die Firma beantwortet darüber hinaus auf Anfrage weitere Fragen zum Update in schriftlicher Form.
..... (ja/nein)
Die Firma unterstützt im Rahmen die Klinik bei anfallenden Tests, indem sie angefragte Sachverhalte zeitnah beantwortet.
..... (ja/nein)

Kundendienst/Service
Existiert eine Hotline / Störungsannahme der Firma?
..... 24x7
..... nein
andere, Angabe: .....
Sprache (ja/nein) deutsch ..... englisch .....
andere, Angabe: .....

2. Datenauswertung

Der Auftragnehmer liefert ein Monitoring System zur lokalen Erfassung und Bereitstellung von Maschinen- und Prozessdaten aus Maschinen desselben Loses. Das Monitoring System ist im Gerätenetzwerk (s.o.) verortet und liest die Betriebsdaten der angeschlossenen Maschinen in einem für die Daten angemessenen Intervall aus.

Dabei erfasst das Monitoring System mindestens die folgenden Informationen:

- Los I:
  - Maschinenkennung
  - Stromverbrauch
  - Wasserverbrauch
  - Spültemperaturen (im Zeitverlauf)
  - Trocknungstemperaturen (im Zeitverlauf)
  - Fehlermeldungen
- Los II:
  - Maschinenkennung
  - Stromverbrauch
  - Wasserverbrauch
  - Spültemperaturen (im Zeitverlauf)
  - Trocknungstemperaturen (im Zeitverlauf)
  - Fehlermeldungen

Die Schnittstelle zu den Maschinen ist wie folgt gestaltet:

- Bei Änderungen der Schnittstelle seitens angebundener Maschine, **muss** durch den Auftragnehmer kostenfrei eine Aktualisierung der Schnittstelle des Monitoring Systems geliefert werden, so dass der Datenfluss an das Monitoring System gewährleistet ist.
- Falls die angebunden Maschinen die zu übertragenden Daten puffern, **soll** das Monitoring System fehlende Daten - z.B. aufgrund einer Störung von Schnittstelle, Monitoring System oder Übertragungsweg - nachträglich auslesen bzw. entgegennehmen.

Das Monitoring System legt die Daten in einem lokalen Speicherbereich automatisiert ab. Es bereitet die Daten auf und stellt sie dem Benutzer strukturiert mit Bezug zur jeweiligen Maschine z.B. im Tagesraster zur Verfügung. Die Datenbereitstellung erfolgt lokal, ohne Cloud-Anbindung.

Dem Benutzer muss mindestens eine der folgenden Schnittstellen zur Verfügung stehen:

- Dateisystemzugriff: Ablage der Daten in einem definierten Verzeichnis auf einem lokalen Server
- Netzwerkfreigabe (SMB 3.1.1/NFS 4.2): Zugriff auf die Daten über ein freigegebenes Verzeichnis im lokalen Netzwerk.
- SFTP: Optional kann ein lokaler FTP-Server zur Datenbereitstellung genutzt werden.

Das System schützt die Daten eigenständig vor unbefugtem Zugriff und stellt zusätzlich durch geeignete Authentifizierungsmechanismen sicher, dass nur berechtigte Nutzer Zugriff erhalten.

Das Monitoring System stellt die Daten wie folgt zur Verfügung:

- Die Daten müssen sowohl in mindestens einem maschinenlesbaren Format (z.B. CSV, JSON, XML), als auch in mindestens einem menschenlesbaren Format bereitgestellt werden (z.B. CSV, XLS)
- Jede Datei muss eindeutig identifizierbar sein durch MaschinenID und Zeitstempel
- Eine strukturierte Bereitstellung der Daten – z.B. durch eine Gliederung nach Maschine, Jahr, Monat und Tag- erleichtert den gezielten Abruf der Daten.

Der Anbieter ist aufgefordert das Monitoring System wie gefordert zu erläutern. Die Erläuterung muss mindestens enthalten:

- Eine Beschreibung der Systemarchitektur
- Anforderungen an Hardware, Software und die nötige Infrastruktur
- Konzept zur Integration in einen Datenverbund/Netzwerk
- Eine Beschreibung der Schnittstelle zum Abruf der Daten
- Ein Datensicherungskonzept

Der Auftragnehmer muss alle Anforderungen entsprechend den Best-Practice-Empfehlungen für Anforderungen an Lieferanten zur Gewährleistung der Informationssicherheit in Kritischen Infrastrukturen erfüllen (bsi.bund.de, UP KRITIS 11/2023).

Vom Auftragnehmer im Rahmen des Projektes gelieferte und integrierte Softwaremodule anderer Hersteller, werden vom Auftragnehmer, im Rahmen der Systempflege und Wartung entsprechend den nachfolgenden Zusagen/Vereinbarungen, als Generalunternehmer gehandhabt. Der Auftragnehmer übernimmt die Verantwortung für eine fehlerfreie und vollständige Funktion der Softwarekomponenten und erbringt die erforderlichen Pflege-, Wartungs- und Supportdienstleistungen zu den gleichen Bedingungen wie für die selbst entwickelten.

Die folgenden nichtfunktionalen Anforderungen sind zu erfüllen:

- Es gibt ein Incident & Problem Management
- Es gibt ein Change und Release Management
- Es gibt ein Havarie Konzept.
- Das Monitoring System des AN bieten alle erforderlichen Konfigurationsoptionen um die Anforderungen eines BSI-Grundschutzes / ISO27001 abbilden zu können.
- Der Auftraggeber hat das fortlaufend das Recht Datenschutzaudits und Lieferantenbewertungen im Sinne ISO 27001 beim AN durchzuführen.

Der Auftragnehmer stellt das Monitoring System mit unbeschränkten Nutzungsrechten zu Verfügung. Die Nutzung wird im Enterprise-Lizenzmodell lizenziert. Bei der Nutzungsgebühr handelt es sich um eine Pauschale unabhängig von der Anzahl der Nutzer des UKA und verbundener Unternehmen. Bei der Nutzung des Monitoring Systems fallen keine weiteren Kosten an.
Das Angebot muss vollständig sein. Es darf keine weiterführenden Kosten verursachen. Alle Komponenten, Abhängigkeiten und Voraussetzungen sind im Lizenzumfang enthalten.

Der Betrieb des Monitoring Systems erfolgt durch den Auftragnehmer im auf der Hardware des Auftraggebers, die Verantwortung für das Monitoring System trägt der Auftragnehmer. Installation, Wartung und Updates des Monitoring Systems übernimmt der Auftragnehmer. Zu diesem Zwecke schließt der Auftraggeber einen Wartungsvertrag mit dem Auftragnehmer.
Löschroutinen für Daten, die z.B. bedingt durch das Erreichen der gesetzlichen Aufbewahrungsfrist nicht mehr gespeichert werden müssen bzw. dürfen, müssen durch den Auftragnehmer beschrieben und dokumentiert werden, sodass die entsprechenden Prozesse bei der Implementierung des Produkts eingerichtet werden können. Daten in Protokolldateien sind ebenso zu berücksichtigen.

Im Falle einer Außerbetriebnahme verpflichtet sich der Auftragnehmer zu kostenfreien Übergabe der im Monitoring System enthaltenen Daten.

Der Auftragnehmer verpflichtet sich, die von ihm gelieferten Produkte zu härten, um die Auswirkungen potenzieller Sicherheitsrisiken zu minimieren. Es dürfen nur die Produkte installiert werden, die zur Nutzung notwendig sind. Jeder nicht benötigte Netzwerkzugang (TCP/IP- oder UDP-Port) muss deaktiviert sein. Die Nutzung jedes Zugangs muss in der Dokumentation des Aufragnehmers erläutert werden. Der Auftragnehmer muss im Rahmen seiner Möglichkeiten

sicherstellen, dass seine Produkte frei von „Backdoors“ sind, die die verwendeten Sicherheitsmechanismen umgehen können.

Wird vom Auftraggeber oder Auftragnehmer eine kritische Sicherheitslücke in dem Monitoring System bekannt, sind beide Seiten verpflichtet, einander im engen zeitlichen Zusammenhang darüber zu informieren und zu prüfen, ob sich aus der kritischen Sicherheitslücke eine Bedrohung ergibt.
Im Falle einer Bedrohung behält sich der Auftraggeber vor, den Zugang zum Monitoring System von außerhalb des Hausnetzes zu sperren oder das Monitoring System abzuschalten. Der Auftragnehmer informiert den Auftraggeber bei Sicherheitsvorfällen der Stufen kritisch und hoch innerhalb von 24h nach Bekanntwerden über Auswirkung und Umgang.

Der Auftragnehmer muss alle Angaben offenlegen, die für das Risikomanagement erforderlich sind. Dazu sind mindestens folgende Angaben für das angebotene Monitoring System zu liefern:

- Verhalten bei Netzwerkausfall Verhalten bei Virenbefall/ Virenangriff
- Verhalten bei Hackerangriff
- Verhalten bei Netzspannungsunterbrechung

Die Daten müssen vor Verlust, Zerstörung, vor unbeabsichtigter oder beabsichtigter Manipulation, Löschung und vor unberechtigter Einsichtnahme geschützt werden. Die Datensicherheit der ausgeschriebenen Lösung wird vom Auftragnehmer durch eine geeignete technische Umsetzung auf der Seite der Systemumgebung gewährleistet. Auch organisatorisch erforderliche Rahmenbedingungen und Vorkehrungen werden durch den Auftragnehmer berücksichtigt.