



CROSSHEALTH

Empfehlung
für den Rechenzentrumsbetrieb

STAND
08/2023

INHALTSVERZEICHNIS

Services	3
Hardware Server / Virtuelle Maschine VM	3
Partitionsgröße Virtuelle Maschine	3
Update Windows-Server-OS	3
Weitere Managed Services mit CROSSOS	4
Datensicherung	4
Netzwerk	5
Freizugebende Ports	6
Erforderliche Dienste unter Windows	9
URL Update Freigaben	9
Telematikinfrastruktur	9
CROSSHEALTH Connector	10
Dezentrale Komponenten	12
Clients	12
Kartenlesegerät	12
Peripherie Geräte Drucker/Scanner	12
Microsoft-Office	13

Services

Hardware Server / Virtuelle Maschine VM

Der CROSSHEALTH-Server läuft auf gängigen Virtuellen Maschinen (VMWare, HyperV, XenServer, KVM). Als Minimalanforderung definieren wir 64 GB RAM. Als Rechnerleistung wird ein Intel Xeon Serverprozessor mit einer Mindestgeschwindigkeit von 3,5 GHz für die VM empfohlen. Als Minimalanforderung empfehlen wir, der VM acht Kerne zur Verfügung zu stellen.

Basis dieser Lastanforderung ist die Basislizenz mit 12 Benutzern.

HINWEIS: CROSSSOFT stellt ausschließlich CROSSOS als Betriebssystem/Operating System zur Verfügung. Bei Verwendung von Windows-Lizenzen sind diese bauseitig zu stellen.

Server: 64GB Arbeitsspeicher (RAM)
Prozessor: 8 Kernen ab 3,5 GHz
OS: min. Windows Server 2016
SSD: 3 Terabyte

Partitionsgröße Virtuelle Maschine

Die Speicher-Bedarfs-Größe für 1000 Patienten liegt durchschnittlich bei 10 GB. Bei 30.000 Patienten kann man von einem Speicherbedarf von ca. 300 GB ausgehen. Wir empfehlen den Server mit 3 TB Speicher (vorzugsweise SSD's) auszustatten. Das Speichermedium muss mind. 3-mal so viel Platz aufweisen wie die Größe der Datenbank. Der Speicherbedarf eines eingescannten Arztbriefes sollte 500 KB nicht überschreiten. Werden andere Bilder (Patienten-Portraits, Fremdbefunde, Kindervorsorgehefte etc.) gescannt, kann der Speicherbedarf ansteigen.

Bei Nutzung von 64-bit Datenbanken erhöht sich der Speicherbedarf exponentiell.

HINWEIS: CROSSSOFT hat für unterschiedliche Betriebssystem-Umgebungen Programmerweiterung entwickelt und Nutzungslizenzen erstellt. Bevor Sie Betriebssystem-Umgebungen wechseln, sollten Sie die entsprechenden Anpassungen lizenzieren.

Update Windows-Server-OS

Wenn der Betreiber ein aktuelles Windows Server Betriebssystem stellt, hat das Update des Betriebssystems gemäß Richtlinie der Bundesärztekammer und Vorgaben der Gematik nach dem aktuellen Stand der Technik zu erfolgen. Hierzu wurden von der Bundesärztekammer die technischen Anlagen veröffentlicht, diese sind [hier](#) zu finden.

Bundesärztekammer und KBV haben die „Empfehlungen zur ärztlichen Schweigepflicht,

Datenschutz und Datenverarbeitung in der Arztpraxis“ überarbeitet.
Deutsches Ärzteblatt |09. 03. 2018| DOI: 10.3238/arztebl.2018.ds01 A
<https://www.crosssoft.de/assets/files/PDF/down138782477.pdf>

Alle Sicherheitsupdates sind nach dem Stand der Technik zu verwenden. Es sind die von Microsoft BSI-zertifizierten Windows Defender Security Center Funktionen zum Viren- und Bedrohungsschutz zur Laufzeit zu verwenden. Zur Erst-Installation oder beim Update sind die Veränderungen durch die CROSSSOFT- Installationsroutine zu bestätigen.

Weitere Managed - Services mit CROSSOS

Gerne informieren wir Sie auch zur Bereitstellung von durch CROSSSOFT überwachte Instanzen in Ihrem Rechenzentrum. Als Betriebssystem setzen wir CROSSOS ein. Unser speziell gehärteter Kernel und das ZFS-Dateisystem erledigen die Virtualisierung aller wichtigen Dienste (DNS, DHCP, Active-Directory, Mail, etc.).

Sektorenübergreifende Medizinische Informationssysteme einer neuen Generation mit CROSSOS:

Mit Hilfe der von uns genutzten „Jails“-Technologie und der webbasierten Administrationskonsole tragen wir mit CROSSOS dazu bei, ein hoch-sicheres, sehr stabiles und einfach zu wartendes Betriebssystem bereitzustellen.
CROSSOS basiert auf dem BSD-Microkernel (UNIX POSIX.1-Standard).

Der Applikations- Server wird von CROSSSOFT ausgeliefert und aktualisiert. Wir nutzen GlassFish bzw. Payara als Basis für den Open-Source-Anwendungsserver für Java EE.

Datensicherung

Führen Sie unbedingt täglich eine Datensicherung durch. Das Speichermedium muss mind. 2,5-mal so viel Platz aufweisen wie die Größe der Datenbank. CROSSSOFT stellt Verfahren zur Datensicherung zur Verfügung. Als Auftraggeber sollten Sie die Aufbewahrung dieser Daten in einer getrennten Brandschutzzone sicherstellen.

Im Weiteren verweisen wir auf die Rechtsprechung zum Thema Datensicherung und bitten Sie diese Anforderungen umzusetzen:

Ein Rechenzentrum, Provider oder Hostler ist dazu verpflichtet, ein Backup der Daten des Kunden anzufertigen – unabhängig davon, ob hierzu vertraglich etwas geregelt ist. Selbst wenn auch der Kunde keine Datensicherung vorgenommen hat, trägt der Provider den Schaden aus einem Datenverlust allein.

LG Duisburg, Urt. v. 25.7.2014 - 22 O 102/12

BGB §§ 241 Abs. 1, 254, 280 Abs. 1 Satz 1

- Für Endkunden gilt die Empfehlung die letzten sieben Tagessicherungen vorzuhalten
- Der Endkunde muss auch regelmäßig die Daten wieder herstellen, in dem er diese zurück sichert und die Sicherung prüft. Insbesondere bei sehr alten Daten-Beständen

und Servern über 5 Jahre Laufzeit gilt, ist die Datensicherung so langsam, dass die Nacht nicht ausreicht diese abzuschließen ist ein Ersatz zu schaffen.

- Werden Wartungs- und Pflegeintervalle nicht regelmäßig durchgeführt, hat ein Versicherer die Möglichkeit über Ausschlussklausel eine Schadenablehnung vorzunehmen. Klären Sie auf jeden Fall mit Ihrer Versicherung welche Maßnahmen (technisch, organisatorisch) zu treffen sind, damit im Schadensfall Ihre Versicherung greift.

HINWEIS:

Wir finden immer wieder abgebrochene Daten-Sicherungen vor, die dann natürlich unvollständig sind. Ein Datensicherungslaufwerk sollte immer einen Puffer an freier Plattenkapazität haben. Faustformel zwei Tagessicherungen als Puffer auf den Speichermedien zur Verfügung stellen.

Beispiel:

- Ihre Datenbank ist 111 GB groß.
- Zur Erzeugung des Dumps mit den Swapdateien benötigt das Betriebssystem ca. 160 GB
- Als Kunde sollten Sie täglich prüfen ob hinreichen freier Speicherplatz zur Verfügung steht.
- Das Rücksichern eines Dumps dauert in dieser Größe 9 Stunden.

Achtung: Wenn das Sicherungsprogramm unter MS auf C: laufen muss – ist auch dort temporärer Speicher zur Erstellung der Auslagerungsdateien erforderlich.

Netzwerk

Bei Neuinstallationen empfehlen wir, eine dem Stand der Technik entsprechende Verkabelung einzusetzen. Stand der Technik ist eine 1GB Verkabelung.

WLAN Verbindungen müssen bauseitig gegen Abhören gesichert werden. Wir empfehlen, 300Mbit/s Sender und Empfänger zu verwenden.

Bei Medizingeräten ist eine galvanische Trennung durch Optokoppler nach MPG bauseitig sicherzustellen. Für zukünftige Updates ist ein Internetzugang über https-Protokoll erforderlich, LTE-Verbindungen sind über VPN abzusichern.

CROSSSOFT stellt JEE Verfahren zur Verbindung der Clients mit der Datenbank zur Verfügung. Die objektorientierten Datenbanken bedürfen keiner externen Lizenzierung und werden gleichfalls von CROSSSOFT gestellt und mit Updates versehen.

Die weitergehende Überwachung der verschlüsselten Netzwerkverbindung hinsichtlich der genutzten Micro-Dienste sollten unbedingt unterbleiben, da diese die Ausführungsgeschwindigkeit der Ressourcen einschränkt.

Seit 01.01.2022 gilt die BSI KRITIS-Verordnung für alle Krankenhäuser.

Identity and Access Management (IAM) bzw. Zugriffs und Berechtigungsmanagement bietet einen Kanon an Sicherheitsmaßnahmen für Krankenhäuser in der kritischen Infrastruktur. Eine Authentifizierung der Benutzerlogins über Microsoft Active Directory ist

lizenzierbar. Ein Zugriff für Drittsoftware sollte gemäß B3S unterbunden werden. Vgl. ANF-MN105

Informationssicherheit im Krankenhaus Branchenspezifischer Sicherheitsstandard (B3S)"
<https://www.dkgev.de/themen/digitalisierung-daten/informationssicherheit-und-technischer-datenschutz/informationssicherheit-im-krankenhaus/>

Freizugebende Ports

Die freizugebenden Ports sind von der Installationsreihenfolge der Anwendungen abhängig. So können diese von der unten dargestellten Liste abweichen, um sicherzustellen, dass die richtigen Ports ausgewählt werden. Müssen diese in der Registry überprüft werden. Dazu gehen Sie bitte in folgendes Verzeichnis:

HKEY_LOCAL_MACHINE\SOFTWARE\CROSSSOFT

Dort werden die Registryeinträge für die einzelnen Anwendungen von CROSSSOFT dargestellt. Im folgenden werden die Einträge dargestellt, wo die Ports für die Anwendung zu finden sind.

- HKEY_LOCAL_MACHINE\SOFTWARE\CROSSSOFT\CROSSHealth\Server
- HKEY_LOCAL_MACHINE\SOFTWARE\CROSSSOFT\Firebird\Server
- HKEY_LOCAL_MACHINE\SOFTWARE\CROSSSOFT\Glassfish
- HKEY_LOCAL_MACHINE\SOFTWARE\CROSSSOFT\PostgreSQL

Beispiele für die Ports:

Port	Bezeichnung	Beschreibung
445	Netzlaufwerk	Samba Netzwerkfreigabe mit Anwendung
3050	Firebird Server	Datenbankserver für Dokumente und Abrechnung
3701	Port ORD	Glassfish Object Request Broker
3820	Port ORBSSL	Glassfish Object Request Broker SSL
3920	Port Mutualauth	Authentifizierung
4533	PostgreSQL	Datenbankserver User
4848	Glassfish	Glassfish Admin KonsoleF
4849	Port Admin	Glassfishkonsole
7677	Port IMQ	Message Queue
8027	Port HL7	HL7-Schnittstelle
8080	HTML SPZManager	HTML-Formulare (bsp. Heilmittel)
8081	HTML PROX/CROSSHEALTH	HTML-Formulare (bsp. Heilmittel)
8089	Launcher	Launcher Dienst zum Updaten der Anwendung
8091	Masterdata	Medikationsdienst
8182	Port HTTPS	HTTPS Aufruf (bsp. Medikationstool)
17676	Port PROX/CROSSHEALTH	Datenbank-Kommunikation 17679 Port_
17679	Port_RMI PROX/CROSSHEALTH	Remote-Method-Inducation

Für CROSSOS Kunden müssen folgende Ports offen sein:

- 445 , Netzlaufwerk, Samba Netzwerkfreigabe auf der die Anwendung ist
- 8091, Launcher, Launcher Dienst zum Updaten der Anwendung
- 8089, Masterdata, Medikationsdienst
- 4848, Glassfish, Glassfish Admin Konsole

Erweiterung der Gruppenrichtlinie

FirebirdGuardiancrosssoft (startet den FirebirdServer mit)

1. CROSSSOFT_PostgreSQL
2. CROSSSOFT_Glassfish

Die Gruppenrichtlinien müssen so eingerichtet werden, dass der Endnutzer Zugriff auf folgende Dateien hat (Pfadregel).

Die .OCX CSWebXCtrl muss durch den Administrator registriert und freigegeben werden, falls das Registry für die Software des Endnutzer gesperrt ist.

Befehl:

```
regsvr32 /PFAD/ZU/SPZMANAGER-INSTALLATION/CSWebXCtrl/CSWebXCtrl.ocx
```


Erforderliche Dienste unter Windows

CROSSHEALTH und PRO X Plattform:

CROSSSOFT_GATEWAY → für CROSSHEALTH Client
CROSSSOFT_Glassfish → Applikations-Server
CROSSSOFT_HEALTH → für Content-Dienste wie Arzneimittel
CROSSSOFT_ICF → für ICF/PART-CHILD
CROSSSOFT_PostgreSQL → Datenbank
FirebirdGuardiancrosssoft → PRO X
Datenbank FirebirdServercrosssoft → PRO X
Datenbank

Bei Problemen und Neustart Reihenfolge beachten.

URL Update Freigaben

Der https Zugriff auf die Content-Dienste muss freigegeben sein:

abdamed-files.crosssoft.de Arzneimittel
crosscloud.crosssoft.de CROSSSOFT Programm-Update
icd-files.crosssoft.de ICD und Heilmittel

Bitte richten Sie in Ihrer Firewall Freigaben für:

*crosssoft.de
und *crosshealth.services ein.

Telematikinfrastruktur

Wir nutzen Managementsoftware, um skalierbare Kartenlesegeräte mit Servern und Konnektoren zu koppeln. Unser Bestätigungsvermerk der Gematik für das hier beschriebene Szenario lautet: Gematik_Konf-PS_2018-06-28_001423
Verfahrensschlüssel Konnektorenschnittstelle: ZLS_Konf-PS_CRSFT_002023

Gemäß aktueller Fassung des §291b Abs. 2 SGB V haben an der vertragsärztlichen Versorgung teilnehmende Leistungserbringer bei der erstmaligen Inanspruchnahme ihrer Leistungen durch einen Versicherten die Leistungspflicht der Krankenkasse durch die Nutzung der Dienste nach § 293 Abs. 1 SGB V zu prüfen.

Dies hat Auswirkungen auf die §301-(AMBO) Abrechnung

„Ab dem 01.01.2021 teilen die von o.g. Regelung betroffenen Einrichtungen den Krankenkassen durch den Abschlag [2,3,4,6,7,8]9200000 die Durchführung der Prüfung im Rahmen der Abrechnungsunterlagen mit dem Rechnungssatz Ambulante Operation

dahingehend mit, dass in den Fällen, in denen keine Onlineüberprüfung nach §291b Abs. 1 SGB V stattgefunden hat, dieser Abschlag (in Höhe von 2,5 von Hundert des zuvor ermittelten Rechnungsbetrages im Segment REC – ohne Berücksichtigung des Abschlags selbst) im Segment ENA zum Ansatz gebracht wird. In allen anderen Fällen erfolgt keine Abrechnung des Abschlags und es wird eine Durchführung der online Überprüfung nach §291b Abs. 1 SGB V durch den Leistungserbringer angenommen.“ Vgl. Aktuelle Anforderung GKV-Spitzenverband vom 15.12.2020 Connector

Zur Vermeidung von Datenschutz relevanten Störfällen sollte im Rahmen der Risiko-Minimierung vom Einsatz unvollständiger oder nicht überschaubarem Austausch von Komponenten abgesehen werden.

Beispiel:

Die Gematik wurde am 30.6.2023 von einem KIM-Anbieter darüber in Kenntnis gesetzt, dass es innerhalb der „Kommunikation im Medizinwesen“ (KIM) zu einer Fehlleitung von Nachrichten gekommen ist. Betroffene KIM-Nachrichten wurden somit nicht, wie beabsichtigt, an die AOK Niedersachsen geleitet, sondern an eine einzelne Arztpraxis. Nach derzeitigen Angaben des Fachdienstes der betroffenen Arztpraxis geht es um ein Mengengerüst von 116.466 eAU-Nachrichten, die seit September 2022 an diese einzelne Arztpraxis fehlerhaft versendet wurden.

Wie kam es zu dem Vorfall?

Jeder Fachbereich hat, wie seit Jahren von der Softwareindustrie kritisiert seinen eigenen Verzeichnisdienst erhalten. Werden unterschiedliche Module unterschiedlicher Hersteller zu einer TI zusammengefügt ist nicht definiert, wo welche Konfigurationen vorgenommen werden.

Ein Kombination mit Drittsoftware sollte gemäß B3S nur nach Test und Freigabe aller beteiligter Anbieter erfolgen.

Informationssicherheit im Krankenhaus Branchenspezifischer Sicherheitsstandard (B3S)
<https://www.dkgev.de/themen/digitalisierung-daten/informationssicherheit-und-technischer-datenschutz/informationssicherheit-im-krankenhaus/>

Abhilfe/Empfehlung:

CROSSSOFT hat deshalb von Anfang an die Komponenten für eine Provider-Zulassung entwickelt und zertifiziert, so dass wir mit den Kooperationspartnern MZD (Secunet/Bertelsmann/eHex) IBM und Telekom den gesamten Prozess abbilden und prüfen können. Entsprechend realisieren wir auch für Dampsoft-Kunden weiterhin die TI.

CROSSHEALTH Connector

Mit dem CROSSHEALTH HL7CONNECTOR. bietet CROSSSOFT eine transparente bidirektionale Datenaustausch-Schnittstelle zu den internen Klinikinformations- und Kommunikationssystemen (KIS) von Krankenhäusern.

Der internationale Standard HL7 (Health Level Seven) ist ein herstellerunabhängiges Übertragungsprotokoll für den Datenaustausch im Krankensektor.

CROSSSOFT Ihre IHE Domäne Caretaker

Wird VSDM in Adaption VSDM an führende Systeme (KIS/ERP) durchgeführt und an CROSSSOFT übergeben, ist die HL7-ADT-Schnittstelle zu erweitern:

Einrichtungsseitig ist zu klären wer die HL7 Version 2/Admission, Discharge and Transfer (ADT) ändern kann. HL7/ADT bezeichnet eine Gruppe von HL7-Nachrichten, die zur Übermittlung von Informationen zur Aufnahme, Entlassung und Verlegung eines Patienten dienen. Der Abschnitt IN3 - Insurance Additional Information, Certification ist zu aktualisieren. Die Felder 28-31 sind zu ergänzen:

IN3 - Insurance Additional Information, Certification

- 1.1 IN3-28 Online Verification Date/Time
- 1.2 IN3-29 Online Verification Result
- 1.3 IN3-30 Online Verification Result Error Code
- 1.4 IN3-31 Online Verification Result Check Digit

Quelle: wiki.hl7.de/index.php?title=Segment_IN3

Dezentrale Komponenten

Clients

Das System kann heterogen auf verschiedenen Devices / Ausgabegeräten für den Nutzer bereit gestellt werden. Rich-Clients bieten als Framework-Softwarelösungen applikationsspezifische Funktionalität wie Benutzerschnittstellen.

Rich-Clients

Ab Windows 10 32 Bit (Client)

Minimale Hardware ab 4 x 3,0 GHz

RAM mind. 16 GB

Grafikkarte mit einer Auflösung von 1024x768 bei 16 Bit Farbtiefe

Serielle und Parallele Schnittstellen

Tastatur, Maus

Monitor 17“, Auflösung mind. 1024x768, 75 Hz ;

4K-Video-Streaming Geräte und Gaming-Konsolen werden nicht empfohlen, da hier immer wieder die Auflösung angepasst werden muss

Festplattenspeicher oder SSD ab 100 GB empfohlen

Thin-Clients

Es können Microsoft RDP Clients, MS Terminalclients oder CITRIX Clients verwendet werden. Entsprechend sind die Netzwerkfreigaben erforderlich: \\IP/CROSSSOFT/CROSSHealth/Client

Nur Leserechte

Empfohlen min. 8 GB RAM je Nutzer

Mit der Installationsroutine des Clientaufrufes wird in der Clientumgebung der Microsoft XML-Parser konfiguriert. Dieses ist bauseits sicherzustellen. Die Desktop-Verknüpfung zum Client kann als Gruppenrichtlinie konfiguriert und ausgerollt werden. Damit entfällt die Installation (Zero-Client).

Kartenlesegerät

Wir unterstützen nur durch die „Gematik“ zertifizierte und zugelassene Lesegeräte.

Peripherie Geräte Drucker/Scanner

Wir empfehlen für den Druck von BTM separierte Nadel-Drucker. Die Nadeldrucker sollten generell im Epson-Modus und nicht im IBM-Modus arbeiten.

Für eine Blankoformularbedruckung können Multifunktionsgeräte nicht empfohlen werden, weil A6 Rezepte häufig unter dem Scanneraufsatz verschwinden.

- . EPSON LQ 570+ und 580 (Für diesen Drucker empfehlen wir den Generic Druckertreiber.)
- . OKI ML 390 FB und 590 FB
- . Panasonic KX P2124

Microsoft-Office

Laut Kammerrichtlinie darf Microsoft-Office 365 nur eingesetzt werden, wenn sichergestellt ist, dass keine Patientendaten über einen von Microsoft oder deren Partnern gehosteten Server laufen.

Wir benötigen dafür den schriftlichen Nachweis. Die CROSSSOFT Makro-Datei heißt CSWord.dot und wird vom CROSSSOFT Word-Installer beim Client-Start aus dem Verzeichnis ...Client\bin\Word in das STARTUP-Verzeichnis von Word kopiert, C:\Users\XXX\AppData\Roaming\Microsoft\Word\STARTUP

Word-Dokumente und Vorlagen werden nicht im Dateisystem, sondern in der Dokumenten-DB gespeichert. Bei Arbeitsgruppeninstallationen, ist bauseits eine Umgebungsvariable anzulegen, damit Word gestartet werden kann.

Microsoft 365 von Microsoft Deutschland GmbH, Konrad-Zuse-Straße 1 85716 Unterschleißheim ist eine individuell für Geschäftskunden zusammengestellte Office-Plattform, deren Einsatz vom Kunden zu testen ist. Insbesondere das Installationsmedium zur Einrichtung von FAT-Clients bedarf des chronologischen Aufbaus der VBA und Patch Einträge in der Registrierung, da ansonsten eine Nutzung der Word Add Ins ausgeschlossen ist.

Kontakt

Bei Fragen stehen Ihnen unsere Fachbereichs-Hotlines von Montag bis Freitag (außer an gesetzlichen Feiertagen) jeweils in der Zeit von 8:00 bis 13:00 Uhr und zusätzlich Montag, Dienstag und Donnerstag von 13:00 - 17:00 Uhr zur Verfügung

Zentrale:

Rufnummer : 0431 - 38 21 77 40
Faxnummer: 0431 - 38 21 77 48
E-Mail: info@crosssoft.de

Besucheradressen CROSSOFT. GmbH

Knooper Weg 126/128 24105 Kiel	Bahnhofstr. 5 96199 Zapfendorf (Bamberg)
-----------------------------------	---



Amtsgericht Kiel
USt-IdNr.:

HRB 6457
DE178 836 476

Geschäftsführender Gesellschafter:

Dirk Sommer

CROSSSOFT. GmbH
Knooper Weg 126/128
24105 Kiel