IT-Richtlinie zur Fernwartung von MIT-Systemen (extern)

Version: 4

Matthies, Daniel MIT-Abteilung 6 Seite(n)

MKK Mühlenkreiskliniken

Inhaltsverzeichnis

MKK Mühlenkreiskliniken

1 Einleitung

Die rasante Weiterentwicklung der MIT-Systemlandschaft im Gesundheitswesen und der damit immer größer werdenden Komplexität der IT-Infrastruktur macht es erforderlich, dass Servicepartner Zugriff auf diese Systeme bekommen. Diese Zugriffe erfolgen in der Regel durch einen Fernzugriff, um Auftrags- und/oder Wartungsarbeiten am System durchzuführen. Dabei kann nicht ausgeschlossen werden, dass zur Bearbeitung einer kundenseitigen Serviceanfrage, wie beispielsweise einer Störmeldung der Zugriff auf personenbezogenen Daten erforderlich ist.

Diese Richtlinie beschreibt die organisatorische und technische Ausgestaltung einer Fernwartung von MIT-Systemen der Mühlenkreiskliniken (MKK) als Ergänzung zum MKK-Standardvertrag zur Auftragsverarbeitung. Sie basiert auf der Praxishilfe der Gesellschaften/Verbände BVITG, GMDS und GDD Anforderungen an die (Fern)Wartung medizinischer IT-Systeme, Version 1.0 vom 23.05.2018 unter Berücksichtigung der datenschutzrechtlichen Anforderungen der EU-Datenschutzgrundverordnung (DS-GVO).

2 Geltungsbereich

Diese Richtlinie gilt für alle Beschäftigte des Unternehmens und Ihrer Tochterunternehmen. Dazu gehören alle Festangestellte, Teilzeitangestellte, Auszubildende, Studenten sowie Aushilfskräfte etc.

Auch externe Personen, die in unserem Unternehmen tätig sind, sind verpflichtet, sich an diese Richtlinie zu halten. Das Unternehmen wird entsprechende Vorkehrungen treffen, damit externen Personen, welche auf Grundlage einer wirksamen Beauftragung für die MKK tätig werden, wirksam auf die Einhaltung dieser Richtlinie verpflichtet sind und somit diese auch für sie verbindlich ist.

3 Verantwortungsbereiche/Verantwortlichkeiten/Weisung

Alle im Geltungsbereich genannten Personen müssen sich der Bedeutung von IT-Sicherheit bewusst sein. Sie müssen die IT in ihrer täglichen Arbeit verantwortungsbewusst einsetzen, das Regelwerk zur IT-Sicherheit beachten und die verantwortlichen Stellen über sicherheitsrelevante Ereignisse informieren.

Die Gesamtverantwortung für die Informationssicherheit obliegt der Unternehmensleitung der MKK. Diese wird fachlich durch das Informationssicherheitsmanagement (ISM) wahrgenommen.

Die fachliche Entwicklung und Umsetzung von technischen IT-Sicherheitskonzepten und Maßnahmen zur Sicherstellung von IT-Schutzbedarfen obliegt der MIT-Abteilung der MKK. Sie begleitet Maßnahmen und Prozesse im Rahmen des für die MKK geltende Informationssicherheitsmanagementsystems (ISMS).

In diesem Rahmen wird diese Richtlinie regelmäßig, jedoch mindestens einmal pro Jahr, durch die MIT-Abteilung der MKK in Zusammenarbeit mit dem ISM auf ihre Aktualität und Konformität mit den IT-Sicherheitsregelungen der MKK überprüft und ggf. angepasst.

Die im Geltungsbereich genannten Personen sind verpflichtet, den Weisungen der MIT-Abteilung mit Bezug auf die Informationstechnik Folge zu leisten. Sofern Zweifel an der Richtigkeit oder der Sinnhaftigkeit von Weisungen der MIT-Abteilung bestehen, kann die Abteilungsleitung MIT eingebunden werden.

4 Zuwiderhandlungen

Im Falle von Mitarbeitern der MKK und deren Tochtergesellschaften kann eine Zuwiderhandlung/ein Verstoß arbeits- oder dienstrechtliche Konsequenzen nach sich ziehen. Im Falle des Vorliegens von grober Fahrlässigkeit oder Vorsatzes können dem Unternehmen entstandene Schäden gegenüber dem Mitarbeitenden ganz oder teilweise geltend gemacht werden.

Im Falle externer Personen, Systemanbieter und Dienstleister kann eine Zuwiderhandlung/ein Verstoß vertragliche Konsequenzen und Strafzahlungen nach sich ziehen. Im Falle des Vorliegens von grober Fahrlässigkeit oder Vorsatzes können dem Unternehmen entstandene Schäden gegenüber dem externen Partner ganz oder teilweise geltend gemacht werden.

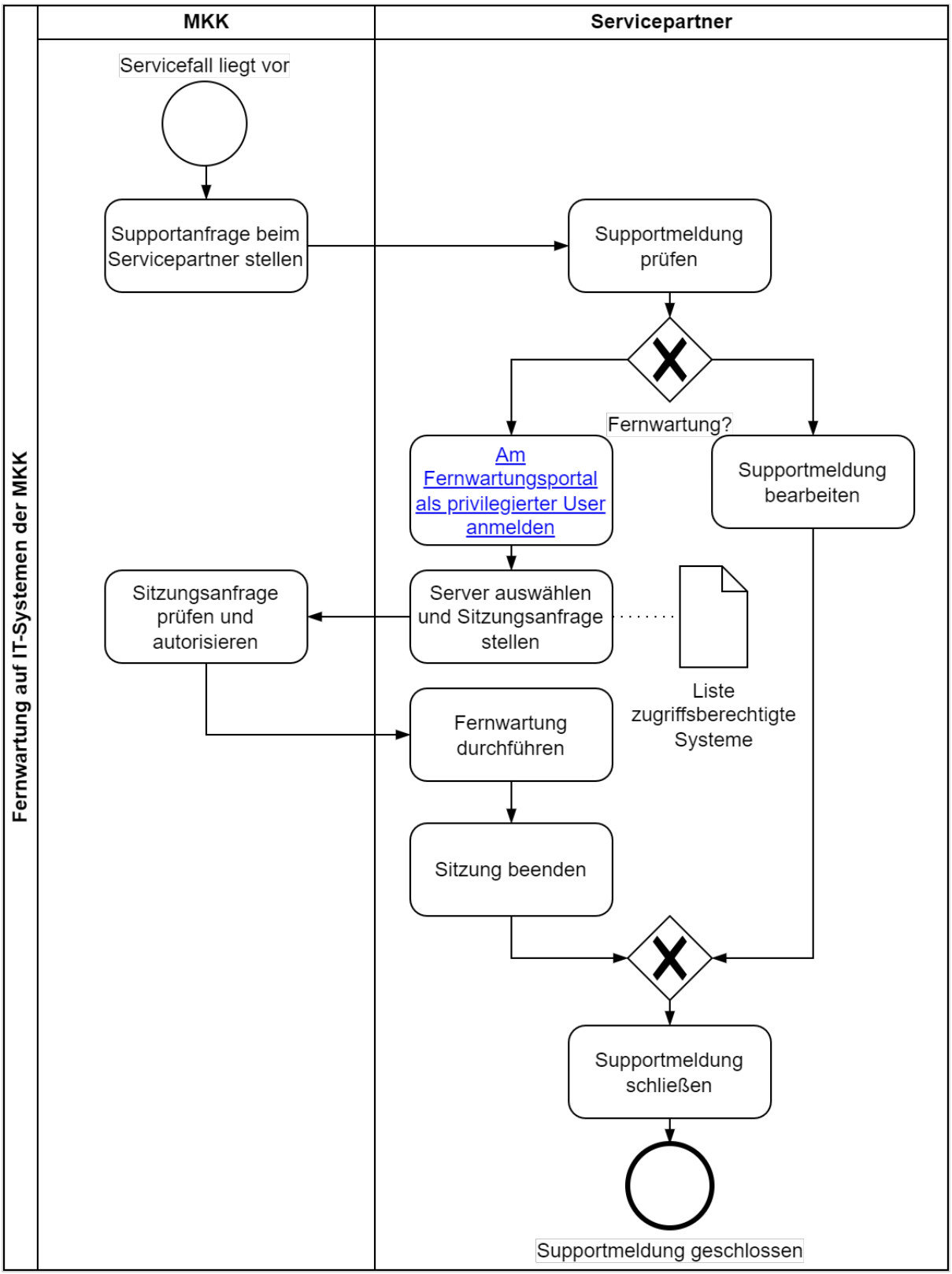
5 Einhaltung von Rechtsvorschriften

Bei der Benutzung der MIT-Systeme und Diensten der MKK sind von den im Geltungsbereich genannten Personen die geltenden Rechtsvorschriften zu Datenschutz und Datensicherheit sowie die Unternehmensregelungen einzuhalten. Sollten die im Geltungsbereich genannten Personen unsicher sein, ob und inwieweit Rechtsvorschriften oder Unternehmensregelungen einzuhalten sind, haben sie sich vorab an ihren Vorgesetzten, den Datenschutzbeauftragten oder an das ISM zu wenden.

Für Servicepartner gelten die rechtlichen Rahmenbedingungen aus dem geschlossenen Vertrag zur Auftragsverarbeitung.

MKK Mühlenkreiskliniken

6 Prozessbeschreibung



Die MKK setzen zur Fernwartung von IT-Systemen das Privileged Access Managementsystem von BeyondTrust ein. An diesem System können sich privilegierte, namentlich benannte Mitarbeitende eines Servicepartners zu Zwecken der

Mühlenkreiskliniken

Fernwartung anmelden. Die technische Umsetzung ist im nachfolgenden Kapitel beschrieben. Mit dem Fernwartungssystem wird sichergestellt, dass die gesetzlichen Vorgaben aus der EU-DSGVO eingehalten werden (Artikel 5, 7, 15, 17, 18, 20, 25, 32, 33).

Der Fernzugriff ist vom Servicepartner zu beantragen und die Korrektheit der Angaben vom Vorgesetzten (Servicepartner) zu bestätigen.

Jeder privilegierte Mitarbeitende eines Servicepartners bekommt ein initiales Passwort in einer verschlüsselten E-Mail mitgeteilt, welches unmittelbar nach der Erstanmeldung geändert werden muss. Das zu setzende Passwort muss komplex sein (mind. 8 Zeichen mit Kleinbuchstaben, Großbuchstaben, Ziffern und Sonderzeichen) und darf nicht weitergegeben werden. Da es sich bei den privilegierten Benutzern um Benutzerkonten mit weitreichenden Berechtigungen handelt, müssen diese mit mind. zwei Authentisierungsmerkmalen geschützt werden. Dazu ist im Grundsatz die Aktivierung der Zwei-Faktor-Authentifizierung im Fernwartungssystem vorgesehen.

Scheidet ein Mitarbeitender aus, so ist dies den MKK unverzüglich mitzuteilen. Das Konto wird dann gelöscht oder mind. gesperrt.

Die Fernwartung muss, sofern zur Bearbeitung einer Serviceanfrage möglich, in einer anonymisierten Testumgebung erfolgen. Der Zugriff auf ein Produktivsystem mit personenbezogenen Daten wird nur gewährt, wenn ein Wartungsziel anders nicht erreicht werden kann. Dazu erfolgt eine temporäre Freischaltung nur auf expliziter Anforderung unter Angabe einer Referenz des Kunden, wie z.B. der Ticket-/Auftrags-Nr. über das Fernwartungssystem. Ohne Angabe der Ticket-/Auftrags-Nr. wird pauschal kein Zugriff gewährt.

Fernwartungstätigkeiten sind frühestmöglich zu planen und als Anfrage über das Fernwartungssystem zu versenden, sodass in der regulären Dienstzeit der MKK IT eine Autorisierung erfolgen kann. Die regulären Dienstzeiten sind Mo.-Do. von 07:30 bis 16:00 Uhr und Fr. von 07:30 bis 12:45 Uhr. Außerhalb der regulären Dienstzeiten der MIT-Abteilung der MKK ist eine Autorisierung des Fernzugriffs durch die MIT-Abteilung der MKK innerhalb der vertraglich vereinbarten Servicezeiten mit dem Vertragspartner sichergestellt.

Beim Start und bei Beendigung einer Sitzung wird automatisch eine Benachrichtigung per E-Mail an den MIT-Systembetreuer der MKK geschickt. Jeder privilegierte Mitarbeitende bekommt eine mit den MKK abgestimmte Auswahl an berechtigten Systemen zugewiesen. Der Fernwartungszugang ist nur innerhalb der vertraglich vereinbarten Servicezeiten mit dem Servicepartner möglich. Die Aktivitäten in einer Fernwartung werden protokolliert, aufgezeichnet und max. 90 Tage aufbewahrt. Die MIT-Abteilung hat im Bedarfsfall Zugriff auf diese Protokolldateien.

7 Technische Umsetzung

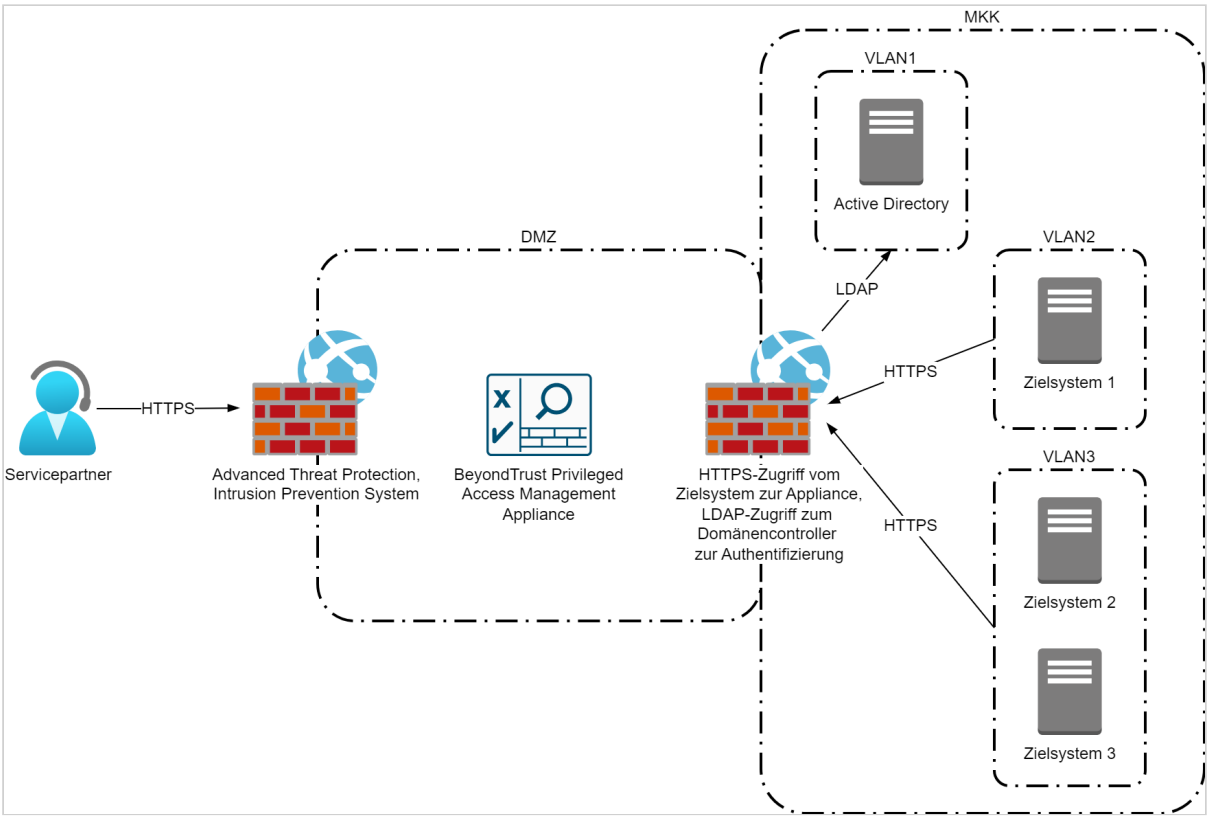
Der Verbindungsaufbau erfolgt über das sichere Übertragungsprotokoll HTTPS an der BeyondTrust Appliance mittels eines persönlichem Benutzerzugangs, der gegenüber dem Active Directory der MKK authentifiziert wird. Die Verbindung ist mittels eines SHA-265 signierten SSL-Zertifikats verschlüsselt.

Die BeyondTrust Appliance wird nach außen mit einer *Stateful Inspection Firewall* und einem *Intrusion-Prevention-System* abgesichert und überwacht. Sie dient als Middleware innerhalb der DMZ und hat extern und intern jeweils eine eigene physikalische Netzwerkverbindung. Zudem ist sie in einem eigenen VLAN isoliert innerhalb der DMZ.

Die Zielsysteme der MKK dürfen nur mittels HTTPS eine Verbindung zu der BeyondTrust-Appliance aufbauen. Dies wird feingranular mittels der Stateful Inspection Firewall von der DMZ in das Unternehmensnetzwerk der MKK für jedes Zielsystem konfiguriert und überwacht. Der zugehörige Jump Client auf den Zielsystemen unterbindet den Sitzungswechsel zu anderen Systemen.

Die komplette Sitzung wird als Video aufgezeichnet. Zudem werden folgende Daten protokolliert.

- Start-/ Enddatum und Uhrzeit
- Login-Name des Dienstleisters
- Zielsystem: IP-Adresse, Computername und Betriebssystem
- Dienstleistersystem: IP-Adresse, Computername und Betriebssystem
- Ausgeführte Anwendungen mit Dateipfad, Zeitstempel und Fenstertitel
- Chatprotokoll
- Session-ID
- Übertragene Dateien (nur Upload möglich)


MKK
VLAN1
Active Directory
DMZ
VLAN2
LDAP
HTTPS
Zielsystem 1
HTTPS
Servicepartner
Advanced Threat Protection, Intrusion Prevention System
BeyondTrust Privileged Access Management Appliance
HTTPS-Zugriff vom Zielsystem zur Appliance, LDAP-Zugriff zum Domänencontroller zur Authentifizierung
HTTPS
VLAN3
Zielsystem 2
Zielsystem 3