Anforderungen an die (Fern) Wartung medizinischer IT-Systeme

Eine Zusammenarbeit von

Bundesverband Gesundheits-IT e. V.
Arbeitsgruppe Datenschutz & IT-Sicherheit

Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V.
Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“

Gesellschaft für Datenschutz und Datensicherheit e. V.
Arbeitskreis „Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen“

Autoren (alphabetisch)

Isele, Christoph	Cerner Health Services Deutschland GmbH
Kaufmann, Pierre	
Koeppe, David	Vivantes - Netzwerk für Gesundheit GmbH
Neumann, Conrad	medatixx GmbH & Co. KG
Schütz, Thorsten	Klinikum Itzehoe
Schütze, Dr. Bernd	Deutsche Telekom Healthcare and Security GmbH
Spyra, Gerald	Ratajczak und Partner mbB Rechtsanwälte

Version 1.0

Stand der Bearbeitung: 23. 05. 2018

Inhaltsverzeichnis

Haftungsausschluss

Das vorliegende Werk ist nach bestem Wissen erstellt, der Inhalt wurde von den Autoren mit größter Sorgfalt zusammengestellt. Dennoch ist diese Ausarbeitung nur als Standpunkt der Autoren aufzufassen, eine Haftung für die Angaben übernehmen die Autoren nicht. Die in diesem Werk gegebenen Hinweise dürfen daher nicht direkt übernommen werden, sondern müssen vom Leser für die jeweilige Situation anhand der geltenden Vorschriften geprüft und angepasst werden.

Die Autoren sind bestrebt, in allen Publikationen die Urheberrechte der verwendeten Texte zu beachten, von ihnen selbst erstellte Texte zu nutzen oder auf lizenzfreie Texte zurückzugreifen.

Alle innerhalb dieses Dokumentes genannten und ggf. durch Dritte geschützten Marken- und Warenzeichen unterliegen uneingeschränkt den Bestimmungen des jeweils gültigen Kennzeichenrechts und den Besitzrechten der jeweiligen eingetragenen Eigentümer. Allein aufgrund der bloßen Nennung ist nicht der Schluss zu ziehen, dass Markenzeichen nicht durch Rechte Dritter geschützt sind!

Copyright

Für in diesem Dokument veröffentlichte, von den Autoren selbst erstellte Objekte gilt hinsichtlich des Copyrights die folgende Regelung:

Dieses Werk ist unter einer Creative Commons-Lizenz (4.0 Deutschland Lizenzvertrag) lizenziert.

D. h., Sie dürfen:

- Teilen: das Material in jedwedem Format oder Medium vervielfältigen und weiterverbreiten
- Bearbeiten: das Material remixen, verändern und darauf aufbauen

und zwar für beliebige Zwecke, sogar kommerziell. Der Lizenzgeber kann diese Freiheiten nicht widerrufen solange Sie sich an die Lizenzbedingungen halten.

Die Nutzung ist unter den folgenden Bedingungen möglich:

- Namensnennung: Sie müssen angemessene Urheber- und Rechteangaben machen, einen Link zur Lizenz beifügen und angeben, ob Änderungen vorgenommen wurden. Diese Angaben dürfen in jeder angemessenen Art und Weise gemacht werden, allerdings nicht so, dass der Eindruck entsteht, der Lizenzgeber unterstütze gerade Sie oder Ihre Nutzung besonders.
- Weitergabe unter gleichen Bedingungen: Wenn Sie das Material remixen, verändern oder anderweitig direkt darauf aufbauen, dürfen Sie Ihre Beiträge nur unter derselben Lizenz wie das Original verbreiten.
- Keine weiteren Einschränkungen: Sie dürfen keine zusätzlichen Klauseln oder technische Verfahren einsetzen, die anderen rechtlich irgendetwas untersagen, was die Lizenz erlaubt.

Im Weiteren gilt:

- Jede der vorgenannten Bedingungen kann aufgehoben werden, sofern Sie die Einwilligung des Rechteinhabers dazu erhalten.

Diese Lizenz lässt die Urheberpersönlichkeitsrechte unberührt.

Um sich die Lizenz anzusehen, gehen Sie bitte ins Internet auf die Webseite:

https://creativecommons.org/licenses/by-sa/4.0/deed.de

bzw. für den vollständigen Lizenztext

https://creativecommons.org/licenses/by-sa/4.0/legalcode

Geschlechtergerechte Sprache

Hinweis bzgl. geschlechtsneutraler Formulierung im gesamten Text:

> Eine gleichstellungsgerechte Gesellschaft erfordert eine geschlechterneutrale Sprache. Im folgenden Text werden daher, soweit möglich und sinnvoll, entsprechende Formulierungen genutzt (z. B. Paarformeln, Ableitungen). Personenbezeichnungen, bei denen es sich um juristische Fachbegriffe handelt, die sowohl natürliche als auch juristische Personen bezeichnen können, werden im folgenden Text nicht durch Paarformeln ersetzt. Dies gilt auch für technische Fachbegriffe, Definitionen und Zitate aus Normen (z. B. DIN EN ISO) und gesetzlichen Vorschriften. Entsprechende Begriffe sind im Sinne der Gleichbehandlung geschlechtsneutral zu interpretieren.

1 Einleitung

Die Weiterentwicklung der IT-Systeme im Gesundheitswesen bedingt einen deutlichen Zuwachs in der Komplexität der eingesetzten Systeme. Aus diesem Grund sind heutzutage kein Krankenhaus und keine Arztpraxis in der Lage, diese Systeme ohne die Unterstützung durch den jeweiligen Hersteller zu betreiben. Insbesondere ist eine (regelmäßige) Wartung der Systeme durch den Hersteller unabdingbar. U.a. bedingt durch die hohe Anzahl von Systemanwendern und der vergleichsweise geringen Anzahl von Personen, die eine Wartung durchführen können, ist eine Wartung vor Ort nur selten realisierbar, die Regel ist die Fernwartung.

Dabei erfolgt der Zugriff von Fremdfirmen auf interne Systeme eines medizinischen Leistungserbringers aus unterschiedlichen Gründen. In einigen Fällen greifen Fremdfirmen auf Anwendungen zu, um die Betreuung der Nutzer bzgl. der Anwendung zu gewährleisten und diesen bei Fragen Unterstützung anzubieten. In anderen Fällen entwickeln Fremdfirmen Anwendungen, testen oder betreiben Systeme im Auftrag des verantwortlichen medizinischen Leistungserbringers. Diese unterschiedlichen Fernzugriffsmöglichkeiten können im Einzelfall eine unterschiedliche rechtliche Bewertung und unterschiedliche technische und organisatorische Schutzmaßnahmen erforderlich machen.

Da bei einer Fernwartung nicht ausgeschlossen werden kann, dass der Dienstleister auf personenbezogene Daten des Auftraggebers zugreift, kommt der Fernwartung auch eine nicht zu unterschätzende datenschutzrechtliche Relevanz zu. Gerade auch vor dem Hintergrund der gestiegenen datenschutzrechtlichen Anforderungen der EU-Datenschutzgrundverordnung (DS-GVO) müssen diese Anforderungen in der rechtlichen, technischen und organisatorischen Ausgestaltung einer Fernwartung berücksichtigt werden.

Da das Thema Fernwartung somit unterschiedliche Bereiche adressiert, ist das vorliegende Dokument wie folgt aufgebaut:

- Zunächst adressiert es die organisatorischen Anforderungen, die an eine Fernwartung gestellt werden sollten.
- Im nächsten Abschnitt werden die sicherheitstechnischen Anforderungen thematisiert.
- Danach geht der Artikel auf die datenschutzrechtlichen Implikationen ein, die mit einer Fernwartung verbunden sind.
- Da die Fernwartung auch einige Herausforderungen auf vertraglicher Ebene stellt, wird im darauffolgenden Abschnitt die vertragliche Seite thematisiert.
- Weil eine Fernwartung mit nicht unerheblichen Risiken einhergeht, finden sich im nächsten Kapitel Ausführungen zum Thema „Risikoanalyse“.
- Um den Lesern eine Handreichung hinsichtlich der Vorgehensweise zu geben, findet sich im siebten Abschnitt eine entsprechende Checkliste.
- Um den Praxisbezug herzustellen folgt zum Ende hin noch ein Beispiel, wie eine Fernwartung in der Praxis umgesetzt werden kann bzw. sollte.

Dabei stellt diese Ausarbeitung eine Praxishilfe dar, soll also bei der Abarbeitung der Thematik helfen. D.h. wenn im folgenden im Rahmen der Anforderungsdarstellung von „muss“, „sollte“ oder „könnte“ die Rede ist, handelt es sich immer noch um eine Empfehlung, wie vorzugehen ist.

2 Organisatorische Anforderungen

Grundlegend für die sichere und rechtskonforme Nutzung von Fernzugriffsmöglichkeiten ist die organisatorische Begleitung. Daher gilt es organisatorische Rahmenbedingungen zu schaffen, welche einen sicheren Betrieb/Einsatz ermöglichen. Im Unternehmen müssen Regeln etabliert werden, die transparent aufzeigen, unter welchen Bedingungen (z. B. wer darf wann aus welchen Gründen einen Fernzugriff auf welche Daten initiieren?) ein Fernzugriff zulässig ist.

2.1 Grundlegende Anforderungen

Anforderung 1) Beschränkung auf Notwendigkeit

Es werden nur die unbedingt erforderlichen Fernzugriffsmöglichkeiten implementiert.

Ratio: Fernzugriffsmöglichkeiten stellen aufgrund der Zugriffsmöglichkeiten von außerhalb des Unternehmens grundsätzlich eine potenzielle Sicherheitslücke dar. Daher muss die Möglichkeit hierzu wann immer möglich eingeschränkt werden.

Anforderung 2) Verzeichnis der Fernzugriffsmöglichkeiten

Sämtliche Fernzugriffsmöglichkeiten werden im Rahmen eines Sicherheitsmanagements erfasst. Dies beinhaltet die Art des Zugangs, die betroffenen Systeme, die berechtigten Personen sowie die zugehörigen Vorgaben und Prozesse.

Ratio: Eine Dokumentation der externen Verbindungen ist eine grundlegende Anforderung, um den Sicherheitsstatus und die Risiken für die internen Netze beurteilen zu können. Nur so kann eine Übersicht gewährleistet werden, welche legitimen externen Zugriffsmöglichkeiten existieren.

Anforderung 3) Zeitliche Beschränkung

Remote-Zugänge werden nur bei Bedarf oder in einem definierten Wartungsfenster freigegeben (z. B. Schlüsselschalter). Die Aktivierung bzw. Deaktivierung ist zu protokollieren.

Ratio: Nur wenn die Initiierung eines Fernzugriffs durch das eigene Personal erfolgt, bleibt der Auftraggeber „Herr der Lage“ und kann im Zweifelsfall auch eingreifen.

Anforderung 4) Prüfung der Funktionsfähigkeit

Es erfolgt eine regelmäßige Prüfung der Funktionsfähigkeit der Fernwartung.

Ratio: Fernzugriffsmöglichkeiten werden nur eingerichtet, wenn dafür eine Erforderlichkeit besteht. Dies bedingt jedoch, dass die Fernzugriffsmöglichkeiten insbesondere auch für zeitkritische Zugriffe im Bedarfsfall funktionieren müssen. Um dies zu gewährleisten, ist eine regelmäßige Prüfung – insbesondere nach Konfigurationsänderungen der Firewall – unabdingbar.

2.2 Arbeitsanweisungen („Standard Operating Procedure“, SOP)

Als vorbeugende Maßnahme kommt der ordnungsgemäßen Durchführung von Wartungsarbeiten eine besondere Bedeutung zu. Die rechtzeitige Einleitung von Wartungsarbeiten und die Überprüfung ihrer Durchführung sind durch eine zentrale Stelle wahrzunehmen.

Anforderung 5) Rechtzeitig und fachkundig

Wartungsarbeiten werden unter Beachtung der Hinweise des Herstellers rechtzeitig initiiert und von fachkundigem Personal durchgeführt.

Ratio: Fachkundiges Personal ist sowohl auf Seiten des Auftraggebers wie auch des Auftragnehmers erforderlich, um die Ordnungsgemäßheit und Sicherheit des Zugriffs zu gewährleisten.

Anforderung 6) Zugriffsdokumentation

Für jedes System wird dokumentiert, wann es gewartet wurde und welche Fehler dabei behoben bzw. Aufgaben erledigt wurden.

Ratio: Eine Dokumentation der externen Verbindungen ist eine grundlegende Anforderung, um den Sicherheitsstatus der internen Netze beurteilen zu können. Nur so kann eine Übersicht gewährleistet werden, wann ein legitimer externen Zugriffe erfolgte und so ggf. erfolgte illegitime Zugriffe erkannt werden.

Anforderung 7) Dokumentationsumfang

Für jede Fernwartung müssen bestimmte Aspekte dokumentiert werden. Dazu gehören mindestens:

a) Verantwortlicher („Anforderer“) beim Auftraggeber (Name, E-Mail-Adresse)
b) Kontaktinformationen des Auftragnehmers (Name des Unternehmens, Standort/Anschrift, Ansprechpartner, E- Mail-Adresse)
c) Kontaktinformationen (Name des Unternehmens, Standort/Anschrift, Ansprechpartner, E-Mail-Adresse) Fernwartungszugang
d) Für die Verbindung verwendete Zugangsplattform in der DMZ (einschl. des jeweiligen Ansprechpartners)
e) Art des Fernzugriffs (z.B. IPSec-VPN über das Internet, Einwahl, …)
f) Zielsysteme
g) Anwendungen auf dem Zielsystem
h) Für den System-/Anwendungszugang verwendete(s) Protokoll(e) (z. B. SSH, RDP, ICA, HTTPS,...)
i) Zugangshäufigkeit

Ratio: Nur wenn zu jeder Fernwartung eine ausreichende Dokumentation verfügbar ist, können im Bedarfsfall die Vereinbarungen nachgelesen bzw. auch überprüft werden.

2.3 Fernwartungsrichtlinie

In einer Fernwartungsrichtlinie wird der Prozess beschrieben, wie die Fernwartung erfolgt. Zum Inhalt gehören:

- Begriffsbestimmungen, z. B.
  - Was wird unter „Wartung“ verstanden?
  - Was ist eine Fernwartungssoftware, was eine Fernwartungssitzung?
- Eine Darstellung der geltenden rechtlichen Rahmenbedingungen, z. B.
  - Bei der Verarbeitung personenbezogener Daten geltende datenschutzrechtliche Bestimmungen
  - Strafgesetzbuch, Strafprozessordnung
  - Ggf. Berufsordnungen (Ärzte, Apotheker)
  - Ggf. BSI-KRITIS-Verordnung, IT-Sicherheitsgesetz

- Datenschutzmaßnahmen
    - Beachtung von Privacy by Design/Privacy by Default
    - Bei Einsatz von externen Dienstleistern: Fernwartungsvertrag, Auftragsverarbeitungsvertrag
    - Beschreibung der Akteure, der Mitwirkenden
    - Darstellung des Ablaufs eines Fernwartungsvorganges
        - Anforderung einer Unterstützungsleistung, welche einen Fernzugriff erfordert: wer darf wann aus welchen Gründen wen und was anfordern?
        - Datenübertragung: Übertragung von Bildschirmanzeigen unerlässlich, jedoch Regelung bzgl. Dateientransfer erforderlich
        - Überwachung / Gewährleistung des 4-Augen-Prinzips
    - Protokollierung
    - Dokumentation
- Beschreibung der technischen Umsetzung
    - Aufbau der Kommunikation
    - Kommunikationsprotokoll
    - Protokollierung
        - Verbindung zwischen Zielrechner und Protokollrechner
        - Verbindung zwischen externem Rechner und Protokollrechner
    - Übertragung von Dateien, z. B. Updates
        - Prüfung der Integrität der Dateien

3 Grundlegende Anforderungen für den sicheren IT-Betrieb

3.1 Benutzerverwaltung

Anforderung 8) Zentrale Benutzerverwaltung

Das zu wartende System muss für die Benutzerverwaltung an ein zentrales System angebunden werden.

Ratio: Ein Identitätsmanagementprozess reduziert die Risiken der Abstreitbarkeit von Handlungen, zudem wird bei Missbrauch eine Überprüfung erleichtert. Dazu muss der Identitätsmanagementprozess etabliert (i.S.v. gelebt) und nachvollziehbar dokumentiert sein. Dabei muss die Zuweisung von Identitäten auf das entsprechende Berechtigungskonzept aufbauen.

Anforderung 9) Eindeutige Benutzerkonten

Es müssen Benutzerkonten verwendet werden, welche die eindeutige Identifizierung des Benutzers ermöglichen.

Ratio: Nur wenn gewährleistet ist, dass die an einem Zugriff auf Daten beteiligten Personen sicher identifiziert werden können, können im Bedarfsfall Zugriffe auf sensible/kritische Daten nachvollzogen werden.

Anforderung 10) Beschränkung notwendiger Berechtigungen

Die Berechtigungen von Benutzerkonten und Anwendungen müssen auf ein für deren Aufgaben notwendiges Minimum reduziert werden.

Ratio: Die Berechtigungen müssen soweit eingeschränkt werden, dass ein Benutzer nur auf Daten zugreifen und Funktionen nutzen kann, die er im Rahmen seiner Arbeit benötigt. Entsprechende Berechtigungen sind auch für den Zugriff auf Dateien, die Bestandteil des Betriebssystems oder von Anwendungen sind oder von diesen erzeugt werden (z. B. Konfigurations- und Protokollierungsdateien), zu vergeben. Weiterhin muss auch die Ausführung von Anwendungen mit möglichst niedrigen Berechtigungen erfolgen. Anwendungen sollten nicht mit Administrator- oder Systemberechtigungen ausgeführt werden, wenn dies nicht zwingend erforderlich ist. Sofern für ausgewählte Tätigkeiten zusätzliche Berechtigungen (z.B. Administratorberechtigung) erforderlich sind, dürfen diese nur zeitbegrenzt durch den Auftraggeber erteilt werden.

Anforderung 11) Rollenkonzept

Der Zugang eines Nutzers der Fremdfirma muss rollenbasiert erfolgen.

Ratio: Nur ein rollenbasierter Zugriff erlaubt auch bei einer Vielzahl von Benutzerkonten den Überblick, welche Rechte vergeben wurden.

Anforderung 12) Löschen inaktiver User

Vordefinierte und nicht benötigte Benutzerkonten müssen gelöscht oder deaktiviert werden.

Ratio: Bei der Installation von Betriebssystemen werden i.d.R. vordefinierte und nicht genutzte Benutzerkonten (z. B. Gast) eingerichtet, die teilweise ohne, teilweise mit bekannten Passwörtern vorkonfiguriert sind. Diese Zugangsdaten sind allgemein bekannt und bieten potenziellen Angreifern die Möglichkeit, sich anzumelden und mit den Rechten dieser Konten zu arbeiten. Diese Standardbenutzer müssen daher entweder gelöscht oder deaktiviert werden. Sollten diese Maßnahmen nicht umsetzbar sein, muss das entsprechende Benutzerkonto für einen Fernzugriff gesperrt werden. Weiterhin müssen gesperrte und deaktivierte Benutzerkonten mit einem möglichst komplexen Passwort (12 Zeichen und mehr, Nutzung von Groß-

/Kleinbuchstaben, Zahlen und Sonderzeichen) versehen werden, so dass auch im Falle einer Fehlkonfiguration die unberechtigte Nutzung eines solchen Benutzerkontos verhindert wird.

3.2 Kennworte und Authentifizierung

Anforderung 13) Änderung Standardkennworte

Vordefinierte Authentisierungsmerkmale müssen geändert werden.

Ratio: Häufig existieren auf Systemen vom Hersteller, Entwickler oder Lieferanten vorkonfigurierte Authentisierungsmerkmale wie Passwörter und kryptographische Schlüssel. Solche Authentisierungsmerkmale müssen in eigene, Dritten nicht bekannte Merkmale geändert werden, um Angreifern den Zugang zu erschweren.

Anforderung 14) Absicherung schutzbedürftiger Daten durch Kennwort u.ä.

Die Nutzung und der Zugriff auf schutzbedürftige Funktionen und Informationen, dürfen nicht ohne erfolgreiche Authentifizierung und Autorisierung möglich sein.

Ratio: Nur eine erfolgreiche Authentifizierung und Autorisierung gewährleistet einen befugten Zugriff auf die Daten.

Anforderung 15) Abmeldefunktion

Das System muss Benutzern ermöglichen, sich von ihrer Sitzung abzumelden.

Ratio: Das Betriebssystem/die Anwendung muss über eine Funktion verfügen, die es dem angemeldeten Benutzer ermöglicht, sich jederzeit abzumelden. Die Fortführung einer abgemeldeten Sitzung darf nicht ohne erneute und erfolgreiche Authentifizierung des Benutzers möglich sein.

Anforderung 16) Zwei-Faktor-Authentifizierung

Bei besonders sensiblen Daten wie z. B. Gesundheitsdaten ist ein Zwei-Faktor-Verfahren als Authentisierungsmechanismus einzusetzen.

Ratio: Eine starke Authentifizierung erfolgt immer auf Basis mehrerer (mindestens zwei) Merkmale wie z.B. Besitz und Wissen oder auf einer einmaligen, dem Nutzer eigenen Eigenschaft. Letzteres sind in der Regel biometrische Verfahren zur Authentisierung wie z. B. die Stimmerkennung oder ein Irisscan.

Hinweis: Nicht alle biometrischen Techniken sind bereits verlässlich, zudem ergeben sich erhebliche sicherheitstechnische Anforderungen durch das notwendige Abspeichern persönlicher Merkmale, daher wird zum heutigen Zeitpunkt vom Einsatz biometrischer Verfahren abgeraten. Mögliche Methoden, die zur Authentisierung genutzt werden können, sind:

- Benutzername/Passwort (statisch)
- Einmal Passwort / Hardware Token
- Einmal Passwort / Mobiltelefon
- PKI / zertifikatsbasierte Anmeldung
- SMS Passwort
- Sicherheitsfragen
- Geo-Lokalisation
- Verhaltensbasierend
- Geräte-Identifikation
- Virtuelle Smartcards

Anforderung 17) Zwei-Faktor-Authentifizierung speziell für Admin-User

Benutzerkonten mit weitreichenden Berechtigungen müssen mit zwei Authentisierungsmerkmalen geschützt werden.

Ratio: Eine starke Authentifizierung erfolgt immer auf Basis mehrerer (mindestens zwei) Merkmale wie z. B. Besitz und Wissen oder auf einer einmaligen, dem Nutzer eigenen Eigenschaft. Letzteres sind in der Regel biometrische Verfahren zur Authentisierung wie z. B. die Stimmerkennung oder ein Irisscan.

Hinweis: Nicht alle biometrischen Techniken sind bereits verlässlich, zudem ergeben sich erhebliche sicherheitstechnische Anforderungen durch das notwendige Abspeichern persönlicher Merkmale, daher wird zum heutigen Zeitpunkt vom Einsatz biometrischer Verfahren abgeraten. Mögliche Methoden, die zur Authentisierung genutzt werden können, sind:

- Benutzername/Passwort (statisch)
- Einmal-Passwort / Hardware Token
- Einmal-Passwort / Mobiltelefon
- PKI / zertifikatsbasierte Anmeldung
- SMS-Passwort
- Sicherheitsfragen
- Geo-Lokalisation
- Verhaltensbasierend
- Geräte-Identifikation
- Virtuelle Smartcards

Anforderung 18) Paßwort – Stärke

Falls Passwörter als Authentisierungsmerkmal genutzt werden, müssen diese mindestens 8 Zeichen lang sein und folgende Zeichentypen beinhalten: Kleinbuchstaben, Großbuchstaben, Ziffern und Sonderzeichen.

Ratio: Triviale und zu kurze Passwörter sind anfällig gegen Brute-Force- und Wörterbuch-Angriffe und sind von einem Angreifer leicht zu ermitteln. Ein einmal ermitteltes Passwort kann dann von einem Angreifer für den unautorisierten Zugriff auf das System und dessen Daten genutzt werden. Passwörter mit der in der Anforderung beschriebenen Komplexität bieten eine hohe Robustheit gegen Angriffe bei gleichzeitig akzeptabler Benutzerfreundlichkeit

Anforderung 19) Paßwort – Gültigkeitsdauer

Falls Passwörter als Authentisierungsmerkmal genutzt werden, muss eine Änderung des eigenen Passwortes jederzeit durch den Benutzer möglich sein.

Ratio: Nur durch die Möglichkeit, dass ein Benutzer sein Authentisierungsmerkmal jederzeit selbsttätig ändern kann, ist eine zeitnahe Änderung möglich, wenn der Benutzer den Verdacht hat, dass dieses in den Besitz Dritter gelangt sein könnte.

Anforderung 20) Paßwort - Begrenzung Eingabeversuche

Falls Passwörter als Authentisierungsmerkmal genutzt werden, muss ein Schutz gegen Wörterbuch- und Brute-Force-Angriffe vorhanden sein, der das Erraten von Passwörtern stark erschwert.

Ratio: Ohne entsprechenden Schutz kann ein Angreifer durch bloßes Durchprobieren von Wörterbuchlisten oder automatisch erzeugten Zeichenkombinationen versuchen, ein Passwort zu ermitteln, um so das entsprechende Benutzerkonto missbräuchlich zu nutzen.

Hinweis: Um Wörterbuch- und Brute-Force Angriffe zu erschweren oder zu verhindern, können verschiedene Maßnahmen oder eine Kombination solcher Maßnahmen umgesetzt werden. Hierzu zählen insbesondere:

- Ansteigende zeitliche Verzögerung (z. B. Verdopplung der Wartezeit bei jedem Versuch) für eine erneute Eingabe eines Passwortes nach einem Fehlversuch.
- Sperren des Benutzerkontos nach einer vorgegebenen Anzahl an Fehlversuchen (typischerweise 5). Allerdings ist bei dieser Lösung zu bedenken, dass dies einen Entsperrprozess erfordert und ein Angreifer dies gezielt nutzen kann, um Konten zu sperren und somit unbrauchbar zu machen.
- Verwendung von CAPTCHA, um ein automatisiertes Ausprobieren zu erschweren.

Anforderung 21) Paßwort - gesicherte Speicherung

Falls Passwörter als Authentisierungsmerkmal genutzt werden, darf deren Darstellung nicht im Klartext erfolgen.

Ratio: Damit eine andere Person bei der Eingabe eines Passwortes dieses nicht zufällig oder absichtlich vom Bildschirm ablesen kann, muss das Passwort bei der Eingabe oder Darstellung unkenntlich gemacht werden.

Hinweis: Typischerweise werden die einzelnen Zeichen des Passwortes durch ein Zeichen wie „*“ ersetzt. Unter bestimmten Voraussetzungen kann es zulässig sein, dass ein einzelnes Zeichen bei der Eingabe kurz angezeigt wird, allerdings darf niemals das ganze Passwort im Klartext auf dem Display angezeigt werden.

Anforderung 22) Paßwort – Angriffserkennung

Es sollte ein Mechanismus zur Detektion von Angriffen auf Passwort-basierte Authentisierungsverfahren (z. B. Brute Force Angriffe) eingesetzt werden.

Ratio: Nur wenn Brute-Force Angriffe erkannt werden, kann darauf reagiert werden.

3.3 Sicherer Einsatz von Software und Diensten

Anforderung 23) Beschränkung auf notwendige Dienste und Protokolle

Nicht benötigte Dienste und Protokolle müssen deaktiviert werden.

Ratio: Sowohl bei der Installation von Betriebssystemen wie auch von Softwareanwendungen werden regelmäßig Dienste und Protokolle installiert und aktiviert, die für den Anwendungsfall nicht notwendig sind. Jeder Dienst wie auch jedes Protokoll stellt eine Sicherheitslücke dar und muss daher desinstalliert oder zumindest deaktiviert werden, wenn er nicht benötigt wird.

Anforderung 24) Beschränkung erreichbarer Dienste

Die Erreichbarkeit von Diensten muss auf die notwendige Erreichbarkeit eingeschränkt werden. D. h. die Erreichbarkeit von Diensten muss auf benötigte Schnittstellen und legitime Kommunikationspartner eingeschränkt werden.

Ratio: Dienste stehen i.d.R. auf allen Schnittstellen des Systems zur Verfügung und sind von allen Anwendungen aus allen Netzen ansprechbar, die mit dem System kommunizieren können. Dies betrifft auch Anwendungen, bei denen dies nicht erforderlich ist. Um die Möglichkeit des Missbrauchs zu verringern, muss die Erreichbarkeit auf die benötigten Anwendungen und Netze eingeschränkt werden

Anforderung 25) Beschränkung auf notwendige Software

Nicht benötigte Software darf nicht installiert oder muss deinstalliert werden.

Ratio: Sowohl bei der Installation von Betriebssystemen wie auch von Softwareanwendungen werden regelmäßig Anwendungen bzw. Software-Komponenten wie z. B. Beispieldatenbanken installiert, welche weder für den Betrieb noch für die Funktion des Systems erforderlich sind. Da auch diese Komponenten potenzielle Sicherheitsprobleme beinhalten können, dürfen diese entweder nicht mit installiert werden oder müssen nach der Installation entfernt werden.

Anforderung 26) Beschränkung auf notwendige Funktionen

Nicht benötigte Funktionen der eingesetzten Software und Hardware müssen deaktiviert werden.

Ratio: Bei einer Softwareinstallation werden i.d.R. Funktionen durch den Installationsprozess aktiviert, die für den Betrieb der Software nicht benötigt werden wie z. B. Scripting-Funktionalitäten. Diese Funktionalitäten können häufig zwar nicht deinstalliert, jedoch in den Konfigurationseinstellungen deaktiviert werden. Da grundsätzlich jede Funktionalität eine potenzielle Sicherheitslücke darstellt, muss jede nicht benötigte Funktionalität deaktiviert werden, soweit dies möglich ist. Gleiches gilt auch für Hardware-Funktionalitäten. Z. B. ist Bluetooth (im BIOS oder über eine Konfigurationsschnittstelle des Betriebssystems) abzuschalten, wenn Bluetooth seitens des Systems nicht benötigt wird.

Anforderung 27) Software/Hardware nur mit Wartung

Software- und Hardware-Komponenten, für die es keine Wartung oder Pflege durch den Lieferanten, Hersteller oder Entwickler gibt, dürfen nicht verwendet werden.

Ratio: Komponenten, die End-of-Life oder End-of-Support sind, dürfen nicht eingesetzt werden, da hier Sicherheitslücken nicht mehr beseitigt werden. Zudem sind diese Sicherheitslücken oftmals allgemein bekannt, so dass ein potenzieller Angreifer relativ leicht einen wahrscheinlich erfolgreichen Angriff starten kann.

Anforderung 28) Beseitigung von Schwachstellen

Bekannt gewordene Schwachstellen in der Software oder Hardware des Systems müssen behoben oder gegen Missbrauch abgesichert werden.

Ratio: Schwachstellen ermöglichen Angreifern Zugriff auf zu schützende Informationen. Komponenten, welche eine Schwachstelle aufweisen, dürfen daher nicht installiert oder verwendet werden. Eine Ausnahme hiervon sind Komponenten, für die bereits eine Maßnahme zum Beheben der Schwachstelle, wie z. B. ein Patch, ein Update oder ein Workaround, existiert, sofern diese Maßnahme auf dem System umgesetzt wurde.

4 Sicherheitstechnische Anforderungen an eine Fernwartung

4.1 Organisatorische Anforderungen

Anforderung 29) Testumgebung wenn möglich

Die Fernwartung erfolgt wenn möglich in Testumgebungen; der Zugriff auf das Produktivsystem sollte nur gewählt werden, wenn ein Wartungsziel anders nicht erreicht werden kann.

Ratio: Ein Zugriff auf ein Produktivsystem beinhaltet immer auch das Risiko der Beeinträchtigung– ob gewollt oder ungewollt – des Produktivsystems. Daher sollte, wann immer möglich, ein Zugriff auf das Produktivsystem vermieden und stattdessen mit Testumgebungen gearbeitet werden.

Anforderung 30) Freischaltung auf Anforderung

Die Fernwartung durch Fremdfirmen soll nur erfolgen, wenn

- Beschäftigte des Arbeitgebers explizit diesen Fernwartungsvorgang beauftragen und
- die Zugangsmöglichkeit der Fremdfirma in das Netz des Arbeitgebers explizit für den beauftragten Fernwartungsvorgang freigeschaltet wurde.

Ratio: Nur wenn die Fernwartung durch den Auftraggeber initiiert werden muss, ist gewährleistet, dass kein Fernzugriff ohne Kenntnis des Auftraggebers erfolgt. Nur wenn der Auftraggeber Kenntnis von der Fernwartung hat, kann er diese überwachen und bei Zugriff auf sensible/kritische Daten ggf. in die Fernwartung eingreifen oder diese auch abbrechen.

Anforderung 31) Zeitliche Beschränkung

Der Zugang zu Produktionssystemen darf nur vorübergehend möglich sein und muss auf einem individuellen Vorfall/Unterstützungsfall basieren.

Ratio: Wird der Zugriff nicht eingeschränkt, ist per Fernwartung jederzeit ein Zugriff möglich. D. h. auch ein unüberwachter Zugriff. Ist letzteres der Fall, existiert keine Kontrolle, auf welche Daten zugegriffen wird. Daher müsste in diesem Fall davon ausgegangen werden, dass ein unautorisierter Zugriff auf personenbezogene Daten erfolgte, d. h. eine unbefugte Offenlegung/Offenbarung. Da auf Produktivsystemen i.d.R. Daten einer Vielzahl von Personen gespeichert werden, müsste von einem massenhaften, unerlaubten, unkontrolliertem Zugriff ausgegangen werden und gem. Art. 33 DS-GVO die Datenschutzaufsichtsbehörde bzgl. des Vorfalls informiert werden.

Anforderung 32) Autologoff

Wird für einen definierten Zeitraum keine Interaktion über eine Schnittstelle festgestellt, muss sich die Session automatisch schließen.

Ratio: Inaktive Sessions unterliegen dem Risiko, missbraucht zu werden, daher müssen diese beendet werden. Der Wert bzw. die Zeit, wann eine Session terminiert werden soll, muss ggf. individuell für jede Anwendung festgelegt werden, ein typischer Timeout-Zeitraum für eine Session beträgt weniger als eine Stunde.

Anforderung 33) Schattenterminal

Die Sitzung eines externen Dienstleisters muss jederzeit von einem Mitarbeiter des Auftraggebers beendet werden können.

Ratio: Die Kontrolle der Fernwartungssitzung muss stets beim Auftraggeber liegen, nur er kann entscheiden, ob irgendein Geschäftsprozess (z. B. die Patientenversorgung) eine Beendigung der

Fernwartungssitzung zwingend erforderlich macht oder ob der Fernwartende auf Daten zugreift, die bspw. aufgrund der ärztlichen Verschwiegenheitspflicht nicht offenbart werden dürfen.

4.2 Anforderung an Dienstleister

Anforderung 34) Zuverlässigkeit Dienstleister

Entscheidendes Kriterium bei der Auswahl des Fernwartungsdienstleisters muss dessen Zuverlässigkeit sein.

Ratio: Nur bei Fernwartungsdienstleistern, bei denen eine hinreichende Zuverlässigkeit[1] nachgewiesen ist, kann davon ausgegangen werden, dass sie die vereinbarten Rahmenbedingungen zur Gewährleistung eines sicheren Fernzugriffs auch in der Praxis einhalten (können).

Anforderung 35) Dienstleister benötigt Identity Management

Die Fremdfirma muss über einen technischen und organisatorischen Identitätsmanagementprozess verfügen, mit dem die Identitäten der Nutzer mit Zugang zu Systemen verwaltet werden.

Ratio: Nur wenn gewährleistet ist, dass die einen Fernzugriff durchführende Person sicher identifiziert werden kann, können im Bedarfsfall Zugriffe auf sensible/kritische Daten nachvollzogen werden.

4.3 Technische Anforderungen

Anforderung 36) Isolation im Netz

Das Fernwartungsobjekt sollte – zumindest während einer Fernwartungssession – so weit wie möglich vom Rest des Netzes isoliert werden, um gewollte oder ungewollte Zugriffe des Fernwartenden auf andere Rechner und Server zu verhindern. Hierzu sollte in jedem Falle mindestens eine Trennung durch Paketfilter eingesetzt werden, sodass der Fernwartungsdienstleister keinerlei Zugriff auf Rechner außerhalb der Fernwartungszone erhält.

Ratio: Die Zugriffsmöglichkeiten müssen soweit wie möglich eingeschränkt werden, damit ein – gewollter oder ungewollter – Zugriff auf Objekte, auf die während der Fernwartung kein Zugriff erfolgen muss, nicht erfolgen kann.

Anforderung 37) Keine Direktverbindung

Es darf keine direkte Verbindung zwischen einer Fremdfirma und einem Zielsystem beziehungsweise umgekehrt geben, d. h. alle Verbindungen müssen in einer DMZ terminiert werden.

Ratio: Nur bei einem Zugriff über eine DMZ kann das für sensible/kritische Daten benötigte Schutzniveau erreicht werden.

Anforderung 38) Firewall

Die Zugangsplattform in der DMZ muss mit zustandsorientierten (stateful) Firewall-Gateways geschützt werden.

---

[1] Zuverlässigkeit ist ein unbestimmter Rechtsbegriff, welcher als rechtserhebliches Kriterium bestimmte Eigenschaften einer natürlichen oder juristischen Person verlangt. Aus rechtlicher Sicht kann als zuverlässig jene Personen gelten, welche gewährleisten, dass sie die ihnen obliegenden gesetzlichen und vertraglichen Pflichten jederzeit sorgfältig beachten und in vollem Umfang erfüllen.
Ein Nachweis bzgl. Zuverlässigkeit kann z. B. dadurch erbracht werden, dass ein Dienstleister von anderen Kunden als „zuverlässig“ bewertet wird, d.h. das der Dienstleister bei anderen Kunden die gesetzlichen und vertraglichen Pflichten jederzeit sorgfältig beachtet und in vollem Umfang erfüllt.

Ratio: Eine zustandsorientierte (stateful) Firewall entspricht dem Stand der Technik und ist daher das Mittel der Wahl zum Schutz dieser Netzschicht.

Anforderung 39) Security-Monitoring

Auf der Zugangsplattform in der DMZ müssen geeignete Security-Monitoring Maßnahmen implementiert werden.

Ratio: Nur wenn ein entsprechendes Monitoring erfolgt, können Vorgänge analysiert und unzulässiges Verhalten festgestellt werden.

Anforderung 40) Schutz vor Überlast

Die Zugangsplattform in der DMZ muss sich gegen Überlastsituationen schützen. Falls eine Überlastsituation nicht verhindert werden kann, muss sich das System dennoch berechenbar verhalten.

Ratio: Überlastsituationen führen häufig zu einem unberechenbaren Verhalten des Systems, in welchem unter Umständen sogar externer Code zur Ausführung gebracht werden kann.

Anforderung 41) Abfangen von Eingabefehlern

Die Zugangsplattform in der DMZ muss robust gegen unerwartete Eingaben sein.

Ratio: Unerwartete Eingaben können zu unerwartetem Verhalten der Anwendung führen, ggf. auch Überlastsituationen verursachen.

Anforderung 42) DMZ-Trennung

Die Netztrennung der Zugangsplattform in der DMZ und angrenzender Dienste muss sich an deren spezifischen Funktionselementen ausrichten.

Ratio: Nur unter Berücksichtigung der benötigten Funktionen kann in einer DMZ der Zugriff so eingerichtet werden, dass das für sensible/kritische Daten benötigte Schutzniveau erreicht wird.

Anforderung 43) Abgestufte Netzwerkzugriffe

Der Fernwartungszugriff sollte möglichst nicht pauschal pro (Sub)Netz erfolgen, sondern vielmehr feingranular pro IP und Port geregelt werden.

Ratio: Eine pauschale (Netz-)Öffnung erlaubt zugleich eine vielfältige Nutzung der Zugriffsmöglichkeit, auch außerhalb der geregelten Fernzugriffsmöglichkeit. Daher muss der Fernwartungszugriff auf benötigte Adressen und Ports beschränkt werden.

Anforderung 44) Malwarescanner

Jeder über die Zugangsplattform in der DMZ abgewickelte Dateiaustausch muss mit einem Malware-Scanner überprüft werden.

Ratio: Grundsätzlich kann jede Datei Malware enthalten und muss daher daraufhin überprüft werden.

Anforderung 45) Application-Layer-Proxy

Verbindungen mit Kommandozeilenprotokollen müssen mit einem Application-Layer-Proxy geschützt werden.

Ratio: Ein Application-Layer-Proxy schützt eine Verbindung bzw. das hierbei genutzte Protokoll im Rahmen eines Kommandozeilenzugriffs, denn nur so kann die Kontrolle der Sitzung erhalten und die Sicherheitskonformität gewahrt bleiben.

4.4 Sichere Kommunikation und Verschlüsselung

Anforderung 46) Sichere Zugänge

Sitzungen müssen gegen eine unautorisierte Übernahme geschützt werden.

Ratio: Für jede Sitzung (auch Session genannt) muss eine Funktion implementiert sein, die verhindert, dass Sitzungen eines legitimen Benutzers von einem anderen Benutzer übernommen und/oder weitergeführt werden können. Ansonsten können Sitzungen u.U. von einem Angreifer weitergeführt werden und ggf. genutzt werden, um unberechtigten Zugriff auf ein System und damit auf die zu schützenden Daten zu erhalten. Ein entsprechender Schutz kann u.a. durch Nutzung der folgenden Maßnahmen implementiert werden:

- Verwendung des TCP-Protokolls (mit Sequence Number) und entsprechenden Filterlisten
- Nutzung kryptografischer Verfahren, z. B. auf Transportebene: SSL/TLS
- Aushandeln eines zufälligen und geheimen Wertes zwischen Sender und Empfänger (z. B. Session-ID, Zeitstempel)

Anforderung 47) Sichere Protokolle

Für die Kommunikation dürfen nur sichere Protokolle verwendet werden.

Ratio: Um vor unberechtigter Einsichtnahme oder einem Abgriff von Daten zu schützen, müssen zur Übertragung hinreichend sichere Protokolle wie z. B. SSL/TLS-Envelopes oder SFTP genutzt werden.

Anforderung 48) Absicherung schutzbedürftiger Daten

Schutzbedürftige Daten müssen bei der Übertragung sowie Speicherung gegen unberechtigte Einsichtnahme und Veränderung geschützt werden.

Ratio: Daten, welche nicht gegen eine unautorisierte Einsichtnahme und Veränderung geschützt werden, kann ein potenzieller Angreifer bei der Übertragung über eine Netzwerkverbindung mitlesen oder manipulieren. Daher müssen die Daten angemessen geschützt werden, auch bei temporärer Speicherung (temporärer Ordner, Web-Cache, usw.). Dementsprechend dürfen auch keine Übertragungsprotokolle genutzt werden, bei welchen die Übertragung unverschlüsselt (z. B. FTP oder Telnet) oder unzureichend verschlüsselt (z. B. SSLv3 oder SSHv1) werden

Anforderung 49) Sichere Verschlüsselung

Es werden hinreichend starke kryptografische Verfahren zur Verschlüsselung verwendet, die mindestens dem Stand der Technik entsprechen.

Ratio: Der Einsatz kryptografischer Verfahren gewährleistet einen Schutz gegen unautorisierte Einsichtnahme und Veränderung, aber nur, wenn die Verfahren dem Stand der Technik entsprechen.

Hinweis: Informationen zur Sicherheit von kryptografischen Verfahren finden sich insbesondere

- BSI: Technische Richtlinie 02102: Kryptographische Verfahren: Empfehlungen und Schlüssellängen. [Online, zitiert am 2017-11-15]; Verfügbar unter https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien /tr02102/index_htm.html
- Erzeugung von Signaturschlüsseln, Hashen zu signierender Daten oder Erzeugung/Prüfung elektronischer Signaturen: Bundesnetzagentur - Auflistung geeigneter Algorithmen und Parameter. [Online, zitiert am 2017-11-15]; Verfügbar unter https://www.bundesnetzagentur.de/DE/Service-Funktionen/Elektronische Vertrauensdienste/QES/WelcheAufgabenhatdieBundesnetzagentur/GeeigneteAlgorithmenfestlegen/geeignetealgorithmenfestlegen_node.html

Anforderung 50) Private Schlüssel

Private Schlüssel müssen sich ausschließlich in der Verfügungsgewalt des jeweiligen Kommunikationspartners befinden, ebenso müssen alle für die Verbindung genutzten Zertifikate fälschungssicher und überprüfbar sein.

Ratio: Liegt die Schlüsselgewalt sowie die Kontrollmöglichkeit nicht in der Hand der Kommunikationspartner, sind Man-in-the-middle-Attacken realisierbar.

4.5 Protokollierung

Anforderung 51) Aufzeichnung von Fernwartungssitzungen

Die Fernwartungssitzung muss vom Auftragnehmer vollständig aufgezeichnet werden. Der Auftraggeber erhält auf Anfrage eine Kopie dieser Aufzeichnung.

Ratio: Für Sessions im Rahmen der Unterstützung/Wartung ist grundsätzlich ein Zugriff auf kritische und/oder sensible Daten nicht auszuschließen und ein detaillierter Audit-Trail, anhand dessen man die Vorgänge im Rahmen der Fernwartung nachvollziehen kann, ist daher zwingend erforderlich. Aufzeichnung bedeutet in diesem Sinne die Erfassung des visuellen Inhalts und/oder Textinhalts einer Unterstützungssession, einschließlich aller Metadaten und übertragenen Dateien (binäre Erfassung). Die Aufzeichnung besteht in der Regel in einem Film, welcher die Session mit allen Interaktionen in Echtzeit zeigt, sowie Kopien der übertragenen Dateien.

Anforderung 52) Protokollierung von Zugangsversuchen

Jeder erfolgreiche/fehlgeschlagene Versuch des Zugangs muss vom System protokolliert werden.

Ratio: Sollte es zu Sicherheitsvorfällen kommen, liefern die Protokolldaten wichtige Informationen zur Aufklärung des Vorfalles.

Hinweis: Für korrekte Datums- und Zeitinformationen müssen alle protokollierenden Systeme an einen Dienst zur Zeitsynchronisation angebunden sein.

Anforderung 53) Protokollierung – Detailanforderung

Für erfolgreiche Versuche des Zugangs muss das Sitzungs-Protokoll definierte Parameter enthalten wie:

a) Zeitzone, Datum und Uhrzeit des Sitzungs-Beginns sowie des Sitzungs-Endes
b) Name und IP-Adresse der zugreifenden Quelle
c) Account-Name (Nutzer) bzw. ID der Schnittstelle
d) Name und IP-Adresse des Zielobjekts (Zielsystem/Anwendung)
e) Name und TCP-Port des Zielservice
f) Aktion (Sitzung hergestellt/beendet, Sitzungsanfrage zurückgewiesen)

Ratio: Sollte es zu Sicherheitsvorfällen kommen, liefern die Protokolldaten wichtige Informationen zur Aufklärung des Vorfalles.

Hinweis: Für korrekte Datums- und Zeitinformationen müssen alle protokollierenden Systeme an einen Dienst zur Zeitsynchronisation angebunden sein.

Anforderung 54) Zeitstempel

Sicherheitsrelevante Ereignisse müssen abhängig vom Verwendungszweck des Systems mit genauem Zeitstempel und einer eindeutigen Systembezeichnung protokolliert werden.

Ratio: Die Protokollierung sicherheitsrelevanter Ereignisse ist eine Grundvoraussetzung, um laufende Angriffe erkennen oder auch bereits stattgefundene Angriffe analysieren zu können. Nur aus einer erfolgten Protokollierung sind sinnvolle Maßnahmen zur Erhaltung oder auch

Wiederherstellung der Systemsicherheit abzuleiten und durchzuführen. Weiterhin können diese Daten der Beweissicherung dienen, um rechtlich gegen Angreifer vorgehen zu können bzw. sich vor Gericht zu exkulpieren. Daher müssen Systeme sicherheitsrelevante Ereignisse protokollieren.

Hinweis: Typische Ereignisse sowie zu protokollierende Daten sind in der nachfolgenden Tabelle exemplarisch dargestellt:

Ereignis	Zu protokollierende Daten
Zugriff auf Auditprotokoll	– Benutzerkonto, von dem aus zugegriffen wurde – Zugriffszeitpunkt – Dauer des Zugriffs – Quelle (IP-Adresse) – Ziel (IP-Adresse)
Export > 1 Dokument zu einem Patienten	– Benutzerkonto – Zugriffszeitpunkt – Patienten-ID – Anzahl Dokumente – Begründung für Export – Quelle (IP-Adresse) – Ziel (IP-Adresse)
Druck > 1 Dokument zu einem Patienten	– Benutzerkonto – Zugriffszeitpunkt – Patienten-ID – Anzahl Dokumente – Begründung für Ausdruck – Quelle (IP-Adresse) – Ziel (IP-Adresse)
Löschen von Dokumenten	– Benutzerkonto – Zugriffszeitpunkt – Patienten-ID – Anzahl Dokumente – Begründung für Löschung – Quelle (IP-Adresse) – Ziel (IP-Adresse)
Fehlerhafte Anmeldeversuche	– Benutzerkonto – Zugriffszeitpunkt – Anzahl der Fehlversuche – Quelle (IP-Adresse) – Ziel (IP-Adresse)
Mehr als eine Anmeldung des Benutzers	– Benutzerkonto – Zugriffszeitpunkt – Anzahl der Anmeldungen – Quelle (IP-Adresse) – Ziel (IP-Adresse)
Anmeldung außerhalb Dienstzeit	– Benutzerkonto – Zugriffszeitpunkt – Anzahl der Anmeldungen – Quelle (IP-Adresse) – Ziel (IP-Adresse)

Ereignis	Zu protokollierende Daten
Änderung von Systemrichtlinien	– Benutzerkonto – Zugriffszeitpunkt – Änderungen – Begründung – Quelle (IP-Adresse) – Ziel (IP-Adresse)
Veränderung am Regelwerk zur Protokollierung	– Benutzerkonto – Zugriffszeitpunkt – Änderungen – Begründung – Quelle (IP-Adresse) – Ziel (IP-Adresse)
Notfallanmeldung	– Benutzerkonto – Zugriffszeitpunkt – Dauer des Zugriffs – IDs der Patienten, auf die zugegriffen wurde – Quelle (IP-Adresse) – Ziel (IP-Adresse)
Erweiterung der Benutzerberechtigung zu administrativen Rechten	– Benutzerkonto – Zugriffszeitpunkt – Geändertes Benutzerkonto – Quelle (IP-Adresse) – Ziel (IP-Adresse)
Systemzugriff von Benutzerkonten mit Administrationsrechten	– Benutzerkonto – Zugriffszeitpunkt – Dauer des Zugriffs – Quelle (IP-Adresse) – Ziel (IP-Adresse)
Administration von Konten	– Benutzerkonto des Administrators – Zugriffszeitpunkt – Durchgeführte Tätigkeit (Einrichten, Löschen, Aktivieren und Deaktivieren) – Quelle (IP-Adresse) – Ziel (IP-Adresse)
Änderung von Gruppenzugehörigkeiten von Konten	– Benutzerkonto des Administrators – Zugriffszeitpunkt – Durchgeführte Tätigkeit (hinzugefügte oder entfernte – Gruppe) – Quelle (IP-Adresse) – Ziel (IP-Adresse)
Kritischer Anstieg von Systemwerten wie Speicherauslastung, CPU-Auslastung über einen längeren Zeitraum	– Zeitpunkt des Beginns – Dauer – Überschrittener Schwellwert – Erreichter Wert

Bei der Protokollierung müssen die jeweils geltenden gesetzlichen, tariflichen und betrieblichen Bestimmungen beachtet werden.

Anforderung 55) Protokollarchiv

Sitzungs-Protokolle und Sitzungs-Aufzeichnungen müssen vom Auftragnehmer in einem separaten Protokollarchiv gespeichert werden.

Ratio: Nur Protokolle, deren Authentizität gewährleistet ist, bieten die notwendige Sicherheit, dass die festgehaltenen Ereignisse auch so geschehen sind. Eine wichtige Anforderung, um dies zu gewährleisten, ist eine separate Speicherung, so dass der Zugriff auf die Daten entsprechend begrenzt werden kann.

Hinweis: Die Übertragung der Protokolle/Aufzeichnungen zum Protokollserver muss auf sichere Weise erfolgen (z. B. über sftp). Das Zeitintervall zwischen den Protokollübertragungen muss so kurz wie möglich sein.

Anforderung 56) Protokollarchiv fälschungssicher

Sitzungs-Protokolle und -Aufzeichnungen müssen manipulations-/fälschungssicher aufbewahrt werden.

Ratio: Nur Protokolle, deren Authentizität gewährleistet ist, bieten die notwendige Sicherheit, dass die festgehaltenen Ereignisse auch so geschehen sind.

Hinweis: Eine Möglichkeit dies zu gewährleisten ist, die Sitzungs-Protokolle und -Aufzeichnungen mit einer digitalen Signatur zu versehen.

Anforderung 57) Zugriffsdokumentation Detailgrad

Für jede Fernwartungs-Verbindung durch externe Firmen/Beschäftigte werden in einem Verzeichnis definierte Details registriert.

Ratio: Eine Dokumentation der externen Verbindungen ist einerseits eine grundlegende Anforderung, um den Sicherheitsstatus der internen Netze beurteilen zu können. Andererseits muss der Zugriff auf sensible Daten ggf. Auditoren gegenüber nachgewiesen werden.

Hinweis: Folgende Details müssen registriert werden:

- Verantwortlicher Anforderer der Verbindung auf der Seite des Auftraggebers (Name, E-Mail-Adresse)
- Kontaktinformationen beim Auftragnehmer (Name des Unternehmens, Standort/Anschrift, Ansprechpartner, E- Mail-Adresse)
- Zweck- und Aufgabenbeschreibung sowie eine Begründung für den Zugang
- Für die Verbindung verwendete Zugangsplattform (einschl. des jeweiligen Plattform-Anwendungsmanagers und/oder Service-Provider-Ansprechpartners)
- Priorisierter (erster) Medienzugang (z. B. IPSec-VPN über das Internet, Einwahl,...)
- Zielsysteme und -anwendungen
- Für den System-/Anwendungszugang verwendete(s) Protokoll(e) (z. B. SSH, RDP, ICA, HTTPS,...)
- Zugangshäufigkeit

Anforderung 58) Absicherung schutzbedürftiger Informationen

Schutzbedürftige Informationen dürfen nicht in Dateien, Ausgaben und Meldungen enthalten sein, die unautorisierten Benutzern zugänglich sind.

Ratio: Protokolle liegen oft an allgemein bekannten Speicherorten und liegen unverschlüsselt vor, so dass ein Zugriff auf diese Daten leichter fällt. Stehen schutzbedürftige Daten in Protokolldateien, können diese Informationen von einem potenziellen Angreifer genutzt werden, um gezielte Angriffe auf ein System vorzubereiten und durchzuführen. Neben personenbezogenen Daten gehören zu den schützenswerten Daten insbesondere auch

Informationen über das genutzte Betriebssystem, verwendete Middleware oder Anwendungen, wie z. B. Hersteller, Produktnamen, Produkt-Identifier, installierte Software-Versionen, installierte Service-Packs, Patches, Hotfixes oder Seriennummern. Diese Daten dürfen nur autorisierten Benutzern zugänglich sein.

5 Datenschutzrechtliche Anforderungen

5.1 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DS-GVO)

Grundsätzlich gilt, dass Verarbeitungen personenbezogener Daten die Anforderungen von „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“ (Art. 25 DS-GVO) genügen müssen. Daher gilt diese Anforderung auch für die Fernwartung. (Siehe hierzu die Ausarbeitung der GMDS[2].)

Anforderung 59) Wird bei der Fernwartung darauf geachtet, dass die Technikgestaltung so datenschutzfreundlich wie möglich erfolgt? („privacy by design“)

Ratio: Die Datenschutzgrundverordnung fordert, dass „sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen“ die Datenschutzgrundsätze (Art. 5 DS-GVO)

- Rechtmäßige Verarbeitung
- Verarbeitung nach Treu und Glauben
- Transparente Verarbeitung für die betroffenen Personen
- Beachtung der Zweckbindung
- Datenminimierung
- Gewährleistung der Richtigkeit der Daten
- Begrenzung der Speicherdauer
- Sicherstellung von Integrität und Vertraulichkeit
- Erfüllung der Rechenschaftspflicht bzgl. der Umsetzung der Anforderungen der Datenschutz-Grundverordnung

gewährleistet werden.

Anforderung 60) Wird bei der Fernwartung darauf geachtet, dass datenschutzfreundliche Voreinstellungen vorhanden sind? („privacy by default“)

Ratio: Die Datenschutz-Grundverordnung verlangt, dass geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass „durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich sind, verarbeitet werden“. Dementsprechend müssen die Prozesse bei der Fernwartung auf eine minimale Verarbeitung personenbezogener Daten ausgerichtet sein und insbesondere auch die Voreinstellungen in der Fernwartungssoftware dahingehend angewendet werden.

5.2 Datenschutz-Folgenabschätzung (Art. 35 DS-GVO)

Können besondere Kategorien von Daten im Rahmen der Fernwartung verarbeitet werden, so ist ggf. eine Datenschutz-Folgenabschätzung für die Fernwartung erforderlich. Siehe hierzu die Ausarbeitung der GMDS[3].

[2] Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DS-GVO). [Online, zitiert am 2018-04-28]; Verfügbar unter http://ds-gvo.gesundheitsdatenschutz.org/html/privacy_design_default.php

[3] Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO. Gemeinsame Ausarbeitung von bvitg e.V., GMDS e.V. und DKG e.V. [Online, zitiert am 2018-04-28]; Verfügbar unter http://ds-gvo.gesundheitsdatenschutz.org/html/dsfa.php

Anforderung 61) Wurde beurteilt, ob eine Datenschutz-Folgenabschätzung erforderlich ist? Wenn diese erforderlich ist: Wurde die Datenschutz-Folgenabschätzung vor Beginn der Verarbeitung durchgeführt und erfolgte eine entsprechende Dokumentation?

Ratio: Art. 35 schreibt vor, dass der „Verantwortliche“ falls erforderlich eine Datenschutz-Folgenabschätzung durchführen muss. Dies bedingt, dass bei jeder Verarbeitung personenbezogener Daten eine Beurteilung erfolgen muss, ob eine Datenschutz-Folgenabschätzung erforderlich ist. Die Entscheidung wie auch die Begründung, die in einer Form erfolgen muss, die externen Dritten die Möglichkeit des Nachvollziehens der Entscheidung erlaubt, ist zu dokumentieren und der Aufsichtsbehörde auf deren Nachfrage vorzulegen. Bei der Fernwartung bietet es sich an, diese Klärung im Laufe des Beschaffungsprozesses oder bei Vertragsabschluss durchzuführen.

5.3 Sicherheit der Verarbeitung (Art. 32 DS-GVO)

Art. 32 DS-GVO verlangt, dass ein angemessenes Schutzniveau bei der Verarbeitung personenbezogener Daten gewährleistet sein muss[4]. Bei der Auswahl der Maßnahmen sind

- der Stand der Technik,
- die Implementierungskosten,
- Art, Umfang, Umstände und Zwecke der Verarbeitung sowie
- die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die persönlichen Rechte und Freiheiten betroffener Personen

zu berücksichtigen. Zur Gewährleistung des Schutzniveaus sind entsprechend den Vorgaben der DS-GVO geeignete technische und organisatorische Maßnahmen zu ergreifen. Zu diesen Maßnahmen zählen u.a.

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten auf Dauer sicherzustellen;
- die Fähigkeit, die Verfügbarkeit der Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Da diese Punkte explizit von der DS-GVO als ggf. zu ergreifende Maßnahmen genannt werden, ist immer eine von externen Gutachtern, wie z.B. der Datenschutz-Aufsichtsbehörde, nachvollziehbare Begründung erforderlich, wenn auf eine der Maßnahmen wie z.B. Pseudonymisierung oder Verschlüsselung verzichtet wird.

Vertraulichkeit, Integrität und Verfügbarkeit sind aus dem Umfeld der IT-Sicherheit bekannte Schutzziele, Belastbarkeit erscheint auf den ersten Blick hingegen eine neue Anforderung zu sein. Im englischen Text findet sich hierzu der Begriff „resilience“, der in der entsprechenden Fachliteratur jedoch nicht mit „Belastbarkeit“, sondern mit „Widerstandsfähigkeit“ oder „Ausfallsicherheit“

[4] Siehe hierzu auch: GMDS AG "Datenschutz und IT-Sicherheit im Gesundheitswesen" (DIG): Sicherheit personenbezogener Daten: Umgang mit Art. 32 DS-GVO. [Online, zitiert am 2018-02-13]; Verfügbar unter http://ds-gvo.gesundheitsdatenschutz.org/html/sicherheit_verarbeitung.php

übersetzt wird[5]; und diese Begrifflichkeiten sind aus dem Bereich der IT-Sicherheit ebenfalls wohlbekannt.

Anforderung 62) Pseudonymisierung und Verschlüsselung müssen zum Schutz personenbezogener Daten eingesetzt werden. Sollte dies nicht erfolgen, muss diese Entscheidung begründet werden.

Ratio: Art. 32 DS-GVO schreibt als Schutzmaßnahmen insbesondere Pseudonymisierung und Verschlüsselung vor. Daher sind diese Maßnahmen grundsätzlich umzusetzen, außer dies ist zur Erreichung des Zweckes nicht möglich. In diesem Fall muss eine Begründung erfolgen.

Anforderung 63) Es muss ein System eingesetzt werden, welches die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten auf Dauer sicherstellt.

Ratio: Art. 32 DS-GVO schreibt dies für jede Verarbeitung, somit auch für eine Fernwartung vor.

Anforderung 64) Es muss ein Mechanismus implementiert sein, welcher die Verfügbarkeit der Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherstellt.

Ratio: Art. 32 DS-GVO schreibt dies für jede Verarbeitung, somit auch für eine Fernwartung vor.

Anforderung 65) Es muss ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung vorhanden sein.

Ratio: Art. 32 DS-GVO schreibt dies für jede Verarbeitung, somit insbesondere auch für eine Fernwartung vor.

[5] Siehe z. B.: Wagner SM, Bode C. Empirische Untersuchung von SC-Risiken und SC-Risikomanagement in Deutschland. In: Vahrenkamp/Siepermann (Hrsg.) Risikomanagement in Supply Chains: Gefahren abwehren, Chancen nutzen, Erfolg generieren. Erich Schmidt Verlag. 2007 ISBN 978-3503100415

6 Regelungen zum Schutz der eigenen Mitarbeiter (Beschäftigten) bei innerbetrieblichen Fernwartungen

6.1 Einleitung

Der Begriff der Fernwartung impliziert nicht zwangsläufig, dass diese nur durch externe Auftragnehmer (Dienstleister) wahrgenommen wird. Vielmehr kommt es durchaus häufig vor, dass eine „Fernwartung“ innerhalb einer Organisation durch eigene Beschäftigte z. B. der IT-Abteilung wahrgenommen wird. Auch wenn eine solche „Fernwartung“ intern erfolgt, gilt es immer zu beachten, dass es sich bei ihr um eine bzw. mehrere Datenverarbeitungen handelt, die dem Rechtmäßigkeitsgrundsatz folgend, stets einer gesetzlichen Legitimation bedürfen. Gerade weil bei einer „internen“ Fernwartung Mitarbeiter der Organisation, im Namen des Arbeitgebers auf Daten anderer Beschäftigter Zugriff nehmen können, die das Verhältnis Arbeitgeber – Arbeitnehmer betreffen, sollten gerade bei internen Fernwartungen die speziellen Regelungen des Beschäftigtendatenschutzes und des Arbeitsrechts zwingend beachtet werden. In diesem Zusammenhang erlangen insbesondere die Regelungen von Artt. 6 Abs. 2, 88 DS-GVO i. V. m. § 26 BDSG-neu eine besondere Relevanz.

Die für die Fernwartung eingesetzten Remote-Control-Systeme bieten neben der Fernwartungsmöglichkeit noch weitere Möglichkeiten wie z. B. das Übertragen und Löschen von Dateien und Daten, die Inventarisierung von Hard- und Software, das Diagnostizieren von Hardwarefehlern und die zentrale Verteilung neuer Software oder neuer Softwareversionen (Updates). Weil man theoretisch durch diese Software-Funktionen auch in der Lage ist Mitarbeiter zu überwachen, sollten beim Einsatz von interner Fernwartung immer auch die Mitbestimmungsrechte der Personalvertretungen wie Betriebs- oder Personalrat mit berücksichtigt werden. Durch die mannigfaltigen Möglichkeiten dieser Softwaresysteme lassen sich diese durchaus als sog. „technische Kontrolleinrichtungen“ bewerten, die gemäß § 87 Abs. 1 Nr. 6 BetrVG bzw. § 75 Abs. 3 Nr. 17 BPersVG mitbestimmungspflichtig sind[6]. Entsprechend § 80 Abs. 2 BetrVG und § 68 Abs. 2 BPersVG muss der Arbeitgeber die Belegschaftsvertretung über die konkrete Ausgestaltung der Fernwartung und über die Funktionen der entsprechenden Software rechtzeitig und umfassend informieren. Hierbei bietet sich an, dass beide Parteien eine entsprechende Vereinbarung in Form einer „Betriebsvereinbarung“ abschließen.

6.2 Betriebsvereinbarung

Eine Betriebsvereinbarung stellt die innerbetriebliche Möglichkeit dar, in einer Art Vertrag zwischen Arbeitgeber und Personalvertretung (Betriebsrat oder Personalrat) verbindliche Regelungen aufzustellen, die innerhalb der jeweiligen Organisation, im Verhältnis zwischen Arbeitgeber und Arbeitnehmer Anwendung finden.

Aus datenschutzrechtlicher Sicht können Betriebsvereinbarungen, die mit den Grundprinzipien der Datenverarbeitung (vgl. Art. 5 DS-GVO) in Einklang stehen und auch sonst nicht gegen geltendes Recht verstoßen, legitimierende Wirkung für die entsprechende betriebliche Datenverarbeitung haben (vgl. Art. 88 und § 26 BDSG-Neu). Gerade auch um etwaige Fernwartungstätigkeiten von

[6] Auch eine Betriebsvereinbarung kann eine dauerhafte Verarbeitung „einzelner Arbeitsschritte und damit des wesentlichen Arbeitsverhaltens der Arbeitnehmer anhand quantitativer Kriterien während ihrer gesamten Arbeitszeit“ legitimieren, siehe z.B. BAG Urt. v. 25.04.2017 1 (AZ: ABR 46/15), [Online, zitiert am 2017-12-08]; Verfügbar unter https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=BAG&Datum=25.04.2017&Aktenzeichen=1%20ABR%2046%2F15

Mitarbeitern, die dem Arbeitgeber einer Organisation im Hinblick auf die Datenverarbeitung anderer Beschäftigter unternehmenseinheitlich zu regeln und zu legitimieren, kann der Abschluss einer solchen Betriebsvereinbarung (falls möglich) durchaus ein probates Mittel sein.

6.3 Inhalte einer Betriebsvereinbarung

Die Inhalte der Betriebsvereinbarung sind in erster Linie natürlich abhängig von den abschließenden Parteien, dementsprechend kann hier keine fertige Betriebsvereinbarung zur Verfügung gestellt werden. An dieser Stelle werden nur die wichtigsten Punkte bzgl. IT-Sicherheit und Datenschutz dargestellt, auf die in einer Betriebsvereinbarung eingegangen werden sollte.

- Beschreibung der eingesetzten Programme
    - Es sollte die Remote Control Software benannt werden.
    - Desgleichen die Ziele, die mit dem Einsatz verbunden werden.
    - Weiterhin ist die Funktionalität anzugeben.

  Beispiel: „Zur Fernbetreuung von PC-Problemen (z.B. Anwendung, Konfiguration) wird die Software „Fern&Gut“ des Herstellers „Gottseibeiuns“ eingesetzt. Die Software dient dazu, Anwendern bei Problemen schnell und unkompliziert eine Unterstützung anbieten zu können. Der Anwender dieser Fernbetreuungs-Software kann beispielsweise
    - eine Übersicht über die Hardwarekomponenten und der aktiven Software erhalten,
    - den Bildschirm angezeigt bekommen,
    - Software auf dem Rechner installieren oder deinstallieren,
    - Eingriffe in Dateien vornehmen,
    - steuernd in den Dialog eingreifen,
    - den gesteuerten Rechner neu starten oder auch
    - die Bedienung übernehmen.“
- Darstellung, wer die Software bedienen darf
    - Nur der eigene IT-Support? Externe Dienstleister?

  Beispiel: „Der First-Level-Support wird von der hauseigenen IT-Abteilung geleistet. In der Regel werden durch ihn alle Schwierigkeiten gemeistert. In einzelnen Fällen kann es vorkommen, dass der Hersteller des Krankenhaus-Informations-Systems als Second-Level-Support hinzugezogen wird. In diesen Fällen steht die Fernwartungs-Funktionalität auch diesem offen.“
- Datenschutzrechtliche Vorgaben
    - Der Fernzugriff auf eine nutzereigene Umgebung ist nur mit der vorherigen Zustimmung der Benutzerin oder des Benutzers zulässig. D. h. jegliche Fernwartungssitzung wird von der betroffenen Person initiiert. Automatische Updates der System- und Anwendungssoftware sind ohne Zustimmung zulässig, wenn an dem Arbeitsplatzrechner zu dem Zeitpunkt niemand angemeldet ist.
    - Dateien mit personenbezogenen Daten werden nur im eigenen Haus verarbeitet. Müssen Dateien mit personenbezogenen Daten für Zwecke der Fehleranalyse und –behebung zum Hersteller eines Systems übertragen werden, so müssen die Daten anonymisiert werden. Ist dies nicht möglich, ist die Zustimmung aller betroffenen Personen, deren Daten in den Dateien enthalten sind, also beispielsweise Beschäftigte und Patienten, einzuholen. Ohne Zustimmung ist die Übermittlung verboten.
    - Daten dürfen nicht an Dritte weitergegeben werden.

- Schulung: Alle Anwender der Fernwartungssoftware müssen einerseits in deren Bedienung unterwiesen werden, andererseits auch bzgl. des gewissenhaften Umgangs mit den Funktionen sensibilisiert werden. Eine Unterweisung bzgl. datenschutzrechtlicher Verschwiegenheitspflichten wie auch ggf. eine Verpflichtung zur Schweigepflicht nach §203 StGB ist ebenfalls zu gewährleisten, idealerweise mit regelmäßiger Wiederholung.
  - Erstellung und Aufbewahrung von Protokollen sowie Zugriff auf diese
    - Es müssen Protokolle erstellt werden, die festhalten, wann wer welche Funktionen auf welchem Rechner ausgeführt hat.
    - Protokolle werden für den Zeitraum von XXX Monaten aufbewahrt, darüber hinaus nur bei Vorliegen von konkreten Anhaltspunkten für eine Straftat.
    - Protokolle dürfen nur im Beisein eines Vertreters der Personalvertretung sowie des Datenschutzbeauftragten eingesehen werden. Einsichtsberechtigt sind der Datenschutzbeauftragte bei Vorfällen, die in seinem Zuständigkeitsbereich liegen, die Personalvertretung, wenn es für ihre Belange erforderlich ist sowie IT-Administratoren, wenn dies zu ihrer Aufgabenerfüllung (z. B. Fehlersuche) erforderlich ist.
  - Verhaltens- und Leistungskontrolle,
    - Die Nutzung der sich aus dem Einsatz der Fernwartungssoftware ergebenden Möglichkeiten einer Verhaltens- und Leistungskontrolle ist nicht gestattet.
    - Eine personenbeziehbare Auswertung von Protokollen ist nur bei hinreichendem Verdacht der Verletzung dienstrechtlicher bzw. arbeitsvertraglicher Pflichten oder auf Anordnung eines Gerichts bzw. einer Strafverfolgungsbehörde zulässig.

7 Vertrag mit einem externen Dienstleister

7.1.1 Allgemeines

Es werden alle mitgeltenden Vertragsbestandteile benannt, insbesondere alle ergänzenden Vertragsbedingungen wie z. B. AGBs von Auftraggeber und Auftragnehmer, vereinbarte Service Level Agreement usw. Grundsätzlich ist zu jedem Vertrag ein Auftragsverarbeitungsvertrag abzuschließen, welcher hier genannt werden muss.

Anforderung 66) Zu jedem Fernwartungsvertrag muss (mindestens) ein Vertrag zur Auftragsverarbeitung abgeschlossen werden, welcher den Anforderungen von Art. 28 DS-GVO genügt.

Ratio: Es kann i.d.R. nicht 100%ig ausgeschlossen werden, dass während der Fernwartung auf personenbezogene Daten zugegriffen werden muss. Bei Daten von „normalen" Kategorien kann dies ggf. durch Art. 6 Abs. 1 lit. f DS-GVO (ist zur Wahrung der berechtigten Interessen des Verantwortlichen, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen) einen Erlaubnistatbestand darstellen. Bei Daten der besonderen Kategorien gemäß Art. 9 DS-GVO ist dies nicht möglich. Daher muss in diesen Fällen ein Auftragsverarbeitungsvertrag abgeschlossen werden.

Weiterhin sind die Art und der Umfang der Leistung vertraglich zu vereinbaren. Dies können z. B. Leistungen zur Mängelbehebung, zur Lieferung von Upgrades/Releases/Versionen oder auch Umsetzungs- und Installationsleistungen sein. Ggf. ist es sinnvoll, bei Beginn der vertraglichen Leistung die Erfassung der Ist-Situation zu dokumentieren und eine detaillierte Beschreibung des Soll-Zustands darzulegen.

Anforderung 67) In jedem Fernwartungsvertrag muss die zu erbringende Leistung vertraglich vereinbart sein.

Ratio: Der Zweck muss hinreichend genau abgebildet werden, daher ist eine entsprechende Leistungsbeschreibung erforderlich.

Hinweis: Schlechte Anforderungsbeschreibungen gelten als der Hauptgrund für ausufernde Kosten und wiederholte Terminüberschreitungen[7]. Während bei anderen IT-Projekten meistens anlässlich Streitigkeiten bzgl. der vereinbarten Leistungserbringung eine Möglichkeit der Rückabwicklung besteht, ist beim Outsourcing nach dem „Go-Live" eine Rückabwicklung i.d.R. so unwirtschaftlich, dass die Fortführung der Zusammenarbeit bestehen bleibt und ggf. ein Streit über die Vergütung zwischen den Vertragsparteien die Vertragsdauer begleiten kann. Auch aus dieser Sicht ist eine detaillierte Leistungsbeschreibung zu fordern. Weiterhin können auch gesetzliche Anforderungen bestehen, die eine detaillierte Leistungsbeschreibung fordern[8]. Diese Forderung nach einem ausreichenden Detailgrad verhindert nicht eine gewisse Flexibilität. Klauseln, welche beispielsweise dem Auftraggeber erlauben, auf technologische Trends, Entwicklungen und Verbesserungen in Bezug auf die outgesourcten Leistungen zu reagieren, sind allgemein üblich und für beide Vertragspartner von Vorteil. Und natürlich können sich während der Laufzeit des Vertrags Rahmenbedingungen ändern, so dass Neu- bzw. Nachverhandlungen erforderlich werden.

[7] Siehe z. B. Hoppen P. (2015) Software-Anforderungsdokumentation. CR : 747-760

[8] Witzel M. (2017) Risiken und Fallstricke unvollständiger Leistungsbeschreibungen bei Outsourcing. CR: 557-563

Anforderung 68) In jedem Fernwartungsvertrag sollte der Ist-Zustand bei Vertragsbeginn wie auch der Beschreibung des Soll-Zustand während der Vertragslaufzeit beschrieben werden.

Ratio: Nur wenn der Ist- wie auch der Soll-Zustand festgehalten wird, kann festgestellt werden, ob die Entwicklung der Fernwartungssituation in die richtige Richtung verläuft.

Im Vertrag sollten die zeitlichen Anforderungen dargelegt werden: wann ist ein System produktiv einsetzbar (Betriebszeit), welche Servicezeiten stehen zur Verfügung, welche Reaktions- und Wiederherstellungszeiten gelten, welche Wartungszeiten sind zu erwarten, welche Ausfallzeit usw.

Anforderung 69) In jedem Fernwartungsvertrag sollten die Produktivzeiten vereinbart werden.

Ratio: Es muss festgehalten werden, zu welchen Zeiten eine Fernwartung abgerufen werden darf. Nur so kann festgestellt werden, ob ein Zugriff im Rahmen der Fernwartungsmöglichkeiten außerhalb der vereinbarten Zeiten erfolgt.

Anforderung 70) In jedem Fernwartungsvertrag sollten die Reaktionszeit sowie die Servicezeiten vereinbart werden.

Ratio: Bei jeder Verarbeitung personenbezogener Daten muss der Verantwortliche die Verfügbarkeit der Daten gewährleisten. Da eine Fernwartung i.d.R. auch zu Supportzwecken eingesetzt wird, dient die Fernwartung auch der Gewährleistung dieser Anforderung. Somit muss festgehalten werden, wie die Reaktionszeiten sind.

Anforderung 71) In jedem Fernwartungsvertrag sollte die Zeit vereinbart werden, wann Wartungsarbeiten ausgeführt werden können.

Ratio: Wartungsarbeiten können die Verfügbarkeit der Daten beeinflussen. Daher müssen diese Zeiten eingeplant und ggf. Anwendern gegenüber kommuniziert werden. Auch müssen Wartungsarbeiten explizit durch den Auftraggeber beauftragt werden. Damit der Fernwartende dennoch planen kann, müssen entsprechende Zeiten vereinbart werden.

7.1.2 Gegenstand der Vereinbarung

Hier ist detailliert aufzuführen, was die Vereinbarung zur Fernwartung umfasst. D. h. es erfolgt eine Beschreibung

- der Systeme, auf die per Fernwartung zugegriffen werden soll
- der Softwareprodukte, welche während einer Fernwartungssitzung betreut werden
- der Softwareprodukte, die bei der Fernwartung eingesetzt werden sollen
- des Umfangs der Fernwartung (in welchen Fällen erfolgt eine Fernwartung)
- der Art der Fernwartung (nur Fernwartung, auch vor Ort, …)
- des Zweckes der Fernwartung, also z. B. Fehlerbehebung oder Einspielen von Updates/Patches
- der Umfang der Zugriffe (auf welche Laufwerke/Verzeichnisse/Dateien darf zugegriffen werden, erfolgt auch ein schreibender oder nur ein lesender Zugriff)
- der Zeiten der Fernwartung (z. B. permanent, nur wochentags, Mo-Fr 8:00 bis 18:00 Uhr)
- der Art der personenbezogenen Daten, die vom Zugriff betroffen sein können
- der vom Zugriff ausgenommenen Systeme und Softwareprodukte
- des Kreises der Betroffenen.

7.1.3 Pflichten des Auftraggebers

1) Der Auftraggeber gewährleistet die Rechtmäßigkeit der beauftragten Verarbeitung der Daten. Insbesondere ist der Auftraggeber für die Beurteilung der Zulässigkeit der Fernwartung sowie für die Wahrung der Rechte der Betroffenen verantwortlich.

2) Soweit bei Arbeiten besondere gesetzliche oder betriebliche Sicherheitsbestimmungen zu befolgen sind, wird der Auftraggeber diese dem Auftragnehmer rechtzeitig vor Aufnahme der Arbeiten zur Verfügung stellen.

3) Der Auftraggeber stellt dem Auftragnehmer die für die Leistungserbringung erforderlichen Daten und Informationen zur Verfügung und benennt dem Auftragnehmer die internen und externen Ansprechpartner.

4) Der Auftraggeber benennt dem Auftragnehmer einen Sicherheitsbeauftragten als Ansprechpartner.

5) Der Auftraggeber benennt dem Auftragnehmer alle ihm gegenüber für den Auftrag geltenden Datenschutz- und Sicherheitsanforderungen.

6) Der Auftraggeber ist berechtigt, Anweisungen über Art, Umfang und Ablauf der Fernwartung zu erteilen.

7) Der Auftraggeber überwacht die Fernwartung. Alle Zugriffe, die im Rahmen der Fernwartung in Systemen des Auftraggebers erfolgen, werden protokolliert. Die Protokollierung muss revisionssicher sein und darf vom Auftragnehmer nicht abgeschaltet werden.

8) Der Auftraggeber hat das Recht, die Fernwartung zu unterbrechen, insbesondere wenn er den Eindruck gewinnt, dass unbefugt auf Dateien zugegriffen wird. Die Unterbrechung kann erfolgen, wenn eine Fernwartung mit nicht vereinbarten Hard- und Softwarekomponenten festgestellt wird.

7.1.4 Pflichten des Auftragnehmers

1) Der Auftragnehmer ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftraggebers geheim zu halten und in keinem Fall Dritten zur Kenntnis zu bringen.

2) Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen.

3) Der Auftragnehmer sichert die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Insbesondere erfolgt der Zugriff auf Daten und IT-Systeme des Auftraggebers ausschließlich im Rahmen getroffener Vereinbarungen.

4) Der Auftragnehmer gewährleistet die Einhaltung der vom Auftraggeber vorgegebenen Datenschutz- und Sicherheitsanforderungen. Insbesondere müssen alle notwendigen Datenübertragungen zu Zwecken der Fernwartung in dem Stand der Technik entsprechender verschlüsselter Form erfolgen; Ausnahmen sind besonders zu begründen und nur nach Genehmigung des Auftraggebers zulässig.

5) Die Einhaltung der vertraglich vereinbarten und einzuhaltenden Datenschutz- und Sicherheitsanforderungen werden vom Auftragnehmer stichprobenartig überprüft und das Ergebnis dokumentiert. Die Dokumentation muss auf Anfrage dem Auftraggeber zur Verfügung gestellt werden. Der Auftragnehmer erkennt an, dass der Auftraggeber berechtigt ist, die Einhaltung der vertraglich vereinbarten Anforderungen im erforderlichen Umfang zu kontrollieren, wenn die Dokumentation den Anforderungen des Auftraggebers nicht genügt oder ein Vorfall eine Prüfung erforderlich macht.

6) Entscheidungen zur Organisation und Durchführung der Fernwartung, insbesondere sicherheitsrelevante Entscheidungen, sind mit dem Auftraggeber abzustimmen.

7) Die Fernwartung von Privatwohnungen aus ist nicht gestattet. Soll im Einzelfall davon abgewichen werden, bedarf dies einer gesonderten schriftlichen Zustimmung des Auftraggebers. In diesem Fall ist der Zugang zur Wohnung durch den Auftraggeber vorher mit dem Auftragnehmer abzustimmen. Der Auftragnehmer sichert zu, dass auch die anderen Bewohner dieser Privatwohnung mit dieser Regelung einverstanden sind.

8) Der Auftraggeber ist in der Lage, jederzeit detaillierte Informationen (einschließlich Berechtigungen) über die zugewiesenen fernwartenden Anwender bereitzustellen.

9) Der Auftragnehmer hat ein aktuelles Security Framework umgesetzt. Dies kann der Auftraggeber dem Auftragnehmer auf Nachfrage jederzeit nachweisen.

10) Der Auftragnehmer muss seine Beschäftigten im Zusammenhang mit dem bei ihm eingesetzten Security Framework angemessen und regelmäßig ausbilden.

11) Der Auftragnehmer muss dem Auftraggeber einen Sicherheitsbeauftragten benennen, der im Zusammenhang mit allen Anliegen auf dem Gebiet der Informationssicherheit der Ansprechpartner für den Auftraggeber ist.

12) Der Auftragnehmer muss sicherstellen, dass Sicherheitsvorfälle unverzüglich nach deren Feststellung dem ihm gegenüber benannten Sicherheitsbeauftragten des Auftraggebers gemeldet werden.

13) Beabsichtigt der Auftragnehmer, die dem Auftraggeber bereitgestellten Dienstleistungen beziehungsweise Teile davon vertraglich an einen Unterauftragnehmer zu vergeben, muss der Auftragnehmer vorher eine schriftliche Erlaubnis des Auftraggebers einholen.

14) Der Auftragnehmer muss sicherstellen, dass alle Sicherheitsanforderungen an den von ihm bereitgestellten Dienst auch für seine Unterauftragnehmer gelten.

15) Vertrauliche Daten, die dem Auftraggeber gehören, darf der Auftragnehmer nicht ohne den Anforderungen des Auftraggebers entsprechende Schutzmechanismen lokal speichern.

16) Erfolgt eine lokale Speicherung, so sichert der Auftragnehmer zu, dass die verarbeiteten Daten von sonstigen Datenbeständen getrennt gespeichert werden.

17) Vor Zugriff auf personenbezogene oder personenbeziehbare Daten holt der Auftragnehmer grundsätzlich die Zustimmung des Auftraggebers ein.

18) Die Übertragung personenbezogener oder personenbeziehbarer Daten zum Auftragnehmer ist verboten.

19) Erfolgt im Rahmen einer Fernwartungssitzung ein Zugriff auf einen Arbeitsplatzrechner, so darf ein Aufbau einer Fernwartungssitzung nur nach erfolgter Zustimmung durch den mit der Arbeitsstation verbundenen Beschäftigten erfolgen.

8 Risikomanagement

Im Rahmen der Pflichten von Versicherungen, insbesondere auch von Haftpflichtversicherungen, besteht die Verpflichtung vorhandene Risiken wo immer möglich zu identifizieren, zu bewerten und – wo möglich – durch Ergreifung geeigneter Maßnahmen die Risiken zu minimieren. Dies betrifft insbesondere natürlich auch alle IT-Verarbeitungen, somit auch Fernwartungsprozesse.

Aktiengesellschaften sowie Gesellschaften, die 2 der 3 Kriterien in 2 aufeinander folgenden Jahren erfüllen

- Bilanzsumme > 3,44 Mio. Euro,
- Umsatz > 6,87 Mio. Euro
- Mitarbeiterzahl > 50,

sind auch aufgrund von § 91 AktG bzw. dem Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) verpflichtet, Risikofrüherkennungssysteme, Risikomanagement- und -steuerungssysteme zu installieren. D. h. für diese Unternehmen gilt neben den evtl. vorhandenen Anforderungen aus Versicherungsverträgen auch aus diesen Gesetzen eine Pflicht zum Risikomanagement.

Weiterhin können diesbezügliche unternehmerische Anforderungen aus den Prüfstandards des Instituts der Wirtschaftsprüfer resultierend, insbesondere aus den Prüfungsstandard 330 und 33, die vom Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW) herausgegeben wurden.

Kurz: eine Risikoanalyse muss durchgeführt werden. Anleitungen zum durchführen einer Risikoanalyse sind an verschiedenen Stellen zu finden, u.a. auch in einem Papier der GMDS[9].

Anforderung 72) Erfolgte eine Risiko-Analyse bzgl. des Fernwartungsvorganges und wurden ggf. Maßnahmen zur Verringerung des Risikos getroffen?

Ratio: Ein Fernwartungsvorgang bedingt immer die Öffnung des eigenen Netzwerkes nach außen, was potentiell das Risiko bzgl. ungewollter externer Netzzugriffe erhöht.

Anforderung 73) Erfolgte eine Analyse bzgl. des Einflusses des Fernwartungsvorganges auf vorhandene Risikoanalysen?

Ratio: Das einem Fernwartungsvorgang innewohnende Risiko kann potentiell auch andere Prozesse betreffen und damit die Risiken für diese Prozesse verändern. D.h. eine Risikobetrachtung für die Fernwartung muss immer auch die dem Fernwartungsprozess innewohnenden Auswirkungen auf andere Vorgänge/Prozesse beinhalten.

[9] GMDS AG "Datenschutz und IT-Sicherheit im Gesundheitswesen" (DIG): Leitfaden zur Erstellung eines IT-Sicherheitskonzeptes. [Online, zitiert am 2018-02-13]; Verfügbar unter https://www.gesundheitsdatenschutz.org/doku.php/gmds-dgi-empfehlungen

9 Checkliste

9.1 Fernwartungskonzept

	Ja	Nein
Existiert ein Fernwartungskonzept?		
Enthält dieses Regelungen für die Fernwartung der IT-Komponenten?		
Enthält dieses Regelungen für die Fernwartung der TK-Komponenten?		
Gibt es einen Verantwortlichen, der sich regelmäßig über die Sicherheit der verwendeten Systeme und relevante Sicherheits-Updates der eingesetzten Software informiert?		
Gibt es schriftlich festgehaltene Vorgaben zum Testen von geplanten Änderungen von Hardware oder Software?		

9.2 Art der Fernwartung

	Benennen, was genau
Hardware	
Software	
Betriebssystem	
Anwendungen	
Benutzeradministration	
TK-Anlage	
Sonstiges	

9.3 Inhalte der Fernwartung

	Ja	Nein
Benutzerbetreuung		
Einspielen von Updates/Upgrades mit Sicherheitsrelevanz		
Einspielen von Updates/Upgrades zur Verbesserung der Systemstabilität		
Einspielen von Updates/Upgrades zur Änderung der Funktionalität		

9.4 Rechte der Fernwartenden

	Ja	Nein
Benutzerrechte		
Shell-Kommando-Zugriff		
Administrationsrechte		
Sonstige (Bitte benennen)		

9.5 Fernwartungszugang

9.5.1 Zugangsweg

	Ja	Nein
Telefonnetz / Modem		
ISDN		
Standleitung		
VPN		
3-Anbieter-Software (PCAnywhere / VNC / Teamviewer / … - benennen)		

9.5.2 Identifizierung

	Ja	Nein
Keine		
call-back		
Rufnummernidentifikation		
Benutzerkennung		
Passwort		

9.5.3 Verschlüsselung

Werden die Daten bei der Übertragung verschlüsselt?	
Mit welchem Verfahren?	
Welche Daten?	
Wie wird die Verschlüsselung protokolliert?	
Werden die Protokolle ausgewertet?	

9.6 Datenschutzrechtliche Vorgaben

	Ja	Nein
Existiert hierüber ein Auftragsverarbeitungsvertrag entsprechend Art. 28 DS-GVO		
Erfolgt ein Monitoring der Fernwartung? Wenn ja, welches?		
Vier-Augen-Prinzip		
Protokollierung Login/Logout		
Protokollierung Systemänderungen		
Videoaufzeichnung		
Werden die Protokolle ausgewertet?		
Ist gewährleistet, dass vor dem Zugriff auf personenbezogene oder personenbeziehbare Daten die Zustimmung des Verantwortlichen eingeholt wird?		
Wurde die Übertragung personenbezogener oder personenbeziehbarer Daten im Rahmen der Fernwartung verboten?		

10 Beispiele

10.1 Ermittlung des Schutzbedarfs

10.1.1 Grundsätzliches zur Einstufung des Schutzbedarfs

ErwGr. 51 DS-GVO sieht bei besonderer Kategorien von personenbezogenen Daten einen besonders hohen Schutzbedarf: „Personenbezogene Daten, die ihrem Wesen nach hinsichtlich der Grundrechte und Grundfreiheiten besonders sensibel sind, verdienen einen besonderen Schutz, da im Zusammenhang mit ihrer Verarbeitung erhebliche Risiken für die Grundrechte und Grundfreiheiten auftreten können."

Art. 9 DS-GVO benennt diese besonderen Datenkategorien:

- Daten, aus denen die rassische und ethnische Herkunft, hervorgeht,
- Daten bzgl. politischer Meinungen,
- Daten hinsichtlich religiöser oder weltanschaulicher Überzeugungen,
- Daten, aus denen die Gewerkschaftszugehörigkeit hervorgeht,
- genetischen Daten,
- biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person,
- Gesundheitsdaten
- Daten zum Sexualleben oder der sexuellen Orientierung.

Eine Verarbeitung dieser Datenkategorien beinhaltet also immer „erhebliche Risiken für die Grundrechte und Grundfreiheiten" betroffener Personen (ErwGr. 51 DS-GVO), d. h. diese Daten haben immer einen hohen Schutzbedarf. Dies wird auch von deutschen Datenschutzaufsichtsbehörden so gesehen. Das Bayerische Landesamt für Datenschutzaufsicht schreibt in ihrem Kurzpapier „[EU] Besondere Kategorien personenbezogener Daten - Art. 9 DS-GVO" dazu[10]: „Auch unter der DS-GVO bleiben die genannten Kategorien besonders schutzbedürftig".

Sobald daher die in Art. 9 DS-GVO benannten besonderen Kategorien personenbezogener Daten verarbeitet werden, muss immer von einem hohen Schutzbedarf ausgegangen werden, welcher besondere Maßnahmen zur Gewährleistung eines entsprechend hohen Sicherheitsniveaus verlangt.

Neben diesen besonderen Kategorien personenbezogener Daten existieren natürlich auch Datenkategorien, die ggf. einen geringeren Schutzbedarf aufweisen. Dabei müssen die zu verarbeitenden Daten immer genau betrachtet werden. Beschäftigtendaten beispielsweise ´sind in der Auflistung von Art. 9 DS-GVO nicht enthalten. Jedoch sind in den Beschäftigtendaten ggf. Daten bzgl. der religiösen Überzeugungen vorhanden, da die Religionszugehörigkeit zur Erhebung der Kirchensteuer erfasst wird. Ggf. werden Mitgliedsbeiträge zu Gewerkschaften direkt vom Lohn abgebucht, so dass auch diese besondere Datenkategorie enthalten sein kann. Krankmeldungen werden in der Personalakte aufbewahrt, so dass Beschäftigtendaten i.d.R. auch Gesundheitsdaten beinhalten.

D. h. um aus den Datenkategorien die Risiken und damit den Schutzbedarf abzuleiten, müssen immer die zu verarbeitenden Daten genau betrachtet werden. Die in Art. 9 DS-GVO genannten

[10] Bayerisches Landesamt für Datenschutzaufsicht (BayLDA): [EU] Besondere Kategorien personenbezogener Daten - Art. 9 DS-GVO. [Online, zitiert am 2018-03-17]; Verfügbar unter https://www.lda.bayern.de/media/baylda_ds-gvo_6_special_categories.pdf

Datenkategorien erfordern immer ein hohes Schutzniveau, aber auch bei anderen Datenarten muss ggf. von einem hohen Schutzbedarf ausgegangen werden.

10.1.2 Beispiele für Fernwartung

Typische Beispiele für die Fernwartung, bei der ein Zugriff auf sensible Daten nicht immer zwingend notwendig ist:

- Regelmäßige Überprüfung des zu wartenden Systems (Systemmonitoring)
- Regelmäßiges Einspielen von Software Patches (Sicherheitsupdates, Fehlerbehebungen, funktionalen Erweiterungen, etc.).

Typische Beispiele bei denen Varianten gewählt werden können, die keinen Zugriff auf sensible Daten benötigen:

- Konfiguration, Zusatzentwicklungen oder Anpassungen auf Entwicklungssystemen, die sich anschließend auf die Produktivumgebung übertragen lassen.

Typische Beispiele, bei denen der Zugriff auf die sensiblen Daten sich nicht vermeiden lässt:

- Fehleranalyse und -behebung in der Produktivumgebung
- Konfiguration in der Produktivumgebung
- „produktive Dienstleistungen“ wie Notfallvertretung, die eigentlich keine Fernwartung sind jedoch über die Wartungsinfrastruktur erbracht werden.

Für die technisch organisatorischen Maßnahmen wäre zu prüfen, ob der Zugriff auf sensible Daten bereits über das zu wartende Produkt eingeschränkt und deshalb für die Fernwartungsverbindung und die Sessionkontrolle der Aufwand reduziert werden kann, oder ob es einfacher ist, einen einheitlichen hohen Maßstab zu etablieren.

10.2 Planung der Fernwartung

Fernwartung für Hardware/Software: …

Nummer		Standort:	
Erfasst am:		Erfasst durch:	

Planung des Einsatzes von Fernwartung

Umsetzung bis:		Kostenschätzung:	
Verantwortlich:		Bemerkungen:	

Regelungen zu Kommunikationsverbindungen mit Dienstleister treffen

Umsetzung bis:		Kostenschätzung:	
Verantwortlich:		Ansprechpartner Dienstleister:	
Ergebnis		Bemerkungen:	

Auswahl geeigneter Fernwartungswerkzeuge

Umsetzung bis:		Kostenschätzung:	
Verantwortlich:		Bemerkungen:	

Gewährleistung einer sicheren Verbindung für Fernwartung

1) Einsatz kryptographischer Verfahren bei der Fernwartung				
Umsetzung bis:			Kostenschätzung:	
Verantwortlich:			Ergebnis:	
2) Authentisierungsmechanismen bei der Fernwartung				
Umsetzung bis:			Kostenschätzung:	
Verantwortlich:			Ergebnis:	
3) Passwortsicherheit bei der Fernwartung				
Umsetzung bis:			Kostenschätzung:	
Verantwortlich:			Ergebnis:	

Verwaltung des Fernwartungszugangs

Umsetzung bis:		Kostenschätzung:	
Verantwortlich:		Bemerkungen:	

Vorabarbeiten bzgl. Fernwartung

1) Schulungen				
Umsetzung bis:			Kostenschätzung:	
Verantwortlich:			Bemerkungen:	
2) Patch- und Änderungsmanagement				
Umsetzung bis:			Kostenschätzung:	
Verantwortlich:			Bemerkungen:	
3) Datensicherung				
Umsetzung bis:			Kostenschätzung:	
Verantwortlich:			Bemerkungen:	

Dokumentation der Fernwartung

Umsetzung bis:		Kostenschätzung:	
Verantwortlich:		Bemerkungen:	

Protokollierung der Fernwartung

Umsetzung bis:		Kostenschätzung:	
Verantwortlich:		Bemerkungen:	

10.3 Beurteilung einer Fernwartungssoftware

10.3.1 Beschreibung der Funktionalität

1) Die Fernwartungs-Software kann durch entsprechende Einstellungen in der Windows-Registry als Hintergrundprozess vom Nutzer vollständig unbemerkt mit dem Systemstart gestartet werden.
    a. In diesem Fall erscheint auch kein Icon im System-Tray (alle Icons, bis auf die Urzeit werden ausgeblendet).
    b. Erst beim Fernzugriff selbst erscheint ein kleines Fenster.
    c. Dieser Fernzugriff ist auch ohne eine aktive Handlung des Nutzers möglich, wenn der Zugreifende das Passwort für die Fernwartungs-Software kennt, was regelmäßig der Fall ist, wenn dieser den Fernwartungs-Host eingerichtet hat.

2) Die Fernwartungs-Software setzt als kryptographische Verfahren RSA-2048, AES-256 und SRP ein.
    a. In den der Öffentlichkeit zur Verfügung stehenden Unterlagen ist jedoch nicht beschrieben, wie gewährleistet wird, dass der vom (unter Kontrolle des Herstellers der Fernwartungs-Software stehende) Masterserver übermittelte öffentliche Schlüssel tatsächlich zum vermuteten Kunden oder dem fernwartenden Dienstleister gehört.
    b. Dienstleister und Kunde können dies nicht anhand weiterer Informationen, beispielsweise mit Zertifikaten von unabhängigen Stellen, prüfen.
    c. Sie sind in diesem Punkt vollständig auf den Hersteller der Fernwartungs-Software angewiesen.
3) Jegliche Kommunikation erfolgt über die Server der Hersteller-Firma der Fernwartungs-Software, desgleichen und jede Anmeldung an die Fernwartungs-Software.

10.3.2 Beurteilung

1) Wird eine Fernwartungs-Software innerhalb des Unternehmens eingesetzt, wobei ggf. auch personenbezogene Daten wie z.B. Beschäftigtendaten verarbeitet werden, ist grundsätzlich wie bei jeder Verarbeitung die datenschutzrechtliche Berechtigung zu klären.
    a. BDSG (gültig bis 24. Mai 2018)
        i. § 32 BDSG kann mögliche Rechtsgrundlage darstellen.
            – Die Fernwartungs-Software dürfte nicht zur „Durchführung“ eines Beschäftigungsverhältnisses erforderlich sein, wie es § 32 BDSG fordert. Daher scheidet § 32 BDSG aus.
        ii. § 28 Abs. 1 Nr. 2 BDSG: berechtigtes Interesse
            – Eine effektive und zeitnahe Bearbeitung von IT-Problemen über eine Fernwartungssoftware kann durchaus als berechtigtes Interesse des Arbeitgebers im Sinne von §28 Abs. 1 Nr. 2 BDSG gewertet werden.
            – Allerdings dürfen die Interessen der Betroffenen nicht überwiegen, ein milderes Mittel (eine andere Möglichkeit, welche das informationelle Selbstbestimmungsrecht des Betroffenen weniger beeinflusst) darf nicht existieren.
            – Ein milderes Mittel wäre eine Software, die so konfiguriert werden kann, dass eine (heimliche) Überwachung des Beschäftigten nicht ermöglicht wird.
    b. BDSG n.F. (gültig ab 25. Mai 2018)
        i. § 26 BDSG n.F. regelt die Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses
            – § 26 Abs. 1 S. 2 BDSG n.F.: „Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies […]
                - nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung oder
                - zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten

            erforderlich ist.

- D. h., der Arbeitgeber muss die Erforderlichkeit des Einsatzes der Fernwartungs-Software nachweisen. Hierzu ist – neben dem Nachweis bzgl. der Notwendigkeit der Fernwartung - insbesondere der Nachweis erforderlich, dass kein milderes Mittel (i.S. von weniger in das informationelle Selbstbestimmungsrecht des Betroffenen eingreifend) zur Erreichung der Ziele verfügbar ist.

2) Im Falle von Sicherheitslücken müssen ggf. Kunden aktiv über diese Sicherheitslücken informiert werden. (z. B. EU-Verordnung 611/2013. § 96 Abs. 2 TKG oder auch IT-Sicherheitsgesetz)
    a. Wie genügt der Fernwartende seiner Informationspflicht gegenüber dem Auftraggeber bzw. den betroffenen Beschäftigten? Bekommt er die notwendigen Informationen vom Hersteller der Fernwartungs-Software?
3) Entsprechend der Beschreibung von Punkt 1) der Funktionalität ist mittels der Fernwartungs-Software auch ein unbeaufsichtigter Zugriff auf den Rechner des Nutzers, z. B. in dessen Abwesenheit, möglich.
    a. Gemäß § 87 Abs. 1 Nr. 6 BetrVG besteht ein Mitbestimmungsrecht des Betriebsrates bei der „Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen“.
        - Eine technische Einrichtung ist dann zur Überwachung bestimmt, wenn sie objektiv geeignet ist, Verhalten und Leistung der Arbeitnehmer zu überwachen.
        - Die objektive Eignung liegt bereits vor, wenn durch Verarbeitung gleich welcher Daten Aussagen über Verhalten und Leistung der Arbeitnehmer gewonnen werden können. Schließlich ist es irrelevant, ob der Arbeitgeber eine Beurteilung von Verhalten oder Leistung überhaupt beabsichtigt und entsprechend vornimmt. (siehe Gesetzeskommentierung Klebe in Däubler/Kittner/Klebe/Wedde)
    b. Ein unbeaufsichtigter Fernzugriff durch den Arbeitnehmer ist mittels der beschriebenen Funktionalität der Fernwartungs-Software möglich, z.B. mittels Screenshots in regelmäßigen Abständen.
        - Somit können mittels der Fernwartungs-Software Aussagen über das Verhalten und die Leistung der Arbeitnehmer getroffen werden, weshalb die objektive Eignung zur Überwachung vorliegt.
        - Mithin ist die Fernwartungs-Software i.S.d. § 87 Abs. 1 Nr. 6 BetrVG auch dazu bestimmt, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen.

    Fazit 1: Einsatz ist Mitbestimmungspflichtig

4) Entsprechend der Beschreibung von Punkt 2) der Funktionalität der Fernwartungs-Software ist eine Vertraulichkeit der Kommunikation nicht sichergestellt. Bedingt durch die Unkontrollierbarkeit der Zertifikate, kann der Hersteller der Fernwartungs-Software jederzeit als Man-in-the Middle agieren.
    a. Man muss davon ausgehen, dass der Hersteller der Software Zugriff auf die Daten hat. Dementsprechend muss ein Erlaubnistatbestand zur Verarbeitung vorliegen.
    b. Daher muss ein Auftragsverarbeitungsvertrag zwischen dem die Fernwartungs-Software einsetzendem Unternehmen und dem Hersteller der Fernwartungs-Software vereinbart werden.
    c. Ist das die Fernwartungs-Software einsetzende Unternehmen Dienstleister für einen Auftraggeber, muss der Einsatz der Fernwartungs-Software im

Auftragsverarbeitungsvertrag zwischen Auftraggeber und Dienstleister vereinbart werden. In diesem Fall muss der Dienstleister evtl. bestehende Pflichten aus diesem Auftragsverarbeitungsvertrag in seinem Auftragsverarbeitungsvertrag mit dem Hersteller der Fernwartungs-Software weiterreichen.

d. Beschäftigte müssen darüber informiert werden, dass ihre Daten ggf. an Dritte weitergegeben werden.

Fazit 2: Es muss ein Auftragsverarbeitungsvertrag vereinbart werden, Beschäftigte müssen über den Einsatz informiert werden.

5) Entsprechend der Beschreibung von Punkt 3) der Funktionalität der Fernwartungs-Software müssen Artt. 40-49 DS-GVO beachtet werden, wenn die Server in einem Drittland stehen.

Fazit 3: Ggf. ist ein Erlaubnistatbestand für die Verarbeitung in einem Drittland erforderlich.

Abschließende Beurteilung: Bei Anwendungen mit hohem Schutzbedarf, wie es die Verarbeitung von Gesundheitsdaten darstellt, genügt die Fernwartungs-Software nicht den Anforderungen, sie entspricht nicht dem Stand der Technik.

11 Glossar

Aufzeichnung	Dokument, das erreichte Ergebnisse angibt oder einen Nachweis ausgeführter Tätigkeiten bereitstellt (Quelle: ISO 9000)
Authentisierung	Beibringung eines Belegs für die von einer Entität behauptete Identität durch die sichere Verbindung eines Identifikators und seines Authentifikators (Quelle: DIN EN ISO 22600-1)
Authentisierung, starke	Authentisierung mittels kryptographisch abgeleiteter multifaktorieller Identitätsnachweise (Quelle: DIN EN ISO 22600-1)
Autorisierung	Erteilung von Privilegien, einschließlich des Privilegs für den Zugriff auf Daten und Funktionen (Quelle: DIN EN ISO 22600-1)
Business Continuity	Prozesse und/oder Verfahren, die der Sicherstellung eines kontinuierlichen Geschäftsbetriebs Dienen (Quelle: DIN ISO/IEC 27000)
Delegierung	Übertragung eines Privilegs von einer Entität, die dieses Privileg besitzt, auf eine andere Entität (Quelle: DIN EN ISO 22600-1)
Entität	natürliche oder juristische Person, öffentliche Behörde oder Einrichtung oder eine andere Stelle (Quelle: DIN CEN ISO/TS 14441)
Ereignis	Auftreten von ungewöhnlichen Umständen (Quelle. DIN ISO/IEC 27000)
Identifikator	Information, die verwendet wird, um vor einer möglichen Bestätigung durch einen entsprechenden Authentifikator eine Identität zu beanspruchen (Quelle: E NV 13608-1)
Identifizierung	Durchführung von Tests mit dem Ziel, das betreffende Datenverarbeitungssystem in die Lage zu versetzen, bestimmte Entitäten zu erkennen (Quelle: ISO/IEC 2382-8])
Informationssicherheit	Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen; andere Eigenschaften, wie die Authentizität, die Zurechenbarkeit, die Nichtabstreitbarkeit und die Verlässlichkeit, können ebenfalls dazugehören. (Quelle: ISO/IEC 27000)
Integrität	Eigenschaft, die bedingt, dass die Information in keiner Weise, weder absichtlich noch unabsichtlich, geändert Wird (Quelle: DIN EN ISO 22600-2)
Kennung	Durchführung von Tests mit dem Ziel, das betreffende Datenverarbeitungssystem in die Lage zu versetzen, bestimmte Entitäten zu erkennen (Quelle: ISO/IEC 2382-8)
Korrekturmaßnahme	Maßnahme zur Beseitigung der Ursache eines erkannten Fehlers oder einer anderen erkannten unerwünschten Situation (Quelle ISI 9000)

Nicht-Abstreitbarkeit	Fähigkeit, das Auftreten eines behaupteten Ereignisses oder einer Handlung und die verursachenden Einheiten nachzuweisen, um Streitigkeiten über das Auftreten oder Nichtauftreten des Ereignisses oder der Handlung und die Beteiligung von Einheiten an dem Ereignis zu entscheiden (Quelle. DIN ISO/IEC 27000)
Personal	jede Einzelperson, von der erwartet wird, dass sie Aufgaben für das Unternehmen ausführt, einschließlich leitende Angestellte, Arbeitnehmer und Subunternehmer (Quelle: DIN ISO/IEC 19770-1)
Policy	Menge von gesetzlichen, politischen, organisatorischen, funktionellen und technischen Verpflichtungen, die sich auf Kommunikation und Kooperation beziehen (Quelle: DIN EN ISO 22600-1)
Policy-Vereinbarung	schriftliche Vereinbarung, nach der sich alle Beteiligten zur Einhaltung einer festgelegten Reihe von Policies verpflichten (Quelle: DIN EN ISO 22600-1)
Prozess	eine Menge miteinander verknüpfter Aktivitäten, die Eingänge in Ausgänge umwandelt (Quelle: DIN ISO/IEC 19770-1)
Richtlinie	Empfehlung dessen, was an Umsetzung erwartet wird, um ein Ziel zu erreichen (Quelle. DIN ISO/IEC 27000)
Rolle	Menge von mit einer Aufgabe verbundenen Kompetenzen und/oder Leistungen (Quelle: DIN EN ISO 22600-1)
Sensibilität	Eigenschaft einer Ressource, die deren Wert oder Wichtigkeit impliziert (Quelle: DIN EN ISO 22600-2)
Sicherheitsdienst	Dienst, der von einer Schicht miteinander kommunizierender offener Systeme bereitgestellt wird und die Sicherheit der Systeme oder der Datenübertragung in angemessenem Maße sicherstellt (Quelle: ISO 7498-2)
Sicherheits-Policy	Plan oder Vorgehensweise für die Sicherstellung der Rechnersicherheit (Quelle: ISO/IEC 2382-8)
Systemintegrität	Eigenschaft, dass ein System seine vorgesehene Funktion in einer unbeeinträchtigten Art und Weise, frei von vorsätzlicher oder zufälliger unberechtigter Veränderung des Systems, ausführt (Quelle: ISO 27799)
Unleugbarkeit	Dienstleistung, die einen Nachweis für die Integrität und die Herkunft der Daten (beides auf fälschungssichere Art und Weise) erbringt, der von einer beliebigen anderen Partei verifiziert werden kann (Quelle: DIN EN ISO 22600-2)
Unternehmensvorstand oder gleichwertiges Organ	Person oder Gruppe von Personen, die juristische Verantwortung in der Führung oder Kontrolle eines Unternehmens auf höchster Ebene übernimmt/übernehmen (Quelle: DIN ISO/IEC 19770-1)
Verfahren	festgelegte Art und Weise, eine Tätigkeit oder einen Prozess auszuführen (Quelle: ISO 9000)
Verfügbarkeit	Eigenschaft, auf Nachfrage einer berechtigten Entität zugreifbar und verwendbar zu sein (Quelle: SO/IEC 27000)

Verlässlichkeit	Eigenschaft der Übereinstimmung zwischen beabsichtigtem Verhalten und den Ergebnissen (Quelle. DIN ISO/IEC 27000)
Vertrauen	m Allgemeinen kann davon ausgegangen werden, dass eine Entität einer anderen Entität „vertraut“, wenn sie annehmen kann, dass sich die zweite Entität genauso, wie von der ersten Entität erwartet, verhalten wird (Quelle: DIN EN ISO 22600-2)
Vertraulichkeit	Eigenschaft, dass Informationen gegenüber unberechtigten Personen, Entitäten oder Prozessen nicht verfügbar gemacht oder an diese weitergegeben werden (Quelle: ISO 7498-2)
Vorbeugungsmaßnahme	Maßnahme zur Beseitigung der Ursache eines möglichen Fehlers oder einer anderen möglichen unerwünschten Situation (Quelle: ISO 9000)
Wirksamkeit	Ausmaß, in dem geplante Tätigkeiten verwirklicht und geplante Ergebnisse erreicht werden (Quelle: ISO 9000)
Ziel	Ressource, auf die von einem Anwärter zugegriffen wird (Quelle: DIN EN ISO 22600-1)
Zugriffskontrolle	Sicherung, dass ausschließlich autorisierte Entitäten auf zugriffsberechtigte Weise Zugang zu Ressourcen eines Datenverarbeitungssystems haben (Quelle: ISO/IEC 2382-8)
Zugriffssteuerung	Mittel zur Sicherstellung, dass nur autorisierte Entitäten in entsprechend autorisierter Weise Zugriff auf die Ressourcen eines Datenverarbeitungssystems nehmen können (Quelle: ISO/IEC 2382-8)
Zurechenbarkeit	Eigenschaft, durch die sichergestellt wird, dass die Aktionen einer Entität eindeutig auf diese zurückgeführt werden können (Quelle: ISO 7498-2)

12 Literatur

12.1 Bücher

1) Bollhöfer E. Schutz von Unternehmensdaten bei der Erbringung von E-Services. Springer Verlag. 1. Auflage 2017. ISBN 978-3-658-18485-8
2) Buchsein R, Victor F, Günther H, Machmeier V. IT-Management mit ITIL®V3. Vieweg & Sohn Verlag. 1. Auflage 2007. ISBN 978-3-8348-0270-5
3) Erben M. (Hrsg.) Allgemeine Geschäftsbedingungen - IT-Verträge wirksam vereinbaren. Gabler Verlag. 1. Auflage 2011. ISBN 978-3-8349-2908-2
4) Erben M, Günther W. Gestaltung und Management von IT-Verträgen. Springer-Verlag. 3. Auflage 2017. ISBN 978-3-662-54305-4
5) Holtbrügge D, Holzmüller H, v. Wangenheim F. (Hrsg.) Remote Services. Deutscher Universitäts-Verlag. 1. Auflage 2007. ISBN 978-3-8350-0678-2
6) Kunkel C. Vertragsgestaltung - Eine methodisch-didaktische Einführung. Springer-Verlag. 1. Auflage 2016. ISBN 978-3-662-48430-2
7) Olbrich A. ITIL kompakt und verständlich. © Vieweg+Teubner Verlag. 4. Auflage 2008. ISBN 978-3-8348-0492-1
8) Piller E. Beschaffung unter Berücksichtigung der IT-Sicherheit. Springer Verlag. 1. Auflage 2017. ISBN 978-3-658-18598-5
9) Witte F. Testmanagement und Softwaretest. Springer Verlag 2016. ISBN 978-3-658-09963-3

12.2 Internet

1) Bayerische Landesbeauftragte für den Datenschutz. Wartung, Fernwartung und Fernsteuerung. Stand 2008 [Online, zitiert am 2017-11-18]; Verfügbar unter https://www.datenschutz-bayern.de/technik/orient/mainwtg.htm
2) Bundesärztekammer: Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis. Stand 2014 [Online, zitiert am 2017-11-18]; Verfügbar unter http://www.bundesaerztekammer.de/richtlinien/empfehlungenstellungnahmen/schweigepflicht datenschutz/; Technische Anlage, Kap. 10 „Fernwartung“
3) Diözesandatenschutzbeauftragte der Erzbistümer Berlin und Hamburg, der Bistümer Hildesheim, Magdeburg, Osnabrück und des Bischöflich Münsterschen Offizialats in Vechta i.O. Mustervertrag zur Fernwartung. Stand 2011 [Online, zitiert am 2017-11-18]; Verfügbar unter https://www.datenschutz-kirche.de/sites/default/files/MV_Fernwartung.pdf
4) Hessische Datenschutzbeauftragte. Mustervertrag zur Fernwartung. Stand 2003 [Online, zitiert am 2017-11-18]; Verfügbar unter https://www.datenschutz.hessen.de/mustervertrag_fernwartung.htm
5) Landesbeauftragte für Datenschutz und Informationsfreiheit Bremen. Formulierungshilfen für einen Mustervertrag zur Fernwartung zwischen öffentlichem Auftraggeber und öffentlichem oder nicht-öffentlichem Auftragnehmer. Stand 2012 [Online, zitiert am 2017-11-18]; Verfügbar unter https://ssl.bremen.de/datenschutz/sixcms/media.php/13/2012-01-25-Mustervertrag_Fernwartung.pdf
6) Landesbeauftragte für den Datenschutz Niedersachsen. Orientierungshilfe Fremd- und Fernwartung. Stand 2009 [Online, zitiert am 2017-11-18]; Verfügbar unter https://www.lfd.niedersachsen.de/download/32309/Orientierungshilfe_Fremd-_und_Fernwartung_LfD_Niedersachsen_.pdf

7) Landesbeauftragten für den Datenschutz Baden-Württemberg. Fernwartung. Stand 1998 [Online, zitiert am 2017-11-18]; Verfügbar unter https://www.baden-wuerttemberg.datenschutz.de/fernwartung/

12.3 Normen

1) ISO/TR 11633-1: Informationssicherheitsmanagement für die Fernwartung für Medizinprodukte und Informationssysteme im Gesundheitswesen - Teil 1: Anforderungen und Risikoanalyse (Stand 2009-11)
2) ISO/TR 11633-2: Informationssicherheitsmanagement für die Fernwartung für Medizinprodukte und Informationssysteme im Gesundheitswesen - eil 2: Implementierung eines ISMS (Stand 2010-03)

12.4 Zeitschriften

1) Bischof E, Intveen M. (2016) Neue EVB-IT Musterverträge der öffentlichen Hand für die Beschaffung und Pflege von Standardsoftware: EVB-IT Pflegevertrag S. ITRB: 17-23
2) Bischof E, Intveen M. (2017) eue EVB-IT Musterverträge der öffentlichen Hand für die Beschaffung und Instandhaltung von Hardware: Kauf und Instandhaltung. ITRB: 119-127
3) Hoppen P. (2015) Software-Anforderungsdokumentation. CR : 747-760
4) Intveen M. (2001) Fernwartung von IT-Systemen. ITRB: 251-252
5) Intveen M. (2015) Der EVB-IT Servicevertrag. ITRB: 47-50
6) Intveen M. (2015) Verträge über Einrichtung, Betrieb und Wartung von Telekommunikationssystemen. ITRB: 262-265
7) Kiesche E., Wilke M. (2008) Fernwartungsprogramme und Remote-control-Systeme. CuA: 6-10
8) Kremer, S, Sander S. (2015) Der EVB-IT Systemvertrag – doch kein (einheitlicher) Werkvertrag? CR: 146-153
9) Kremer, S, Sander S. (2015) Individuelle Änderungen von EVB-IT Verträgen und Ergänzungen mittels AGB. ITRB: 24-27
10) Poder H, Petri JH. (2016) Technische No-Spy-Klausel in den novellierten EVB-IT-Verträgen. ITRB: 133-137
11) Schierbaum B. (2005) Datenschutz bei Auftragsdatenverarbeitung, Wartung und Fernwartung. Compuer-Fachwissen: 4-8
12) Von Beckerath M. (2017) Veränderte Bedingungen bei IT-Outsourcingverträgen. ITRB: 267-271
13) Witzel M. (2017) Risiken und Fallstricke unvollständiger Leistungsbeschreibungen bei Outsourcing. CR: 557-563