Fernwartung und Datenschutz

Dr. Bernd Schütze

36. Sitzung der GMDS-AG „Datenschutz und IT-Sicherheit im Gesundheitswesen“ (DIG)

Vita

HEALTHCARE SOLUTIONS

Deutsche Telekom Healthcare and Security Solutions GmbH
Dr. Bernd Schütze
Senior Experte Medical Data Security

☎ +49 (160) 9566 - 3145
Bernd.Schuetze@T-Systems.com

Studium

- Informatik (FH-Dortmund)
- Humanmedizin (Uni Düsseldorf / Uni Witten/Herdecke)
- Jura (Fern-Uni Hagen)

Ergänzende Ausbildung

- Datenschutzbeauftragter (Ulmer Akademie für Datenschutz und IT-Sicherheit)
- Datenschutz-Auditor (TüV Süd)
- Medizin-Produkte-Integrator (VDE Prüf- und Zertifizierungsinstitut)

Berufserfahrung

- Über 10 Jahre klinische Erfahrung
- Mehr als 20 Jahre IT im Krankenhäusern
- > 20 Jahre Datenschutz im Gesundheitswesen

Mitarbeit in wiss. Fachgesellschaften

- Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V. (GMDS)
- Gesellschaft für Datenschutz und Datensicherung e.V. (GDD)
- Gesellschaft für Informatik (GI)

Mitarbeit in Verbänden

- Berufsverband der Datenschutzbeauftragten Deutschlands e.V. (BvD)
- Berufsverband Medizinischer Informatiker e.V. (BVMI)
- Fachverband Biomedizinische Technik e.V. (fbmt)
- HL7 Deutschland e.V.
- HE Deutschland e.V.

Agenda

Fernwartung unter der DS-GVO

- Motivation
- Fällt Fernwartung unter die DS-GVO?
- Anforderungen (?)
- Beispiel: Fragestellung TeamViewer
- Vorhandene Anleitungen ausreichend ?

Motivation

Motivation

Warum mit dem Thema beschäftigen: Erhaltene Anfragen

Diverse Anfragen:

- BDSG „fällt weg“, also Fernwartung kein Datenschutzthema mehr?
- Darf Produkt „xy“ zur Fernwartung eingesetzt werden?
  (Insbesondere TeamViewer® der Firma TeamViewer GmbH wurde häufiger genannt)
- Ist Cisco WebEx® von WebEx Communications Deutschland GmbH für Tumorkonferenz nutzbar?

➔ Insgesamt scheinbar eine Unsicherheit, wie mit dem Thema umgegangen werden soll.

Fällt Fernwartung unter die DS-GVO?

Fällt Fernwartung unter die DS-GVO?

Grundsätzliches

- §11 Abs. 5 BDSG in der Fassung der Bekanntmachung vom 14. Januar 2003 mit Änderung vom 30.6.2017 fällt weg
- Damit keine spezielle gesetzliche Vorgabe mehr
- Für jede Verarbeitung i. S. d. DS-GVO wird ein Erlaubnistatbestand benötigt
- Entscheidungskriterium
  - Erfolgt bei Wartung/Fernwartung eine Verarbeitung (z.B. „Sichtung“) personenbezogene Daten i.S. d. Art. 4 Ziff. 1 DS-GVO?
- Zu beachten:
  - Auftragsverarbeitung: Keine Verarbeitung durch Dritte
  - Keine Auftragsverarbeitung: Verarbeitung durch Dritte
    - → Verarbeitende Stelle (= wartende/fernwartende Stelle) = Verantwortlicher i.S. d. DS-GVO
    - → Auftraggeber benötigt erlaubnistatbestand für Verarbeitung (= Datenweitergabe)
    - → Auftragnehmer benötigt eigenen Erlaubnistatbestand für Verarbeitung

Fällt Fernwartung unter die DS-GVO?

„Allgemeine“ Daten

- Grundsätzlich Art. 6 DS-GVO bzgl. Rechtmäßigkeit der Verarbeitung anzuwenden
- Art. 6 Abs. 1 lit. f DS-GVO
  - „die Verarbeitung ist zur Wahrung der **berechtigten Interessen des Verantwortlichen** oder eines Dritten **erforderlich**, sofern **nicht** die **Interessen oder Grundrechte** und Grundfreiheiten der **betroffenen Person**, die den Schutz personenbezogener Daten erfordern, **überwiegen**, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.“
- Interessenabwägung erforderlich
  - Grundsätzlich ist Interesse des Verantwortlichen an Wartung/Fernwartung seiner Systeme berechtigt
  - Überwiegt das Interesse des Verantwortlichen → Erlaubnistatbestand zur Weitergabe an mit der Wartung/Fernwartung beauftragtes Unternehmen
  - Interesse des mit der Wartung/Fernwartung beauftragtes Unternehmens i.d.R. auch berechtigt → i.d.R. wird Interesse der betroffenen Person aber überwiegen, daher kein Erlaubnistatbestand zur Verarbeitung der Daten

➔ Ggf. Erlaubnistatbestand für Datenweitergabe an Dritten (Auftragnehmer) vorhanden

➔ Für Verarbeitung der Daten durch Auftragnehmer vermutlich kein Erlaubnistatbestand vorhanden

➔ Einwilligung? Kaum möglich: wenn eine Person nicht einwilligt, ...

Fällt Fernwartung unter die DS-GVO?

Besondere Kategorien personenbezogener Daten

- Erlaubnistatbestand Art. 9 DS-GVO
- Interessenabwägung existiert nicht als Erlaubnistatbestand

➔ Auftraggeber fehlt Erlaubnistatbestand zur Weitergabe von Daten an einen Dritten

➔ Auftragnehmer fehlt Erlaubnistatbestand zur Verarbeitung der Daten

Fällt Fernwartung unter die DS-GVO?

Sozialdaten

- §35 Abs. 2 SGB I-neu
  - Die Vorschriften des Zweiten Kapitels des Zehnten Buches und der übrigen Bücher des Sozialgesetzbuches regeln die Verarbeitung von Sozialdaten abschließend, soweit nicht DS-GVO unmittelbar gilt.

  ➔ Abschließende Regelung im SGB
- § 80 Abs. 3,5 SGB X-neu

  (3) Die Erteilung eines Auftrags zur Verarbeitung von Sozialdaten durch nicht-öffentliche Stellen ist nur zulässig, wenn

  1. 1. beim Verantwortlichen sonst Störungen im Betriebsablauf auftreten können oder
  2. 2. die übertragenen Arbeiten beim Auftragsverarbeiter erheblich kostengünstiger besorgt werden können.

  (5) Absatz 3 gilt nicht bei Verträgen über die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag, bei denen ein Zugriff auf Sozialdaten nicht ausgeschlossen werden kann. Die Verträge sind bei zu erwartenden oder bereits eingetretenen Störungen im Betriebsablauf unverzüglich der Rechts- oder Fachaufsichtsbehörde mitzuteilen.

➔ „Alte“ Regelung bleibt bestehen

Fällt Fernwartung unter die DS-GVO?

Antwort: „Kommt darauf an“ ;-)

- Erfolgt während Wartung/Fernwartung ein Zugriff auf personenbezogene Daten
  - sei es geplant oder ungeplant,
  - sei es nur „ausnahmsweise“,
  - und sei der Zugriff so kurz wie möglich,

  so erfolgt eine Verarbeitung im Sinne der DS-GVO.

➔ In diesem Fall gelten alle Regelungen der DS-GVO.

➔ Kann ein Zugriff auf personenbezogene Daten während Wartung/Fernwartung nicht sicher ausgeschlossen werden

- Regelungen der DS-GVO für Wartung/Fernwartung vorsehen
- Insbesondere Vertrag zur Auftragsverarbeitung abschließen

Anforderungen (?)

Anforderungen der DS-GVO

Stichwort: Sicherheit der Verarbeitung

- Besondere Kategorien von Daten: Datenschutz-Folgenabschätzung Art. 35)
- Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25)
- Sicherheit der Verarbeitung (Art. 32)

(siehe Folien TOM)

Anforderungen aus Art. 32

Stichwort: „Stand der Technik“

ISO/TR 11633-1: Informationssicherheitsmanagement für die Fernwartung für Medizinprodukte und Informationssysteme im Gesundheitswesen - Teil 1: Anforderungen und Risikoanalyse (Stand 2009-11)

- Grundsätzliches (Kap. 4.1)
  - Kap. 4.1.2. “Remote maintenance services using a public switched telephone network” heute vermutlich eher selten im Einsatz
  - Kap. 4.1.2.2 Remote maintenance services using the Internet
    - Firewall
    - Tools wie Anti-Virus-Software
    - Nutzung von VPN zur verschlüsselten Kommunikation
    - Bei Authentifizierung Nutzung mehrerer Schutzmöglichkeiten wie one-time passwords, Password-Verschlüsselung und digitaler Zertifikate
- Sicherheitsanforderungen (Kap. 4.2)
  - Kap. 4.2.2: Vertrag zwischen Auftraggeber und Auftragnehmer
  - Kap. 4.2.3: Schutz personenbezogener Daten
- Risikoanalyse (Kap. 6)

Anforderungen aus Art. 32

Stichwort: „Stand der Technik“

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

- Sicherheitskonzept (Kap. 4.3)
- Risikoanalyse (Kap. 4.4)
- Risikomanagement (Kap. 4.5)
- Sicherheitsaudit (Kap. 7)

Anforderungen aus Art. 32

Stichwort: „Stand der Technik“

- ISO/TR 11633-1: knapp 20 Seiten
- ISO/TR 11633-2: knapp 70 Seiten

} Zusätzlich Nutzung anderer Normen erforderlich

Sicherheit der Verarbeitung

Gewährleistung der Sicherheit der Verarbeitung

- ISO/TR 11633-1: knapp 20 Seiten
- ISO/TR 11633-2: knapp 70 Seiten

} Zusätzlich Nutzung anderer Normen erforderlich

Z.B.

- DIN ISO IEC 27002
- DIN EN ISO 27799
- BSI IT-Grundschutz: M 5.33 Absicherung von Fernwartung*

➔ Sind die Hilfen für Krankenhäuser/Arztpraxen wirklich nutzbar?

- Bundesärztekammer: Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis
  - Stand 2014 (http://www.bundesaerztekammer.de/richtlinien/empfehlungenstellungnahmen/schweigepflichtdatenschutz/)
  - Technische Anlage, Kap. 10 „Fernwartung“: ¼ Seite, Checkliste 8 Fragen

➔ Ist das hinreichend konkret für den täglichen Einsatz?

* https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05033.html

Anforderungen seitens deutscher Aufsichtsbehörden

Andere „Anleitungen“

- Landesbeauftragte für Datenschutz und Informationsfreiheit Bremen
  - Formulierungshilfen für einen Mustervertrag zur Fernwartung zwischen öffentlichem Auftraggeber und öffentlichem oder nicht-öffentlichem Auftragnehmer
  - Stand 2012, https://ssl.bremen.de/datenschutz/sixcms/media.php/13/2012-01-25-Mustervertrag_Fernwartung.pdf
- 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, https://www.datenschutz-kirche.de/sites/default/files/MV_Fernwartung.pdf
- Landesbeauftragte für den Datenschutz Niedersachsen
  - Orientierungshilfe Fremd- und Fernwartung
  - Stand 2009, https://www.lfd.niedersachsen.de/download/32309/Orientierungshilfe_Fremd-_und_Fernwartung_LfD_Niedersachsen_.pdf
- Bayerische Landesbeauftragte für den Datenschutz
  - Wartung, Fernwartung und Fernsteuerung
  - Stand 2008, https://www.datenschutz-bayern.de/technik/orient/mainwtg.htm
- Hessische Datenschutzbeauftragte
  - Mustervertrag zur Fernwartung
  - Stand 2003, https://www.datenschutz.hessen.de/mustervertrag_fernwartung.htm
- Landesbeauftragten für den Datenschutz Baden-Württemberg
  - Fernwartung
  - Stand 1998, https://www.baden-wuerttemberg.datenschutz.de/fernwartung/

Beispiel: Fragestellung TeamViewer

TeamViewer

Erkennung des Fernzugriffs

- TeamViewer kann durch entsprechende Einstellungen in der Windows-Registry als Hintergrundprozess vom Nutzer vollständig unbemerkt mit dem Systemstart gestartet werden.
  - In diesem Fall erscheint auch kein TeamViewer Icon im System-Tray (alle Icons, bis auf die Urzeit werden ausgeblendet).
  - Erst beim Fernzugriff selbst erscheint ein kleines Fenster.
  - Dieser Fernzugriff ist mittels der TeamViewer-Host-Version auch ohne eine aktive Handlung des Nutzers möglich, wenn der Zugreifende das Passwort kennt, was regelmäßig der Fall ist, wenn dieser den TeamViewer-Host eingerichtet hat.
  - ➔ Somit ist mittels TeamViewer auch ein unbeaufsichtigter Zugriff auf den Rechner des Nutzers, z.B. in dessen Abwesenheit, möglich.

TeamViewer

Mitarbeitervertretung: Einsatz TeamViewer mitbestimmungspflichtig?

- 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)
- Ein unbeaufsichtigter Fernzugriff durch den Arbeitnehmer ist möglich.
  - Leistungsüberwachung möglich (z.B. mittels Screenshots in regelmäßigen Abständen)
  - Somit können mittels TeamViewer Aussagen über das Verhalten und die Leistung der Arbeitnehmer getroffen werden, weshalb die objektive Eignung vorliegt.
  - Mithin ist TeamViewer auch dazu bestimmt i.S . d. § 87 Abs. 1 Nr. 6 BetrVG das Verhalten oder die Leistung der Arbeitnehmer zu überwachen.

  ➔ Einsatz ist Mitbestimmungspflichtig

TeamViewer

Beschäftigtenverhältnis und Datenschutz

Wird TeamViewer innerhalb des Beschäftigtenverhältnisses eingesetzt, ist die datenschutzrechtliche Berechtigung zu klären.

- § 32 BDSG kann mögliche Rechtsgrundlage darstellen.
  - TeamViewer dürfte nicht zur „Durchführung“ eines Beschäftigungsverhältnisses erforderlich sein, wie es § 32 BDSG fordert. Daher scheidet §32 BDSG aus.
- §28 Abs. 1 Nr. 2 BDSG: berechtigtes Interesse
  - Eine effektive und zeitnahe Bearbeitung von IT-Problemen über eine Fernwartungssoftware kann durchaus als berechtigtes Interesse 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.

TeamViewer

Ort der Datenverarbeitung

- Seit Mai 2014 gehört TeamViewer Permira, laut Handelsblatt sucht Pemira derzeit einen Käufer*.
- Da TeamViewer keine eigenen Server erlaubt, erfolgt jegliche Kommunikation und jede Anmeldung über die Server der Firma. Setzt ein Dienstleister TeamViewer zur Wartung seiner Produkte bei einem Kunden ein,
  1. Muss dies vom Kunden genehmigt werden
  2. Im Auftragsverarbeitungsvertrag zwischen Kunden und Dienstleister vereinbart werden
  3. Ein Auftragsverarbeitungsvertrag zwischen Dienstleister und TeamViewer-Firma existieren, in welchem die Anforderungen des AV-Vertrages zwischen Dienstleister und Kunden weitergereicht werden (Unterauftragsverhältnis)
  4. Beschäftigte müssen darüber informiert werden, dass ihre Daten ggf. an Dritte weitergegeben werden.
  5. Liegen die Server in einem Drittland, sind Artt. 40-49 DS-GVO zu beachten

*http://www.handelsblatt.com/my/unternehmen/it-medien/teamviewer-deutsche-softwarefirma-koennte-milliarden-einbringen/20120478.html?ticket=ST-271343-PpFYQFkFWMGrvwavhJCN-ap3

TeamViewer

Sicherheitslücken

- 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)
- Bekannte Vorfälle aus der Vergangenheit
  - Juni 2016 wurde z.B. bekannt, dass Accounts gehackte wurden.
  - Hacker missbrauchen TeamViewer (Meldung von Kaspersky 2013, "TeamSpy").
  - TeamViewer stand im Verdacht, Trojaner zu verbreiten (Meldung von TrendMicro, 2016).

➔ Wie genügt der Auftragnehmer seiner Informationspflicht gegenüber dem Auftraggeber bzw. den betroffenen Beschäftigten?

TeamViewer

Auswertung

- TeamViewer wendet sich an z.T. an Nutzer der Software und fordert sie auf, die Software zu kaufen, da sie die Software offensichtlich für kommerzielle Zwecke einsetzen.
- D.h. in irgendeiner Form erfolgt auch eine Auswertung der Sessions.

➔ Wie genügt der Auftragnehmer seiner Informationspflicht gegenüber dem Auftraggeber bzw. den betroffenen Beschäftigten?

TeamViewer

Sicherheit der Verarbeitung

- Die von TeamViewer angegebenen kryptographischen Verfahren RSA-2048, AES-256 und SRP entsprechen jedes für sich genommen dem Stand der Technik.
  - In den der Öffentlichkeit zur Verfügung stehenden Unterlagen ist jedoch nicht beschrieben, wie sichergestellt wird, dass der vom Masterserver übermittelte öffentliche Schlüssel tatsächlich zum vermuteten Kunden oder Dienstleister gehört.
  - Dienstleister und Kunde können dies nicht anhand weiterer Informationen, beispielsweise mit Zertifikaten von unabhängigen Stellen, prüfen.
  - Sie sind in diesem Punkt vollständig auf den Hersteller von TeamViewer angewiesen.
  - ➔ Bei Anwendungen mit hohem Schutzbedarf, wie es die Verarbeitung von Gesundheitsdaten darstellt, ist dies nicht hinnehmbar; es entspricht nicht dem Stand der Technik.

Vorhandene Anleitungen ausreichend ?

Vorhandene Lösungen (?)

Erinnerung an Motivation: Darf ich „xy“ nutzen?

- Fragen der Anwender (Beispiel TeamViewer®) werden durch die existierenden Papiere nicht beantwortet-
  - Weder die Darstellungen der Aufsichtsbehörden noch die Normen und auch nicht die Empfehlung der KBV sind detailreich genug, um sie als „Whitepaper“ für Fernwartung im deutschen Gesundheitsmarkt zu nutzen
  - Papiere der Aufsichtsbehörde adressieren überwiegend den daten**schutzrechtlichen** Teil, nicht den datenschutz**informationstechnischen** Bereich.
  - ISO/TR 11633 bleibt bzgl. Anforderungen sehr allgemein

➔ Sollen wir das Thema aufgreifen und konkretisieren? Z.B.

- Wer darf Wartung initiieren?
- Erforderliche Protokollierung
- Verschlüsselung der Verbindung
- Vorgehen bei Meldungen / Störungsentgegennahme, u.a.
  - Patientendaten in E-Mails
  - Datendump inkl. Patientendaten wird an Hersteller geschickt
- Verarbeitung in Deutschland/EU/Weltweit – was ist wann zu beachten?
- Evtl. Ergänzungen zu EVB-IT Pflegevertrag

Diskussion

Kontakt: Bernd.Schuetze@T-Systems.com