Kurzgutachten zur Erteilung eines Datenschutzgütesiegels für das IT-Produkt „e-pacs Speicherdienst“

im Auftrag der Telepaxx Medical Archiving GmbH

datenschutz cert GmbH

11. Dezember 2017

Inhaltsverzeichnis

1. Über dieses Kurzgutachten

Mit diesem Kurzgutachten werden die Ergebnisse der Auditierung des IT-Produkts „e-pacs Speicherdienst“ in der Version 3.0 die Firma Telepaxx Medical Archiving GmbH zusammengefasst. Das IT-Produkt wurde erstmals am 27.05.2003 erfolgreich gemäß der Datenschutzgütesiegelverordnung (DSGSVO)[1] vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein zertifiziert und wurde seit dem regelmäßig re-zertifiziert.

Die Telepaxx Medical Archiving GmbH hat am 23.09.2017 eine Selbsterklärung abgegeben, in der vermerkt wird, dass das Produkt e-pacs weiterhin in der unveränderten Version 3.0 eingesetzt wird. Änderungen betreffen dabei die Aktualisierung der eingesetzten Betriebssysteme der Einsatzumgebung sowie die Online-Spiegelung der Daten in einem Rechenzentrum in Hamburg. Die Selbsterklärung wird diesem Gutachten als **Anlage A** beigefügt.

2. Zeitraum der Prüfung

Die Begutachtung des e-pacs Speicherdienstes erstreckte sich auf den Zeitraum von 12.09. bis 03.11.2017 und beinhaltete die konzeptionelle Analyse der zur Verfügung gestellten Dokumente, der Befragung von Projektverantwortlichen, die Durchführung von Plausibilitäts- und Funktionstests sowie eine Begehung des Rechenzentrums der Telepaxx Medical Archiving am Standort Wasserrunzel 5, 91186 Büchenbach.

3. Antragstellerin

Antragstellerin ist die Telepaxx Medical Archiving GmbH, Wasserrunzel 5, 91186 Büchenbach als Betreiber des e-pacs Speicherdienstes. Ansprechpartner ist Herr Andreas Dobler.

4. Sachverständiger/Prüfstelle

Sachverständige dieses Gutachtens ist die Prüfstelle

datenschutz cert GmbH
Konsul-Smidt-Str. 88a
28217 Bremen

unter der Leitung von Herrn Dr. Sönke Maseberg (Technik) und Frau Irene Karper (Recht). Ansprechpartner für diese Begutachtung sind Frau Dr. Irene Karper (Recht) und Alexey Testsov (Technik).

5. Kurzbezeichnung des IT-Produkts

Begutachtet wurde das Produkt „e-pacs Speicherdienst“ Version 3.0.

6. Beschreibung des IT-Produkts

e-pacs Speicherdienst Version 3.0 besteht unverändert aus den Produktkomponenten:

--- e-pacs Department Server
--- Deep Storage Server
--- Blowfish-Routinen mit Schlüssellängen von 256 Bit

[1] Landesverordnung über ein Datenschutzgütesiegel (Datenschutzgütesiegelverordnung – DSGSVO) v. 30.11.2013, GVOBl. Schl.-H. 2013, S.536ff. Sie ersetzt seit dem 01.01.2014 die Datenschutzauditverordnung.

Die Einsatzumgebung wird stets auf dem neuesten Patch-Stand gehalten. Der Stand zum Auditzeitpunkt stellte sich wie folgt dar:

--- Windows 2012 R2 mit aktuellem Servicepack

--- Datenbank SQL Server 2012 R2 und SQL Server 2014 mit aktuellem Service Pack sowie PostgreSQL 9.0 und 9.3

--- VPN auf Basis von SSH mit RSA und einer Schlüssellänge von 2048 Bit

Sämtliche Produktkomponenten sowie die Komponenten der Einsatzumgebung entsprechen dem aktuellen Stand der Technik und gewährleisten auf diese Weise die Sicherheit der Daten.

7. Tools, die zur Herstellung des Produkts verwendet wurden

Keine.

8. Zweck und Einsatzbereich

e-pacs dient der Archivierung von Röntgenbildern. Das IT-Produkt besteht aus zwei Komponenten: dem lokalen e-pacs Department-Server beim Kunden einerseits und einem dedizierten externen Deep Storage Server beim Archivar andererseits. Zwischen diesen werden die Daten über eine bestehende Netzinfrastruktur verschlüsselt übertragen.

Beim Radiologen oder Krankenhaus wird ein Department-Server installiert, der für den Kunden den Zugang zu e-pacs darstellt. Der Department-Server stellt dem behandelnden Arzt die lokal zu bearbeitenden radiologischen Bilddaten zur Verfügung. Die Schnittstelle zwischen Department-Server und Praxis-EDV bildet der DICOM-Standard, so dass die aktuelle radiologische Medizintechnik angebunden werden kann. Zugleich übernimmt der Department-Server für die Kommunikation mit dem Storage-Server im Rechenzentrum der Telepaxx Medical Archiving GmbH (kurz: Telepaxx) die Datenverschlüsselung, das Prioritätenmanagement, die Transportüberwachung und die Transaktionssicherung.

Gegenstück zum Department-Server ist der Deep Storage Server, der die kundenbezogene Archivierung sowie das eigentliche Backup bzw. Recovery übernimmt. In diesem externen Archiv wird für jeden Kunden eine dedizierte Datenhaltung geführt, bestehend aus eigener Datenbank und eigenem Datenträgerpool.

Die Datenlogistik besteht im Wesentlichen aus den Teilen Speicherung und Retrieval.

Bei der Speicherung werden medizinische Daten und Bilder zunächst lokal auf dem Department-Server gespeichert. Parallel hierzu werden sie zunächst lokal komprimiert, lokal verschlüsselt und anschließend an den externen Storage-Server geschickt und dort weiterhin verschlüsselt auf Datenbändern gespeichert. Jede verschlüsselte Datei erhält hierzu eine eindeutige Archiv-ID, die keinen Patientenbezug aufweist. Zeitnah wird eine weitere Sicherungskopie auf Band erzeugt; dieses wird an einem sicheren dritten Ort gelagert.

Beim Retrieval werden die medizinischen Daten in umgekehrter Reihenfolge vom externen Archiv zum Department-Server übertragen. Dort werden die Bilddaten wieder entschlüsselt, dekomprimiert und dem jeweiligen Patienten zugeordnet.

Die zu archivierende Datei wird vollständig komprimiert und mit einem kundenspezifischen Key verschlüsselt. Dieser Schlüssel ist auf einem Hardware-Zertifikatsspeicher (e-Token)

gespeichert, der nicht Gegenstand des zu auditierenden Produkts ist. Zur Verschlüsselung kommt das Blowfish-Verfahren zum Einsatz.

Die Sicherheit von e-pacs ist nicht nur von Sicherheitsmechanismen geprägt, die Bestandteil des eigentlichen Produkts sind, sondern ist auch von der Sicherheit der bestehenden Einsatzumgebung abhängig. Hierzu gehören eine IPSec-Verschlüsselung, clientseitig realisiert durch einen Router, serverseitig durch ein IPSec-Gateway, eine serverseitige Firewall, einen clientseitigen Paketfilter, ein Hardware-Token bzw. Zertifikat für jeden Kunden (Radiologiepraxis, Krankenhaus), einen CA-Server zur Generierung von IPSec-Zertifikaten sowie diebstahlgesicherte Serverräume des Archivars.

Die Einsatzumgebung wird ausschließlich von Telepaxx konfiguriert, d.h. es werden von der Telepaxx Releasewechsel validiert und erst dann beim Kunden in Betrieb genommen. Hierfür hält die Telepaxx eine komplette Kundenkonfiguration der Einsatzumgebung zu Testzwecken vor. Ein weiterer Vorteil besteht darin, dass der serverseitige Firewall, das IPSec-Gateway und der CA-Server auf Open Source Software basieren.

Die für e-pacs genutzten Serversysteme werden im Storage Center der Telepaxx in Büchenbach gehostet. Storage Center und alle Server des e-pacs sind in einer fensterlosen F90+ - Sicherheitszelle mit massiver Stahltüre betrieben. Der Zugang zum Storage Center ist durch eine Alarmanlage und ein Zugangskontrollsystem geschützt. Alle Zu- und Abgänge werden mit Datum und Uhrzeit protokolliert. Der Zugang zum Storage Center ist nur autorisierten Mitarbeitern der Telepaxx, die mit dem Operating betraut sind, sowie der Geschäftsführung möglich. Die Zelle ist mit Brandmeldeanlage, Löschanlage und Brandfrüherkennungsanlage ausgestattet. Alle Anlagen werden jährlich gewartet, Wartungsprotokolle wurde von dem Auditor gesichtet. Für die Alarmierung ist Monitoring Einheit Rittal CMC-TC angewendet, die alle wichtigen Parameter überwacht und an den Personal bei dem Bedarf weiterleitet.

Ferner setzt Telepaxx ein Rechenzentrum für die Platzierung von Servern und Speichersysteme ein. Das Rechenzentrum der Asklepios Kliniken in Hamburg, Rübenkamp 226 dient der reinen Online-Spiegelung der Daten. Es ist gemäß ISO/IEC ISO27001 durch die TÜV SÜD Management Service GmbH, Zertifikat Nr 12 310 49902 TMS, gültig bis 13.04.2018. Beim Einsatz des neuen Rechenzentrums handelt es sich nach Ansicht der Auditoren um ein Housing, da der Telepaxx vom Rechenzentrumsdienstleister ausschließlich ein Raum im Rechenzentrum zur Verfügung gestellt wird, zu dem der Dienstleister selbst keinen Zutritt hat. Dies wird sichergestellt durch die Tatsache, dass die relevanten Server und die Cages in dem Raum verschlossen sind und der Dienstleister keine Zugriffe auf die Schlüssel hat. Diese liegen ausschließlich in der Hand der Telepaxx. Es liegt somit faktisch keine Zugriffsmöglichkeit auf personenbezogene Daten vor. Eine Auftrags-daten-verarbeitung ist weiterhin nicht einschlägig.

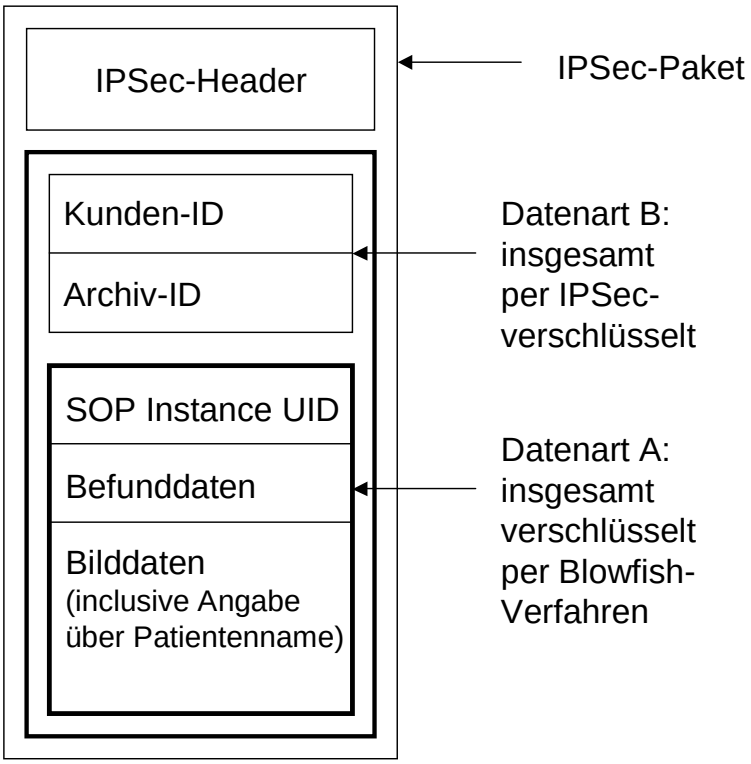
9. Modellierung des Datenflusses

Die archivierten Daten sind Bilddaten einschließlich Befunde nach DICOM-Standard. Folgende Datenarten wurden identifiziert:

Datenart A: Medizinische Daten, z.B. Röntgendaten mit oder ohne Befund und SOP Instance UID, die jedem Röntgenbild eindeutig zugeordnet wird (Primärdaten).

Datenart B: Die Headerinformationen auf Anwendungsebene bestehen lediglich aus zwei Daten. Mittels einer fortlaufenden Registriernummer (Archiv-ID) sowie einer Kundennummer werden die medizinischen Datensätze auf dem Datenbanksystem archiviert. Weitere Protokolldaten (u.a. Angaben über Speicherzeitpunkte) existieren auf dem Storage-Server zur Verwaltung und Revisionsfähigkeit des Archivs.

Die Struktur der verwendeten Daten wird in dem folgenden Container-Modell genauer deutlich.



10. Version des Anforderungskatalogs, die der Prüfung zugrunde gelegt wurde

Version 2

11. Zusammenfassung der Prüfergebnisse

Die Prüfergebnisse im Einzelnen werden wie folgt zusammengefasst:

Nr.	Anforderungsprofil	Bewertung / Kommentar
Datenart A (Primärdaten):		
A1	Verfügbarkeit, Integrität, Vertraulichkeit	angemessen
A2	Nicht-Verkettbarkeit	angemessen
A3	Transparenz	angemessen
A4	Intervenierbarkeit	angemessen
A5	Anpassung des IT-Produkts	angemessen

A6	Privacy by Default	angemessen
A7	Sonstige Anforderungen	Nicht anwendbar
A8	Zulässigkeit der Datenverarbeitung	angemessen
A9	Einhaltung allg. Datenschutzgrundsätze	angemessen
A10	Datenverarbeitung im Auftrag	angemessen
A11	Besondere technische Verfahren	angemessen
A12	Sonstige Anforderungen	Nicht anwendbar
A13	Einzelne technisch-organisatorische Maßnahmen	angemessen
A14	Allgemeine Pflichten	angemessen
A15	Spezifische Pflichten	angemessen
A16	Pflichten nach DSVO	angemessen
A17	Betrieb der Auftragsdatenverarbeitung	angemessen
A18	Sonstige Anforderungen	Nicht anwendbar
A19	Aufklärung und Benachrichtigung	angemessen
A20	Benachrichtigung bei unrechtmäßiger Kenntniserlangung	angemessen
A21	Auskunft	angemessen
A22	Berichtigung, Löschung, Sperrung, Einwand bzw. Widerspruch, Gegendarstellung	angemessen
A23	Sonstige Anforderungen	Nicht anwendbar
Datenart B (Sekundärdaten):		
B1	Datenvermeidung und Datensparsamkeit	angemessen
B2	Zweckbindung	angemessen
B3	Nicht-Verkettbarkeit	angemessen
B4	Transparenz	angemessen
B5	Rechtsgrundlagen	angemessen
B6	Zweckbindung	angemessen
B7	Aufbewahrungsfristen	angemessen
B8	Physikalische Sicherung	angemessen
B9	Zugriffsschutz	angemessen
B10	Ermittlung / Sichtbarkeit der Protokolldaten	angemessen
B11	Technische Umsetzung der Speicherfristen	angemessen

B12	Unzulässige Verkettung	angemessen
B13	Beschreibung der Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nicht-Verkettbarkeit und Intervenierbarkeit	angemessen
B14	Selektive Löschung von Einzeldaten, Beauskunftung, Berichtigung, Sperrung, Einwand	angemessen

12. Beschreibung, wie das IT-Produkt den Datenschutz fördert

Das IT-Produkt e-pacs zeichnet sich weiterhin datenschutzrechtlich dadurch aus, dass die medizinischen Daten während des gesamten Archivierungsprozesses – angefangen mit der Übertragung vom Department-Server zum Storage-Server bis hin zur Rückübertragung vollständig und für den Archivar in nicht nachvollziehbarer Weise verschlüsselt werden. Diese Art der anwendungsbezogenen Verschlüsselung ist diejenige datenschutzfördernde Maßnahme, die die meisten Sicherheits-anforderungen abdeckt. Die medizinischen Daten werden nicht nur vertraulich versendet und archiviert, es wird durch die Verschlüsselung auch die Integrität und Authentizität der Daten gewährleistet sowie ein Beschlagnahme-schutz sichergestellt.

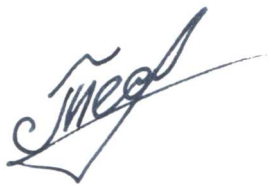
Ferner ist durch die Verwendung von pseudonymen Headerinformationen weder ein Rückschluss auf einzelne Patienten noch ein Rückschluss auf einzelne Kunden möglich, was die Vertraulichkeit sämtlicher Sekundärdaten gewährleistet.

13. Votum der Auditoren

Das IT-Produkt e-pacs Speicherdienst, Version 3.0, erfüllt weiterhin die Anforderungen an den Datenschutz und die Datensicherheit, da die verwendeten technischen Lösungen innovativ die Umsetzung der gesetzlichen Vorgaben ermöglichen.

Gegen eine Re-Zertifizierung bestehen aus Sicht der Auditoren keine Bedenken.

Bremen, 11.12.2017



Dr. Irene Karper LL.M.Eur.
datenschutz cert GmbH

Alexey Testsov
datenschutz cert GmbH