datenschutz cert

Telepaxx Medical Archiving GmbH
Mai 2013

Gutachten zur Re-Zertifizierung des Produktes „e-pacs Speicherdienst“

1. Gegenstand der Prüfung

Mit diesem Gutachten strebt die Firma Telepaxx Medical Archiving GmbH (ehemals Telepaxx Software GmbH) die Re-Zertifizierung des Produktes „e-pacs Speicherdienst“ in der Version 3.0 an. Das Produkt e-pacs wurde erstmals am 27.05.2003 erfolgreich gemäß der DSAVO vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein zertifiziert.

Grundlage der Prüfung ist der Anforderungskatalog des ULD in der Version 1.2.

Die Telepaxx Medical Archiving GmbH hat am 20.03.2013 eine Selbsterklärung abgegeben, in der vermerkt wird, dass das Produkt e-pacs Speicherdienst weiterhin in der unveränderten Version 3.0 eingesetzt wird. Die Selbsterklärung wird diesem Gutachten als Anlage 2 beigefügt.

Aufgrund der Tatsache, dass ein unverändertes Produkt re-zertifiziert werden soll, wird im Folgenden zu den Fragen Stellung genommen,

- inwieweit das unveränderte Produkt weiterhin dem Stand der Technik entspricht, dies gilt insbesondere für die dort verwendeten Verschlüsselungsmechanismen und Schlüssellängen,
- inwieweit die Einsatzumgebung noch auf einem aktuellen Sicherheits-Stand ist,
- inwieweit die an das Produkt zu stellenden Anforderungen unverändert geblieben sind.

2. Zeitpunkt der Prüfung

Die Auditierung des Produktes wurde im Zeitraum vom 20.03.-30.05.2013 durchgeführt.

3. Adresse der Antragstellerin

Antragstellerin dieses Gutachtens ist die Firma Telepaxx Medical Archiving GmbH (ehemals Telepaxx Software GmbH), Wasserrunzel 5, 91186 Büchenbach als Betreiber des e-pacs Speicherdienstes. Ansprechpartner ist Herr Andreas Dobler.

4. Adressen der Sachverständigen / der Prüfstelle

Sachverständige Prüfstelle ist die datenschutz cert GmbH, Konsul-Smidt-Straße 88a, 28217 Bremen. Ansprechpartner sind Frau Dr. Irene Karper (Recht) und Herr Ralf von Rahden (Technik).

5. Unveränderte Produktkomponenten

Das Produkt e-pacs Speicherdienst Version 3.0 besteht aus folgenden Produktkomponenten:

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

Die Einsatzumgebung setzt sich aus folgenden Komponenten zusammen und wird stets auf dem neuesten Patch-Stand gehalten:

- --- Windows 2008 Server SP2
- --- Firewall und VPN-gateway: zwei Juniper-Appliances, SSG140,
- --- MS-SQL Server 2008 R2 und aktuellem Service Pack
- --- VPN auf Basis von SSH mit RSA und einer Schlüssellänge von 2048 Bit
- --- CA-Server (generiert und signiert für Kunden X.509-Zertifikate mit einer Schlüssellänge von 2048 Bit)
- --- e-token der Firma Aladdin

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

Dies gilt insbesondere für die verwendeten Verschlüsselungsverfahren: Blowfish und RSA gelten **mit den genutzten Schlüssellängen als sichere Verschlüsselungsalgorithmen**; RSA wird mit einer Schlüssellänge von 2048 Bit gemäß der „Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen)“ Entwurf vom 12.12.2012 der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen - bis Ende 2019 und damit weit über den Ablauf des Zertifikats hinaus **als sicher eingestuft**.

6. Bewertung der Einsatzumgebung

Windows 2008 Server R2 sowie MS-SQL Server 2008 R2 werden nach wie vor von Microsoft mit Sicherheitsupdates supported (im extended support mindestens bis 2019 (MS-SQL) bzw. 2020 (MS server 2008)). Beide Systeme werden auf dem aktuellen Service Pack Stand gehalten. Es ist **in keiner Weise** eine Beeinträchtigung der Betriebssystem- und Datenbanksicherheit zu erwarten, da Sicherheitspatches für die Server stets zeitnah eingespielt werden.

Die Umstellung der Firewall und des VPN-Gateways auf eine Juniper-Lösung (Juniper SSG140, Hardware Version: 1010(0), Firmware Version: 6.2.0r6.0) erhöht die Sicherheit von e-pacs, da die bisherige Lösung mit FreeS/WAN und iptables nicht weiterentwickelt wird und somit nicht auf neue Bedrohungen reagieren könnte. **Die jetzige Lösung ist auf dem aktuellen Stand der Technik**.

7. Weitgehend unveränderte Rechtsgrundlagen

Bei der Bewertung des e-pacs Speicherdienstes wurden bei den vorherigen Begutachtungen folgende Rechtsnormen als Bewertungsmaßstab hinzugezogen:

--- Bundesdatenschutzgesetz
--- Landesdatenschutzgesetz Schleswig-Holstein
--- Röntgenverordnung
--- Musterberufsordnung der Ärzte

Die genannten Gesetze haben in der Zwischenzeit **keine für das Produkt e-pacs Speicherdienst relevanten Veränderungen** erfahren.

Insgesamt ergeben sich demnach keine Veränderungen im Hinblick auf die rechtlich einschlägigen Rahmenbedingungen des e-pacs Speicherdienstes und kein Bedarf an einer Änderung des seinerzeit zugrunde gelegten Anforderungsprofils.

8. Zusammenfassung

Das Produkt e-pacs Speicherdienst in der Version 3.0 erfüllt weiterhin die Anforderungen an den Datenschutz und die Datensicherheit in besonderer Weise, da die verwendeten technischen Lösungen innovativ die Umsetzung der gesetzlichen vorgaben ermöglichen. Gegen eine Re-Zertifizierung bestehen keine Bedenken.

Bremen, 30.05.2013

Irene Karper LL.M.Eur.
datenschutz cert GmbH

Ralf von Rahden
datenschutz cert GmbH