datenschutz nord

Telepaxx Software GmbH
Juli 2007

Stellungnahme zur Rezertifizierung des e-pacs Speicherdienstes

Die Firma Telepaxx Software GmbH hat am 25.6.2007 eine Selbsterklärung abgegeben, in der vermerkt wird, dass das Produkt e-pacs Speicherdienst weiterhin in der unveränderten Version 3.0 eingesetzt wird. An der Sicherheitsarchitektur, der Verschlüsselung gäbe es keine Änderungen. Lediglich sei die Schlüssellänge bei dem Verschlüsselungsverfahren RSA erhöht worden; zudem habe sich in der Einsatzumgebung das Server-Betriebssystem geändert.

Aufgrund der Tatsache, dass ein unverändertes Produkt rezertifiziert 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,
- --- dass der Wechsel des Server-Betriebssystems zu keiner Beeinträchtigung der Sicherheit geführt hat,
- --- inwieweit die an das Produkt zu stellenden Anforderungen unverändert geblieben sind.

1. 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:

- --- Windows 2003 Server SP2
- --- MS-SQL Server 2005 SP2
- --- FreeS/WAN 1.99
- --- IPSec-Verschlüsselung (Symmetrische Verschlüsselung mit Triple-DES und einer Schlüssellänge von 168 Bit, asymmetrische Verschlüsselung mit RSA und einer Schlüssellänge von 2048 Bit)
- --- CA-Server (generiert und signiert für Kunden X.509-Zertifikate mit einer Schlüssellänge von 1024 Bit)
- --- e-token der Firma Aladdin

Sämtliche Produktkomponenten als auch die Komponenten der Einsatzumgebung entsprechen dem aktuellen Stand der Technik.

Dies gilt insbesondere für die verwendeten Verschlüsselungsverfahren: Blowfish und Triple-DES gelten **mit den genutzten Schlüssellängen als sichere Verschlüsselungs-algorithmen**; RSA wird mit einer Schlüssellänge von 2048 Bit gemäß der „Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen)“ vom 22. Februar 2007 der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen – im Bundesanzeiger veröffentlicht am 12.4.2007 – bis Ende 2012 und damit weit über den Ablauf des Zertifikats hinaus **als sicher eingestuft**.

2. Wechsel des Betriebssystems

Der Wechsel von Windows 2000 Server Service Pack 4 auf Windows 2003 Server Service Pack 2 sowie von MS-SQL Server Service Pack 3 auf MS-SQL Server 2005 Service Pack 2 hat **in keiner Weise** zu einer Beeinträchtigung der Betriebssystem- und Datenbanksicherheit geführt.

Die vorgenommenen Änderungen – Windows 2003 Server bietet wesentlich bessere Schutz- und Kontrollmaßnahmen als Windows 2000 Server – erhöhen vielmehr die Sicherheit und Stabilität der Betriebssysteme bzw. Datenbanken und sind **positiv** zu betrachten.

3. Weitgehend unveränderte Rechtsgrundlagen

Bei der Bewertung des epacs Speicherdienstes wurden bei der Erstbegutachtung 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. Zwar hat sich die Musterberufsordnung für Ärzte durch Beschluss des Vorstands der Bundesärztekammer vom 26.11.2006 geändert, die Änderung betrifft in § 18 jedoch nur die berufliche Kooperation von Ärzten untereinander. Insgesamt ergeben sich demnach keine Veränderungen im Hinblick auf die rechtlich einschlägigen Rahmenbedingungen des epacs Speicherdienstest und kein Bedarf an einer Änderung des seinerzeit zugrunde gelegten Anforderungsprofils.

Bremerhaven, 4.Juli 2007

(datenschutz nord GmbH)