

Datenschutz und Datensicherheit im Deutschen Kinderkrebsregister

Datenschutz

Das Deutsche Kinderkrebsregister (im Folgenden mit Kinderkrebsregister bezeichnet) besitzt ein separates Computernetzwerk (siehe Anhang Netzwerktopologie des Kinderkrebsregisters). Nur innerhalb dieses Netzwerkes kann auf Daten des Kinderkrebsregister zugegriffen werden, das heißt Daten auf einem Computer des Kinderkrebsregisters können nur dann von einem anderen Computer gelesen werden, wenn sich dieser ebenfalls im Netz des Kinderkrebsregisters befindet. Bei dem Netz handelt es sich um ein Fast-Ethernet mit Stern-Topologie. Dies bedeutet, dass alle Netzkomponenten über eine separate Leitung mit einer zentralen Netzeinheit (Switch) verbunden sind. Der Switch regelt den Datenverkehr von dem Sender zum Empfänger. Die Daten laufen nur über die Leitungen des Senders und des Empfängers. Das hat zur Folge, dass der Datenverkehr selbst innerhalb des Kinderkrebsregisternetzes nicht von einer dritten Netzwerkkomponente (z.B. Computer) mitgehört werden kann.

Keine Daten, die dem Datenschutz unterliegen, werden auf lokale Festplatten der einzelnen Arbeitsplatzrechner gespeichert. Somit besteht bei einer eventuellen Entwendung von Computern des Kinderkrebsregisters nicht die Gefahr, dass Daten in unrechtmäßige Hände gelangen. Sensible Daten werden ausschließlich auf den Servern des Kinderkrebsregisters gespeichert, die sich im Maschinenraum des Institutes (IMBEI) befinden. Zu diesem Maschinenraum hat nur ein begrenzter Personenkreis Zugang. Dieser Zugang wird über spezielle Zugangskarten geregelt, wobei beim Betreten entsprechende Daten (Person, Zeit) erfasst und gespeichert werden. Zugriffe auf Daten der Kinderkrebsregister-Server werden über passwortabhängige Zugriffsrechte geregelt. Auf den Servern selbst ist das Betriebssystem Linux mit entsprechenden Sicherheitskomponenten installiert.

Über einen kinderkrebsregistereigenen Firewall besteht die Möglichkeit Daten zwischen dem Kinderkrebsregister und dem Institut sowie der Klinik auszutauschen. Der Firewall regelt streng den Datenverkehr zwischen den Netzen. Es ist nur möglich, einen Verbindungsaufbau vom Kinderkrebsregisternetz aus zu starten. Der Firewall lässt keine Datenverbindung von einem Netz außerhalb des Kinderkrebsregisters in das Netz des Kinderkrebsregisters zu. Über die Firewall-Verbindung werden nur Daten ausgetauscht, die nicht dem Datenschutz unterliegen. Das Institutsnetz selbst ist wiederum durch Firewall-Rechner mit dem Internet verbunden, so dass zwei Sicherheitsstufen zwischen dem Kinderkrebsregister und dem Internet bestehen.

Daten des Kinderkrebsregisters werden nur in kryptographierter oder anonymisierter Form mit anderen Institutionen ausgetauscht. Beim Kryptographieren kommt ein Public-Key-Verfahren mit einem 2048-Bit-Schlüssel zum Einsatz.

Datensicherheit

Der Kinderkrebsregister-Fileserver sichert einmal täglich die gesamten Daten auf eine separate Festplatte. Dabei bleiben auch ältere Versionen der einzelnen Dateien erhalten, die dann einzeln wieder restauriert werden können. Die Daten des Fileservers werden einmal täglich mit dem Ersatz-Fileserver abgeglichen, so dass der Ersatz-Fileserver stets den Datenbestand des Fileservers vom Vortag aufweist.

Der Datenbankserver des Kinderkrebsregisters besitzt 2 Festplatten mit einem RAID-1-Filesystem. Dabei ist eine Festplatte redundant, so dass bei einem Ausfall einer Festplatte keine Daten verloren gehen. Einmal täglich wird eine Kopie sämtlicher Daten in diesem Filesystem angelegt, damit auch beim versehentlichen Löschen von Daten auf eine Sicherung zurückgegriffen werden kann. Auch dieser Server speichert täglich seine Daten auf einen Ersatzserver.

Die Daten sämtlicher Server werden einmal in der Woche auf ein Datenband geschrieben und in einem feuersicheren Safe im Maschinenraum aufbewahrt. Einmal im Monat wird eine Bandsicherung sämtlicher Daten in einem Safe außerhalb des Institutes (Verfügungsgebäude) deponiert.

Netzwerktopologie des Kinderkrebsregisters, des IMBEIs und vom Rest der Welt

