Auszug aus den durchgeführten Interviews

Der Hersteller des Servers hat eine 99,99-prozentige Verfügbarkeit garantiert. Die akzeptierte Ausfallzeit liegt hierbei unter einer Stunde pro Jahr. Unsere Analyse ergab, dass der Server seit der Inbetriebnahme im Schnitt nur alle drei Jahre ausgefallen ist. Ohne gezielte Maßnahmen würde der Ausfall des Servers einen beträchtlichen Schaden anrichten, da hier alle Daten des Krankenhauses gespeichert sind und die einzelnen Abteilungen diese täglich abrufen. Durch ergänzende Sicherheitsmaßnahmen können wir jedoch den Betrieb des Servers sehr rasch wiederherstellen. Der Server wird nämlich redundant ausgelegt, damit sichergestellt ist, dass bei einem Ausfall die virtuelle Infrastruktur weiterhin problemlos betrieben wird. Somit erreichen wir eine Risikoreduktion um eine Stufe.

Einen Missbrauch von Berechtigungen gab es im Klinikum noch nie und auch bei der Personalplanung wird gezielt auf charakterlichen Eigenschaften geachtet. Durch ein verpflichtendes Berechtigungskonzept ist geregelt, dass unbefugte Personen keinen Zugang zu personenbezogenen Daten erhalten. Der Schaden beim Missbrauch von Berechtigungen kann sicherlich katastrophales Ausmaß annehmen, da im Krankenhaus mit hochsensiblen bzw. personenbezogen Daten gearbeitet wird. Risikoakzeptanz. Die Risiken können daher akzeptiert werden, weil die Gefährdung nur unter äußerst speziellen Bedingungen zu einem Schaden führen.

Das Krankenhaus muss jeden Tag etliche Cyber-Angriffe abwehren. Ohne zusätzliche technische und organisatorische Maßnahmen wäre die Schadenshöhe absolut existenzbedrohend. Daher wurde eine DMZ errichtet, die eine Pufferzone zwischen externem (Internet) und internem Netzwerk darstellt. Durch ein zweistufiges Firewall-Konzept soll verhindert werden, dass Sicherheitslücken es erlauben, beide Firewalls gleichzeitig zu überwinden. Dadurch erreichen wir wiederum eine Risikoreduktion.

Der Zugang zum Serverraum ist durch eine Chipkarte für autorisierte Personen gesichert. Mit dem externen Dienstleister Huber IT wurde ein Service und Wartungsvertrag für die IT-Infrastruktur abgeschlossen. Dadurch wurde die Verantwortung für Schäden komplett an den Dienstleister übertragen. Durch Log-Daten des Chipkarten-Lesegerätes kann jederzeit nachvollzogen werden, wer sich zu welcher Zeit im Serverraum befand. Daher müssen keine weiteren Maßnahmen getroffen werden.