

Grundschutz an einem Universitätsklinikum

Sicherheitsstrategie für Klinikum der Universität München

Dipl.-Inf. (FH) Robert Vattig, T-Systems; Dr. Walter Swoboda, CIO, Klinikum der Ludwig-Maximilians-Universität München

Um das Sicherheitsniveau am Klinikum der Universität München zu steigern, wurde durch das Institut Anfang 2009 eine Diplomarbeit gefördert. Das Ziel war, eine geeignete Sicherheitsstrategie für die dort vorherrschenden Insellösungen zu finden.

Im Klinikum der Universität München nutzte jede Abteilung Konzepte und Leitlinien für die IT-Sicherheit, es fehlte jedoch eine allgemeine Sicherheitsleitlinie und ein Sicherheitskonzept. Nach der Sichtung möglicher Strategien fiel schnell die Aufmerksamkeit auf den IT-Grundschutz des BSI. Beim IT-Grundschutz besteht der Vorteil, dass Standardsicherheitsmaßnahmen bereits ausgearbeitet sind und lediglich umgesetzt werden müssen. Das BSI stellt mit den IT-Grundschutzkatalogen Bausteine mit denen ein Informationsverbund abgebildet wird sowie Gefährdungen und Maßnahmen zur Modellierung und Absicherung des Informationsverbundes zur Verfügung. Für Systeme mit erhöhtem Schutzbedarf ist eine ergänzende Sicherheitsanalyse notwendig, bei der für die einzelnen Zielobjekte entschieden wird, ob eine Risikoanalyse auf Basis von IT-Grundschutz durchgeführt wird oder entbehrlich ist. Dies gilt auch für Zielobjekte, zu denen kein passender Baustein in den Katalogen existiert oder die in einer, für den IT-Grundschutz untypischen, Art und Weise oder Einsatzumgebung betrieben werden. Das Ziel der Arbeit war, eine mögliche Sicherheitsstrategie zu finden und diese modellhaft umzusetzen. Dadurch kann der Arbeitsaufwand bei der Umsetzung des IT-Grundschutzes grob abgeschätzt werden. Der Hauptbestandteil der Arbeit war

das Einpflegen der Zielobjekte, die Schutzbedarfsfeststellung und der Basis-Sicherheitscheck mit einer anschließenden Auswertung der Ergebnisse.

Vorarbeiten am Klinikum

Die Ansprechpartner waren der zuständige CIO, der das gesamte Projekt leitete, der IT-Sicherheitsbeauftragte als Hauptansprechpartner und verschiedene Administratoren der IT-Abteilung. Das Vorhaben begann damit, dass die Rahmenbedingungen abgesteckt wurden. Dazu gehörten die Geschäftsziele, die rechtlichen Rahmenbindungen und der Geltungsbereich. Die Geschäftsziele waren bereits definiert und teilten sich in sekundäre und primäre Ziele auf. Zu den Primärzielen gehörte die Patientenbehandlung sowie die Lehre und Forschung. Als Sekundärziel wurden niedrige Kosten definiert. Dazu kamen die strategischen Ziele wie verbesserte Dokumentation oder mögliche Konsolidierungen in der IT. Der Geltungsbereich bezog sich auf die zentralen Rechenzentren, das heißt, alle Systeme außerhalb der Rechenzentren, wie beispielsweise Clients, wurden nicht betrachtet. Weitere organisatorische Vorarbeiten der IT-Grundschutz-Methodik wurden theoretisch in der Arbeit erörtert. Als Werkzeug wurde das GSTOOL in Version 4.6 des BSI

verwendet, eine Lizenz stellte das BSI im Rahmen der Diplomarbeit kostenlos zur Verfügung.

Durchführung der Strukturanalyse und Schutzbedarfsbestimmung

Bei der Stammdatenerfassung und Strukturanalyse traten die ersten Probleme auf. Aus technischer Sicht war es kaum möglich, beim Einpflegen Gruppen zu bilden. Unterschiedliche Betriebssysteme, unterschiedliche Anwendungen sowie virtuelle vernetzte Server, sorgten dafür, dass fast jedes IT-System einzeln erfasst werden musste. Da der Schutzbedarf noch nicht bestimmt war, konnten keine Gruppen basierend auf den Schutzbedarf gebildet werden.

Mit Hilfe der gegebenen Bausteine wurden insgesamt etwa 300 Server in das GSTOOL eingepflegt. Nachdem alle Server erfasst waren, mussten die Anwendungen eingepflegt werden. Aufgrund unzähliger Anwendungen und einer modellhaften Umsetzung, wurden von Anfang an alle Anwendungen direkt in Gruppen erfasst. Daraus entstanden 15 verschiedene Anwendungsgruppen von allgemeinen Informationssystemen über IT-Managementsysteme und Kommunikationsanwendungen bis hin zu den einzelnen SAP-Komponenten, zum Beispiel für das Personalwesen oder dem Patientenmanagementsystem und

weiteren Modulen. Jeder Anwendung wurden anschließend die entsprechenden IT-Systeme (Server) zugeordnet und der Schutzbedarf der Anwendungen bestimmt. Jedes IT-System erbt den Schutzbedarf der untergeordneten Anwendung. Allerdings war die Abbildung der Infrastruktur im verwendeten GSTOOL nicht aussagekräftig, weil viele Verknüpfungen verschiedener Systeme und virtuelle Verbünde kaum darstellbar waren. Die Netzwerkstruktur wird am Klinikum logisch getrennt, somit gehört technisch gesehen alles zu einem Netz. Die logischen Netzwerke unterscheiden sich in die Gebäudeleittechnik (GLT), das medizinische Versorgungsnetz (MedVer) und das Wissenschafts- und Forschungsnetz (WiFo). Die medizinischen Server im Rechenzentrum sind durch zwei Firewalls durch den Zugriff von Außen geschützt. Das WiFo ist Teil des Deutschen Forschungsnetzes und mit dem Internet verbunden. Das GLT spielte eine untergeordnete Rolle, da es noch in der Entwicklung war. Solche komplexen Infrastrukturen lassen sich im GSTOOL nur andeuten und bei einer hohen Anzahl von Zielobjekten fehlt die Übersichtlichkeit.

Hoher Schutzbedarf durch Patientendaten

Nach der Feststellung des Schutzbedarfs wurden 91% der IT-Systeme mit erhöhtem Schutzbedarf bewertet (Maximum-Prinzip), in Abbildung 1 ist die Schutzbedarfsfeststellung der IT-Systeme detailliert dargestellt. Das lässt sich darauf zurückführen, dass fast alle Systeme Patientendaten verarbeiten, denn der Hauptgeschäftszweig eines Krankenhauses ist natürlich die Patientenbehandlung. Da der IT-Grundschutz nur Systeme mit einem "normalen" Schutzbedarf abdeckt, wurde eine umfangreiche Risikoanalyse notwendig. Der Schutzbedarf in den Anwendungsgruppen war annähernd gleich verteilt, jedoch wurden den Anwen-

dungen mit erhöhtem Schutzbedarf bei weitem mehr IT-Systeme zugeordnet. Für eine spätere Umsetzung des IT-Grundschutzes am Klinikum der Universität München, wurde von beiden Diplomanden empfohlen:

„Der Schutzbedarf von jedem Ziel-Objekt sollte einzeln erfasst werden. Wird der Schutzbedarf von vorher definierten Gruppen bestimmt und geerbt, führt eine falsche Zuordnung eines Zielobjektes zu einem falschen Schutzbedarf. Wird der Schutzbedarf eines Systems zu hoch bewerten, könnten bei der Umsetzung teure aber unnötige Schutzmaßnahmen umgesetzt werden. Wird der Schutzbedarf eines Systems hingegen zu niedrig bewerten, werden notwendige Sicherheitsmaßnahmen für dieses System eventuell nicht betrachtet und es entstehen Sicherheitslücken. Zwar ist der Aufwand bei der Strukturanalyse und Schutzbedarfsfeststellung höher, jedoch werden Kosten und Risiken gesenkt.“

Modellierung und Basis-Sicherheitscheck des Informationsverbundes

In jedem Baustein ist ein Überblick über die Gefährdungslage und Maß-

nahmen-Empfehlungen enthalten. Die Standard-Sicherheitsmaßnahmen wurden vom GSTOOL in der Modellierung automatisch aus den Maßnahmen-Empfehlungen abgeleitet und benötigten kaum Nacharbeiten. Der Kernpunkt der Nacharbeiten bezog sich auf fehlende Bausteine, die schon in der Strukturanalyse Probleme verursachten. Diese Probleme konnten durch die Verwendung anderer Baustein der IT-Grundschutzkataloge umgangen werden, traten jedoch in der Modellierung erneut auf, wenn Sicherheitsfragen für ein Zielobjekt veraltet und nicht zutreffend waren. Für die richtige Zuordnung von Maßnahmen zu den Zielobjekten muss der Bearbeiter in jedem Bereich Wissen mitbringen, egal ob Wissen über Hardware, Software, organisatorisches Wissen oder über andere Bereiche.

In der Modellierung im GSTOOL werden die Maßnahmen in fünf Schichten unterteilt, was bei der Auswahl der Interviewpartner hilfreich ist, aber bei der Modellierung kaum Vereinfachungen schafft. Anschließend an die Modellierung folgte der Basissicherheits-Check. Hierzu wurden Interviews mit unterschiedlichen Ansprechpartnern aus verschiedenen Abtei-

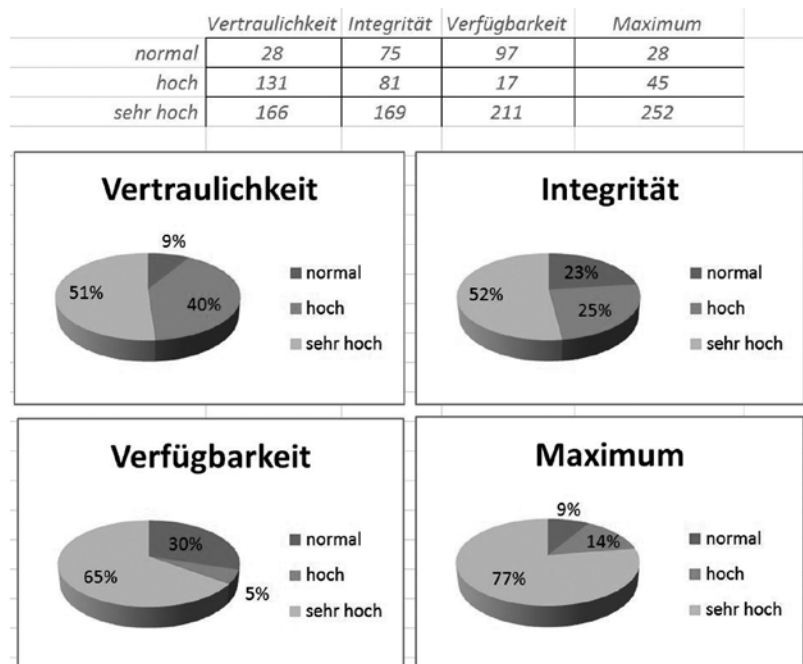


Abbildung 1: Ergebnisse der Schutzbedarfsfeststellung der IT-Systeme am getesteten Klinikum.

IT-Verbund:											
	Anzahl Maß- nahmen	umgesetzt		nicht umgesetzt		teilweise umgesetzt		entbehrlich		unbearbeitet	
Gesamt	2351	1276	54,3%	349	14,8%	445	18,9%	252	10,7%	29	1,2%
Priorit. 0	2253	1213	53,8%	349	15,5%	442	19,6%	249	11,1%	0	0,0%
Priorit. 1	90	61	67,8%	0	0,0%	3	3,3%	3	3,3%	23	25,6%
Priorit. 2	2	1	50,0%	0	0,0%	0	0,0%	0	0,0%	1	50,0%
Priorit. 3	4	1	25,0%	0	0,0%	0	0,0%	0	0,0%	3	75,0%
Priorit. 5	2	0	0,0%	0	0,0%	0	0,0%	0	0,0%	2	100,0%

Abbildung 2: Umsetzungsstatus der Standard-Sicherheitsmaßnahmen am getesteten Klinikum (GSTOOL-Bericht).

lungen durchgeführt. Da die Sicherheitsmaßnahmen durch die IT-Grundschutz Kataloge schon formuliert waren und sogar mit Kontrollfragen endeten, benötigten die Vorbereitungen auf die Interviews nur wenig Zeit.

Während der Interviews erklärten einige Gesprächspartner zu jeder Maßnahme jedes Detail, andere beantworteten die Fragen ausschließlich mit Ja oder Nein. Problematisch waren die Maßnahmen, zu denen sich kein Ansprechpartner fand bzw. bei denen der potentielle Ansprechpartner keine Zeit hatte. In diesem Fall bezogen der IT-Leiter und der IT-Sicherheitsbeauftragte Stellung zu den betreffenden Maßnahmen. Im Durchschnitt dauerte ein Interview mit 20 Maßnahmen etwa 45 Minuten. Bei den Gesprächen kamen gelegentlich Missverständnisse auf, zum Beispiel wegen technischer Details. Die Erfahrung zeigte, dass hier zwei Ansprechpartner Abhilfe schufen. Es wurde keine Bewertung der Kosten und Arbeitszeit für die Maßnahmen vorgenommen, da kein Mitarbeiter hierzu Aussagen tätigen konnte.

Auswertung der Ergebnisse

Die Auswertung ergab, dass 54,3% der Maßnahmen umgesetzt, 14,8% nicht umgesetzt, 18,9% nur teilweise umgesetzt, 10,7% entbehrlich sind und 1,2% unbearbeitet blie-

ben, wie aus Abbildung 2 ersichtlich. Demzufolge weisen 33,7% Mängel auf und sind entweder nicht oder nur teilweise umgesetzt. Bei näherer Betrachtung zeigte sich, dass technische Maßnahmen größtenteils umgesetzt sind und organisatorische Maßnahmen vorwiegend Mängel aufwiesen. Dazu gehörten Dokumentation, Notfallmanagement, Bildung eines IT-Sicherheitsmanagements, Einteilen der Aufgaben und Verantwortlichkeiten und weitere. Diese fehlenden organisatorischen Maßnahmen machten den größten Prozentsatz aus, wobei Fehler bei technischen Maßnahmen oft auf die organisatorischen Mängel zurückführbar waren.

Eine technische Maßnahme besteht oft zusätzlich aus organisatorischen bzw. konzeptionellen Fragestellungen wie der Dokumentation und dem Notfallmanagement. Bei der Einführung einer allgemeinen Leitlinie zur Dokumentation und zum Notfallmanagement würden demzufolge technische Maßnahmen ebenfalls verbessert werden. In dieser Auswertung wurden nur die Maßnahmen des IT-Grundschutzes und nicht die ergänzende Sicherheitsanalyse betrachtet. Das heißt, hauptsächlich Systeme mit normalem Schutzbedarf werden durch den IT-Grundschutz abgedeckt. Ob weitere Maßnahmen für Systeme mit erhöhtem Schutzbedarf umgesetzt werden müssten, wurde nicht bearbeitet.

Fazit

Auf Grundlage dieser Diplomarbeit wurden am Klinikum der Universität München konzeptionelle und organisatorische Maßnahmen eingeleitet, um das Sicherheitsniveau zu steigern. Das BSI stellt mit der IT-Grundschutz-Methodik eine standardisierte und umfassende Strategie zu Schaffung von Informationssicherheit zur Verfügung. Bereits mit den organisatorischen beziehungsweise konzeptionellen Maßnahmen kann das Sicherheitsniveau deutlich gesteigert werden. Das Klinikum der Universität München sollte gerade in diesem Bereich aufholen, da die Sicht auf die technischen Maßnahmen bereits als akzeptabel angesehen werden kann. So sind die meisten mangelhaften technischen Maßnahmen auf konzeptionelle oder organisatorische Maßnahmen zurückzuführen. Die Akzeptanz der Mitarbeit bezüglich der Sicherheitsmaßnahmen ist sehr hoch und damit eine gute Grundlage zur Weiterentwicklung der vorhandenen Konzepte und Leitlinien. Das genutzte GSTOOL ist als Werkzeug gut geeignet, um nach der IT-Grundschutz-Methodik zu agieren. Die IT-Grundschutz-Kataloge sind im Tool integriert und Automatisieren im Tool erleichtern die Arbeit. Leider kann die Infrastruktur mit dem Tool nicht optimal dargestellt werden und bei der Auswertung fehlen ebenfalls grafische Ausgaben. ■