IT-Sicherheit bei den Kliniken des Bezirks Oberbayern

Toni Kehr · Sebastian Dännart

Universität der Bundeswehr München
{toni.kehr | sebastian.daennart}@unibw.de

Zusammenfassung

Der Schutz der Patientendaten in Kliniken ist ein wichtiges Thema in der IT-Sicherheit. Die Kliniken des Bezirks Oberbayern (kbo) haben im Rahmen einer laufenden Aktivität zur Erhöhung der IT-Sicherheit auf eine Bedrohung der IT-Sicherheit durch Ransomware kurzfristig reagiert und diesen Impuls in eine nachhaltige Steigerung der IT-Sicherheit und des Bewusstseins für IT-Sicherheit umgesetzt. kbo setzt dabei auf eine Strategie des ausgewogenen Risikomanagements in der IT-Sicherheit. Wichtige Elemente des IT-Sicherheitsmanagements sind ein multiprofessionelles IT-Sicherheitskomitee mit Prozessen, die externe Kompetenzen einbinden, Verantwortungsdruck für Mitarbeiter vermeiden sowie schnelle, transparente Entscheidungen von IT und Anwendern gemeinsam ermöglichen. Der vorliegende Beitrag ist die Kurzfassung einer Fallstudie zur IT-Sicherheit in Kritischen Infrastrukturen. Die vollständige Fallstudie ist in der Quelle [LDR+18] veröffentlicht sowie unter www.itskritis.de kostenfrei verfügbar.

1 Kontext der Fallstudie

1.1 Unternehmensprofil

Die Kliniken des Bezirks Oberbayern – kbo – sind ein Verbund von ambulanten und stationären Einrichtungen, die seit 2007 als Kommunalunternehmen zusammenarbeiten. Mit 6.700 Mitarbeitern werden jährlich 110.000 Patienten stationär, teilstationär und ambulant behandelt, gepflegt und betreut. An den über 22 Standorten stehen in den Kliniken des Unternehmensverbundes insgesamt 3.000 Betten zur Verfügung. Zur kbo gehört auch eine forensische Psychiatrie mit 200 Maßregelvollzugsbetten.

Als Verbund von Einrichtungen des Gesundheitswesens lässt sich kbo dem Sektor „Gesundheit“ und der Branche „Medizinische Versorgung“ als Kritische Infrastruktur (KRITIS) zuordnen [BSI16]. Die Rechtslage sieht entsprechend dem IT-Sicherheitsgesetz mit der KRITIS Verordnung einen Schwellenwert von 30.000 stationären Fällen pro Krankenhaus vor, ab dem Kliniken als Kritische Infrastrukturen gelten. kbo erreicht diesen Schwellenwert allerdings nur im Verbund und wird daher nach dem IT-Sicherheitsgesetz [Bund15] und der KRITIS Verordnung [BSI16] nicht als KRITIS-Betreiber angesehen. Bereiche, wie die Forensik (Maßregelvollzug) mit über 200 Betten, können jedoch nicht einfach von anderen Kliniken oder Institutionen übernommen werden, daher sieht sich kbo selbst als Kritische Infrastruktur und die IT würde sich auch eine gesetzliche Anerkennung als KRITIS wünschen.

P. Schartner · N. Pohlmann (Hrsg.) · D•A•CH Security 2018 · syssec (2018) 228-231.

1.2 IT-Sicherheit im Unternehmen

Der Schutz der Patientendaten ist das oberste Gebot bei kbo und auch bei deren IT-Dienstleister „IT des Bezirks Oberbayern GmbH“. Das Gesamtsystem, mit seinen Schnittstellen zu anderen Unternehmen wie Banken oder Apotheken, beispielsweise für Gehaltsabrechnungen und Medikamentenbestellungen, muss geschützt sein.

Ein IT-Sicherheitskomitee ist das Bindeglied zwischen der IT, dem Anwender und dem Konzernvorstand und setzt sich aus Vertretern der verschiedenen Funktionsbereiche des Unternehmens zusammen. Mitglieder sind der Geschäftsführer IT, der IT-Compliance Officer und die drei Bereichsleiter der Bereiche Service Management, Applikationen und Infrastruktur sowie der Datenschutzbeauftragte und der IT-Sicherheitsbeauftragte. Das IT-Sicherheitskomitee trifft Entscheidungen zur IT-Sicherheit immer gemeinsam mit IT und Anwendern. Im Fall von Cyberangriffen werden im IT-Sicherheitskomitee die Maßnahmen abgestimmt und freigegeben.

Als initiale IT-Sicherheitsmaßnahme wurde ein „Anforderungskonzept an die IT-Sicherheit“ mit Anteilen gängiger Rahmenwerke (COBIT, BSI IT-Grundschutz etc.) und Normen (ISO/IEC 27000 etc.) erstellt. Die Sicherheitsanforderungen werden mindestens einmal jährlich überprüft – dies wird durch den IT-Sicherheitsbeauftragten kontrolliert. Jährlich erfolgt zudem ein Penetrationstest. Der IT-Sicherheitsbeauftragte erstellt das IT-Sicherheitskonzept und legt damit auch wichtige Aspekte des Risikomanagements fest, welches unter anderem auf Prozessen und Controls von COBIT basiert. Das IT-Sicherheitskonzept wird durch den Vorstand freigegeben.

2 Maßnahmen und Treiber

Die Kliniken des Bezirks Oberbayern hatten bereits mit der Planung und Umsetzung von Maßnahmen zur Erhöhung der IT-Sicherheit begonnen – zunächst wurde eine neue Firewall implementiert und das IT-Sicherheitskomitee wurde eingerichtet. Weitere Maßnahmen sollten Schritt für Schritt ausgeplant und umgesetzt werden. Der Angriff mit Ransomware auf mehrere Krankenhäuser war vier Wochen später im Februar 2016 [Borc16] jedoch Anlass für kbo das Sicherheitsniveau kurzfristig zu erhöhen und IT-Sicherheitsmaßnahmen sofort vorzunehmen bzw. geplante IT-Sicherheitsmaßnahmen vorzuziehen.

Zur Erhöhung der IT-Sicherheit sollten die interne Organisation und IT-relevante Sicherheitsvorgänge überprüft und gegebenenfalls geändert werden. Möglichkeiten für Gegenmaßnahmen standen ebenso auf der Agenda, wie ein Upgrade der IT-Infrastruktur mit Hardware und Software.

Unter anderem folgende Maßnahmen wurden im Rahmen der Erhöhung der IT-Sicherheit unmittelbar umgesetzt:

IT-Sicherheitskomitee in Verbindung mit Change Management: Die wohl wichtigste Maßnahme war die Schaffung des multiprofessionellen IT-Sicherheitskomitees mit Prozessen wie dem Change Management im Zusammenhang mit IT-Sicherheitsvorfällen. Der Prozess gewährleistet Verantwortungsteilung sowie schnelle, transparente Prozesse und zieht dabei den externe IT-Sicherheitsdienstleister mit ein.

Überprüfungsprozess für E-Mail Anhänge: Der Prozess sorgt für einen wirkungsvollen Schutz vor Schadsoftware und schützt unter anderem gegen die üblichen Angriffsvektoren

Phishing und Spear-Phishing sowie gegen „Fake Bewerbungen“ als Träger von Schadsoftware, nicht selten Ransomware. Anhänge in Form von PDFs und einigen Bauplanformanten können im Gegensatz zu Zip- oder Exe-Dateien in zugestellt werden. Die Virenscanner im Schleusen-PC, mit dem Anhänge überprüft werden, schlagen häufig an und tragen zur Vertrauensbildung in die IT im Allgemeinen und die IT-Sicherheitsmaßnahmen im Speziellen bei.

Internet-Policy und aktive Inhalte: Die Internet-Policy wurde verschärft, jedoch aufgrund von speziellen Anforderungen aus den Fachbereichen in Teilen kurze Zeit später wieder gelockert. Die Makros für Arztbriefe, welche nicht deaktiviert werden können, liegen alle in einem geschützten Bereich und wurden als vertrauenswürdig gekennzeichnet.

Sperrung Internetzugriff für Administrator-Konten: Durch die Sperrung ist die Gefahr reduziert, dass Administrator-Konten mit Schadsoftware kompromittiert werden (beispielsweise über Outlook) und damit das Netzwerk auf einer hohen Rechteebene infiziert wird.

Management der Fernzugänge: Der Login in das kbo-Netz von externen Standorten wird überwacht, Zugangskontrollen finden statt und die Zugänge sind auf das Notwendige beschränkt. Es besteht Transparenz, welche medizinischen Geräte Fernzugang bspw. für Wartung benötigen.

Maßnahmenkatalog BSI für Krankenhäuser: Die Expertenempfehlung des BSI wurden, soweit es für kbo machbar war, umgesetzt und gibt so weiteren Schutz vor Schadsoftware.

Anwenderrechte: Mit einem Skript werden die Anwenderrechte überprüft; nicht nötige Anwenderrechte werden entzogen, sodass die Anwenderrechte auf das Notwendige beschränkt sind.

Update-Policy: Clients, die sich länger als 180 Tage nicht im Netz von kbo angemeldet haben, werden automatisch gesperrt und müssen durch die IT wieder freigegeben werden. So befinden sich keine Rechner mit veralteten IT-Sicherheitskonfigurationen im Netz.

Sonderprüfungen/Audits: Sie stellen den tatsächlichen Stand der Maßnahmen in der IT fest, sodass das IT-Sicherheitskomitee über geplante und genehmigte Maßnahmen – zusätzlich zum Berichtswesen – Feedback erhält.

Dass die Sorge der Kliniken des Bezirks Oberbayern hinsichtlich eines Cyber-Angriffs nicht unbegründet sein sollte, zeigte sich im September 2016. Seit drei Uhr morgens verzeichnete die IT eine massive Anzahl von Zugriffen auf die Firewall. Das war extrem ungewöhnlich für das Krankenhaus. Die neue Firewall war so konfiguriert, dass sie den Netzzugang im Falle einer Überlast automatisch abschaltet und so war kbo wieder offline. Die Telekom wurde zur Hilfe gezogen, um den Traffic zu analysieren und konnte einen Botnetz-Angriff identifizieren und nach Osteuropa zurückverfolgen. Nach zwei Stunden wurde die Firewall teilweise hochgefahren und in einem durch die Telekom gesicherten Testbetrieb beobachtet. Die Muster des Netzwerkverkehrs entsprachen denen der vorangegangenen Woche und so konnte nach zwei weiteren Stunden in den normalen operativen Betrieb übergegangen werden.

3 Erfolgsfaktoren

kbo konnte den kurzfristigen Impuls, die IT-Sicherheit zu verbessern, in eine nachhaltige Optimierung der IT-Sicherheit umsetzen und die Strategie eines ausgewogenen Risikomanagements hat sich in der Praxis bewährt. Die IT-Strategie wird hierbei von einem gemeinsamen Entscheidungsgremium vorgegeben und stellt den organisatorischen Rahmen

dar. Dieser wird in den einzelnen Abteilungen von der IT dann individuell umgesetzt und realisiert. Durch diese zweistufige Hierarchie, kann die finanzielle Argumentation auf einer höheren Ebene erfolgen und lässt den IT-Abteilungen gleichzeitig größtmögliche Freiheit auf individuelle Bedürfnisse einzugehen.

Ein zentraler Erfolgsfaktor ist die Einrichtung des IT-Sicherheitskomitees und die multiprofessionelle Zusammensetzung dieses Komitees. Die erfolgreiche Abwehr des Angriffs im September 2016 war ein wichtiges Vertrauenssignal: kbo konnte intern weiterarbeiten, das Sicherheitskomitee und die IT haben die Lage im Griff gehabt und das Frühwarnsystem hat funktioniert. Wichtig war dabei, dass die Entscheidungsprozesse schnell und transparent abliefen: Die IT kann jetzt – ohne Gefahr für den operativen Betrieb – das Internet für kbo sperren, weil sie weiß, welche Bereiche wieder schnell freigeben werden müssen und wie sie diese Dienste dann auch wieder schnell in Betrieb nehmen kann.

Das Prinzip des ausgewogenen Risikomanagements wird umgesetzt: Weder IT, noch Anwender können Fragen der IT-Sicherheit alleine entscheiden, das Risikomanagement bezieht sie gleichermaßen mit ein und Lösungen für IT-Sicherheitsfragen werden gemeinsam getragen.

Das entschlossene Handeln und das pragmatische Umsetzen der nötigen Adhoc-Maßnahme und die anschließende strategische Umsetzung der Maßnahmen in konsequentem Einklang mit den Bedürfnissen der Mitarbeiter und der Organisation, ermöglicht kbo eine IT-Sicherheitsstrategie, die bestmöglich auf die Anforderungen eines Klinikverbundes abgestimmt ist. Trotz des angesprochenen Handelns war der tägliche Betrieb auf den Stationen, insbesondere die Patientenversorgung, zu jeder Zeit gesichert.

Literatur

[Borc16] U. Borchers (2016): Ransomware-Virus legt Krankenhaus lahm. Heise online. https://www.heise.de/newsticker/meldung/Ransomware-Virus-legt-Kranken haus-lahm-3100418.html (abgerufen am 14.05.2018).

[BSI16] Bundesamt für Sicherheit in der Informationstechnik (2016): Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz. https://www. gesetze-im-internet.de/bsi-kritisv/BJNR095800016.html (abgerufen am 03. August 2017).

[Bund15] Bundesgesetzblatt: Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz). Bundesgesetzblatt Jahrgang 2015 Teil I Nr. 31.

[LDR+18] U. Lechner, S. Dännart, A. Rieb, S. Rudel: CASE KRITIS – Fallstudien zur IT-Sicherheit in Kritischen Infrastrukturen, Logos (2018).