Wenn der Server im Keller neben dem Papeterielager steht…

Wie hoch sind die Risiken, wie sicher die IT-Infrastruktur?

Über die Datensicherheit schreiben wir auch in diesem Magazin ausführlich. Hier behandeln wir einen speziellen Aspekt: Nicht selten sieht es übel aus, wenn externe IT-Techniker zu Besuch kommen. Selbst zentrale Komponenten stehen schlecht geschützt an ungünstigen Standorten. Und während bei Banken und Versicherungen strengste Aufsichtsbehörden über die Qualität der IT-Infrastruktur wachen, besteht im Gesundheitswesen Nachholbedarf – Anlass genug für «clinicum», der Sache auf den Grund zu gehen. Experten trafen sich bei der HINT AG in Lenzburg.

So präsentiert sich die Situation an einigen Orten: Server und weitere zentrale IT-Infrastrukturen stehen in Kellerlokalen, unweit von Papier- und Papeterielagern, die HINT-Spezialisten trafen auch schon Einrichtungen an, die in wenig klimatisierten Estrichräumen standen, ungenügend vor sommerlicher Hitze geschützt. Darüber hinaus sind eklatante Schwächen bei der Vernetzung unterschiedlicher Systeme zu sehen. Gefahren lauern bekanntlich am ehesten bei den Schnittstellen, die Kette ist so stark wie das schwächste Glied. Reisst es oder fällt der Server wegen klimatischer Einwirkungen oder ungenügender unterbrecherfreier Stromversorgung aus, wird die Lage rasch prekär. Und im Gegensatz zu Banken und Versicherungen, wo die pickelharte Kontrolle der FINMA für eine praktisch 100%ige Sicherheit sorgt, geht es im Spital nicht bloss um den kurzfristig eingeschränkten Zugriff auf Kontodaten, sondern im wahrsten Sinne des Wortes «ums Lebendige», vergessen wir nicht, dass zahlreiche Stellen im Spital – namentlich die Operateure – heute ohne digitalen Zugriff auf bildgebende Verfahren und KIS-Daten überhaupt nicht mehr arbeiten können.

Ein «Absturz» mit Folgen

Blenden wir kurz zurück: Im Juli dieses Jahres wuchsen zahlreichen Verantwortlichen fürs Gesundheitswesen in Irland eine ganze Anzahl grauer Haare. Im Beaumont Hospital in Dublin stand der Betrieb während rund 30 Stunden still. Die in die Jahre gekommene IT-Architektur hielt den laufend gestiegenen Anforderungen an die Verarbeitung rasch wachsender Datenmengen und den sicheren, blitzschnellen Zugriff auf klinische und administrative Daten nicht mehr Stand. Das System kollabierte und die Spitalleitung beinahe mit ihm. Das Fiasko zog eine Reihe von Untersuchungen nach sich. Schleunigst musste die komplette IT-Architektur neu aufgesetzt werden. Der Imageschaden war irreparabel.
Auch die Schweiz hat solche Vorfälle schon erlebt, der letzte Fall ist sogar jüngeren Datums. Glücklicherweise resultierten daraus nicht dermassen schwerwiegende Folgen (deshalb wäre es auch unfair, den Namen des letzten Falles publik zu machen). Es zeigt sich aber dennoch, dass auch hierzulande eine gewisse Labilität vorhanden ist – und die Komplexität der Systeme wie auch der Umfang der Datenflut werden mit Sicherheit nicht abnehmen. Die Ursache möglicher Risiken ist folgende: Früher bestand die Spital- IT aus Office-Produkten und vielleicht noch aus einem ERP für die Patientenadministration und die Buchhaltung. Entsprechend war die Abhängigkeit von der IT auch nicht sehr gross – Ausfälle, die vorkamen, waren zwar störend, aber verkraftbar. Dadurch, dass auch die medizinischen Daten zunehmend digitalisiert werden, kommt der IT heute punkto Sicherheit eine viel grössere Bedeutung zu. Darauf müssen sich die Spitäler einstellen.

Beim Bewusstsein fängt's an

Markus Goldschmid, Service Delivery Manager bei HINT, stellte die Ausgangslage für mehr IT-Sicherheit dar: «Wir müssen mit einer geeigneten IT-Architektur die Voraussetzung dafür schaffen, dass eine hohe Verfügbarkeit der Daten und ein optimaler Schutz der Informationen andauernd gegeben sind. Was wir neu aufbauen, ist allerdigs auch zu einem bestimmten Umfang von früher genutzten IT-Systemen mitgeprägt. So treffen wir häufig auf Situationen, bei denen die Sicherheit grundsätzlich verbessert werden muss. Spitäler haben in der Schweiz noch keineswegs den Standard von Banken oder Industriebetrieben erreicht, dabei geht es im Krankenhaus doch um Menschenleben. Wir stellen insbesondere ein teilweise fehlendes Bewusstsein für dieses Thema fest. Oft werden auch die damit verbundenen Kosten gescheut. Schliesslich ist die Vielfalt der eingesetzten Systeme einer klaren Fokussierung hinderlich. Die Schnittstellenproblematik ist enorm.»

Markus Goldschmid, Service Delivery Manager bei HINT

> « Wir stellen ein teilweise fehlendes Bewusstsein für IT-Sicherheit fest. Auch ist die Vielfalt der eingesetzten Systeme einer klaren Fokussierung ist hinderlich. »
>
> Markus Goldschmid

Albert Besewski, Business Development Manager von ATSP Schweiz, wies auf die beiden Grundfaktoren hin, welche Sicherheits-Investitionen beeinflussen: die Technik, aber ebenso sehr der Mensch, der als Spitaldirektor, Arzt oder Pflegefachkraft Prozesse bestimmt. Alle stellen potenzielle Sicherheitsrisiken dar. Im Zentrum stehen dabei die Auswirkungen, die eintreten können, die Frage, wo denn Schäden überhaupt beginnen, relevant zu werden, wer die Verantwortung dafür zu tragen hat, wer genügend Kompetenz für die Lösung hängiger Sicherheitsprobleme mitbringt und wer schliesslich die nötige Zeit einsetzen kann, sich damit auseinanderzusetzen.

Albert Besewski, Business Development Manager von ATSP Schweiz

«Dabei», so Besewski, «ist jeweils die Betriebsblindheit ein arger Hemmschuh. Das beflügelt auch die exakte Analyse nicht besonders. Diese ist aber von ausschlaggebender Bedeutung, gilt es doch neben technischen und applikatorischen Aspekten gerade umfassend abzuklären, wo sich denn Bruchstellen in der IT-Sicherheit zeigen könnten. Es kann also von Vorteil sein, sich mit externem Know-how zu verstärken. Im Hinblick auf die Swiss DRG erachte ich es als besonders wichtig, die Verkettung klinischer und administrativer Prozesse harmonisch auszugestalten. Das kann die Betriebssicherheit wesentlich erhöhen.»

Sicherheit muss erste Priorität einnehmen

«Weiter muss die IT-Sicherheit ganz einfach erste Priorität erhalten», betonte Dr. med. Georg Sasse, Riskmanager des Kantonsspitals Aarau. «Bei uns leben wir danach. So nimmt IT-Sicherheit als Grunderfordernis eines reibungslosen, störungsfreien Betriebs klar den ersten Platz ein und war auch 2011 höher gewichet als die DRG-Einführung. Wir beurteilen systematisch die Eintretenswahrscheinlichkeit und das mögliche Schadensausmass. Bei unserem Jahresumsatz von rund 500 Mio. Franken beziffern wir potenziell kritische Situationen auf 10%. Das entspricht den Einnahmen von 5 Wochen Arbeit. Würde es beispielsweise bei einem Ausfall des Zugriffs auf unsere Datenbank nötig, mit medizinischen Notfallteams ohne digitale Unterstützung ‹händisch› zu operieren, wären bloss noch 50% der Eingriffe möglich, selbstverständlich wären das eher einfachere und daher weniger lukrative OPs. Entsprechend nehmen wir die Sache äusserst ernst, damit die Risiken aufs absolute Minimum reduziert werden.»

Im Kantonsspital Aarau erfüllt ein IT-Kernteam diese Aufgabe, das über eine umfangreiche industrielle Erfahrung verfügt. Dabei ist allen klar, dass es einerseits Industriestandards und andererseits spezifische Standards im Gesundheitswesen gibt. Ebenso bedeutungsvoll ist es zu beachten, dass zwei Kulturen existieren: Geschäftsleitung und Ärzte. «Wir müssen damit leben, dass Ärzte im Notfall dazu tendieren, bestimmte Sicherheitvorschriften im IT-Einsatz zu unterlaufen, um Menschenleben zu retten. Für sie ist die blitzschnelle Verfügbarkeit verständlicherweise wichtiger als der absolute Datenschutz. Das gilt es zu respektieren. Diese Haltung kann ja auch sehr wertvoll sein. Vergessen wir nicht, dass Behandlungsfehler teuer zu stehen kommen. Erst kürzlich bestimmte ein Schweizer Gericht die gesamte Beeinträchtigung eines schwer geschädigten Patienten auf 6 Mio. Franken. Das grösste Risiko ist aber der Ausfall von Systemen. In der täglichen Arbeit geht es somit primär darum, dass eben gerade das nicht passieren darf.»

Richtig in die IT investieren – Risiken eliminieren

«Effektiv dürften Ausfälle in Informations- und Medizintechnik gar nicht vorkommen», betonte Matthias Meierhofer, Verwaltungsratspräsident der MEIERHOFER Schweiz AG, Bern, «deshalb lohnen sich auch gezielte Investitionen in die IT-Infrastruktur und Software. Diese Investitionen machen ja auch nur einen Bruchteil der möglichen Risiken aus. Mit der zunehmenden Komplexität medizinischer Prozesse wächst logischerweise auch die Bedeutung der IT, namentlich auf der applikatorischen Ebene. Dort muss alles vorgekehrt werden, damit kein Vertauschen von Daten oder ein Ausfall von Datenzugriffen vorkommen, die zu irreparablen Schäden bei Patienten führen könnten. Es besteht also ein Datenhaltungs- und -Abbildungsrisiko. Wer es nicht im Griff hat, läuft grosse Gefahr, einen veritablen Imageschaden einzufangen, den die Medien nicht müde werden, genüsslich zu verbreiten. Im Zeitalter der freien Spitalwahl kann das betriebswirtschaftlich letal sein. Es wäre von grossem Nutzen, wenn die Sicherheit und Unversehrbarkeit der Patienten von den Ärzten mehr ins Zentrum gerückt würde und im gleichen Atemzug wie das Nutzen der modernsten Medizintechnik genannt würde.»

> « Eine exakte Analyse ist von ausschlaggebender Bedeutung, gilt es doch neben technischen und applikatorischen Aspekten gerade umfassend abzuklären, wo sich denn Bruchstellen in der IT-Sicherheit zeigen könnten. »
>
> Albert Besewski

«Hier besteht halt eben ein grosser kultureller Unterschied zu den angelsächsischen Staaten», ergänzte Albert Besewski, «in Deutschland und der Schweiz steht bisweilen die übergrosse Angst vor dem Einblick in Patientendaten einem sichereren und effizienteren Operieren und Behandeln im Weg. Im ansonsten viel geschmähten NHS in Grossbritannien ist das keine Diskussion; hier werden alle relevanten Daten ganz einfach genutzt, niemand stört sich daran, sondern empfindet das in der täglichen Arbeit als grossen Vorteil. Wir tun gut daran, hierzulande Ängste abzubauen und Lücken zu schliessen, die gerade in der Notfallversorgung zu ernsten Konsequenzen führen könnten.»

Strukturelle Hürden sind eine grosse Bremse

Lücken, die es zügig zu schliessen gebe, ortete auch Markus Goldschmid, Service Delivery Manager bei HINT. «Wir treffen heute in allen Spitälern einen unerhörten Erfolgsdruck an, überall sind mehr Wirtschaftlichkeit und höhere Produktivität gefragt. Damit hat die IT-Architektur vielerorts nicht mithalten können. Teilweise sind leider während der letzten zehn Jahre eklatante Lücken entstanden, die nun unter knapper Zeit und Stress zu schliessen sind. Gefährlich sind dabei folgende Tatsachen:

- nicht vorhandene korrekte IT-Budgets,
- ein umfangreicher Nachholbedarf im gesamten IT-Umfeld,
- ungenügende Optimierung des Gesamtsystems bei Erneuerungen von Teilsystemen,
- gefährliche Schnittstellen,
- ungenügende Verkettung von Prozessen und
- ungenutztes Effizienzpotenzial innerhalb von Spitalzusammenschlüssen.»

«Es ist aber auch alles andere als einfach», warf Albert Besewski ein, «ich möchte nicht in der Haut eines Spital-IT-Chefs stecken. Er oder sie muss eine

Matthias Meierhofer, Verwaltungsratspräsident der MEIERHOFER Schweiz AG, Bern

Riesenaufgabe im täglichen Routinebetrieb erfüllen und Ansprechpartner/-in für alle IT-Fragen sein. Gleichzeitig werden Visionen erwartet, wie denn die IT der Zukunft zu gestalten sei. Das ist eine Quadratur des Kreises. Zurzeit verdoppelt sich das Datenvolumen innerhalb von bloss 18 Monaten. Dazu kommen neue, jedes Mal komplexere Technologien, die es IT-mässig zu unterstützen und abzubilden gilt. Schliesslich dreht sich immer mehr um den blitzschnellen Datenaustausch, was ausserordentliche Anforderungen an die Archivierung und strukturierte Datenbereitstellung bedeutet.»

« Gerade weil die Risiken zunehmen, sollten sich Spitäler überlegen, ob die IT-Budgets nicht auszubauen seien. Im Vergleich zur Industrie, wo europaweit 8% der Umsätze für IT-Investitionen und -Unterhalt ausgegeben werden, beträgt der Anteil im Gesundheitswesen lediglich 2,5%. »

Matthias Meierhofer

Matthias Meierhofer warnte vor einem gefährlichen Stehenbleiben. «Trotz der enormen Belastung, denen sich die Spitalverantwortlichen ausgesetzt sehen, müssen sie mutige Schritte tun. Technologisch sind die Herausforderungen schon in den Griff zu kriegen, es fragt sich aber, ob die Branche bereit ist, das zu bezahlen. Gerade weil die Risiken zunehmen, sollten sich Spitäler überlegen, ob die IT-Budgets nicht auszubauen seien. Im Vergleich zur Industrie, wo europaweit 8% der Umsätze für IT-Investitionen und -Unterhalt ausgegeben werden, beträgt der Anteil im Gesundheitswesen lediglich 2,5%. «18'000 Todesfälle, die allein in Deutschland auf Behandlungsfehler zurückzuführen sind, machen ein Aufstocken der Budgets sicher überlegenswert. Verkehrstote gibt es im Jahresvergleich mit ca. 3600 deutlich weniger. Es wäre also im Bereich der IT-Sicherheit viel zu tun.»

Gibt es zu wenig Druck?

Fehlt den Spitälern ein gesunder Druck, um IT-mässig für mehr Sicherheit aufzurüsten? – Dr. med. Georg Sasse ist nicht dieser Meinung. «Druck ist genug vorhanden, allein schon von der DRG-Einführung her. Es ist ein Spital-interner Druck. Wir beschäftigen uns im KSA deshalb ganz intensiv mit der Datenintegration, weil wir wirtschaftlicher arbeiten müssen. Wenn wir das vernachlässigen würden, wären die Kosten, die aufgrund ungenügender Sicherheit entstehen könnten, rasch grösser als die Investitionen,

Dr. med. Georg Sasse, Riskmanager des Kantonsspitals Aarau

die wir deshalb konsequent tätigen. Dabei spüren wir den Machtfaktor der Ärzte sehr stark; weitere Überzeugungsarbeit wird nötig sein, um in der Spital-IT die dort noch unüblichen kompromisslosen Industriestandards zu erreichen.»

Matthias Meierhofer verwies auf deutsche Erfahrungen seit der Einführung der DRG: «In Deutschland sind die IT-Ausgaben eher gesunken, während die Personalkosten angestiegen sind. Das mag in der Schweiz anders sein. Generell muss sich die IT-Industrie aber gewaltig anstrengen, den Nutzen ihrer Marktleistungen zu kommunizieren. Es muss transparent werden, wo mehr Wirtschaftlichkeit und höhere Versorgungsqualität entstehen.»

«Dabei darf IT, die der Sicherheit und Qualität dient, nicht mehr länger als reiner Kostenfaktor angesehen werden», postulierte Albert Besewski. «IT ist ein lebenswichtiger Faktor. Damit ihr die nötige Bedeutung zukommt, muss ein IT-Chef Mitglied der Geschäftsleitung sein.»

Markus Goldschmid kann das nur unterschreiben: «Historisch gewachsene Organisations- und Entscheidungsstrukturen müssen überdacht werden. Heute genügt es nicht mehr, wenn der CFO eines Spitals IT gewissermassen als Hobby mitbetreut. Wesentlich vorteilhafter ist eine kompetente und erfahrene Ansprechperson, so wie wir das beispielsweise im Kantonsspital Aarau antreffen.»

Riskmanagement und IKS etablieren

Licht am Ende des Tunnels sieht Dr. Sasse, und das auf breiter Flur. «Nach den Banken hat sich die Einsicht, dass ein professionelles Riskmanagement nötig sei, auch bei den Spitälern durchgesetzt. Fast jedes Spital hat heute einen RM-Verantwortlichen. Sie vernetzen sich untereinander und pflegen einen regen Informationsaustausch, von dem alle profitieren. Neben dem eigentlichen Riskmanagement ist auch das Interne Kontrollsystem sehr wertvoll. Hier werden unterschiedlichste Risiken und ihre möglichen Einflussfaktoren analysiert sowie entsprechende Gegenmassnahmen aufgebaut und Zuständigkeiten definiert. Auf diese Weise entsteht ein integrales Riskmanagement. Entscheidend wird nun sein, ob es der Geschäftsleitung gelingt, die erabeiteten Massnahmen gegenüber Ärzten und Pflege durchzusetzen. Ausserdem ist auch die Ebene der Trägerschaft zu beachten. Auch ein Gesundheitsdepartement oder ein Stiftungsrat wollen erst überzeugt werden.»

«Das braucht wohl noch einiges an Zeit», meinte Matthias Meierhofer, «wir leben halt noch immer in einer Art ‚planwirtschaftlicher Marktwirtschaft'. Die Administration nimmt einen zu grossen Stellenwert ein. Allerdings gibt es etliche hervorragende Beispiele, und private wie öffentlich-rechtliche Spitäler ihr integrales Riskmanagement beherrschen. Weil eine generelle politische Regelung für die Breite aller Leistungserbringer allerdings nicht zu erwarten ist, bleiben die vorbildlichen Beispiele aus der Branche von grosser Bedeutung. Zudem liegt es auch an der Industrie, zu zeigen, wo Risiken bestehen und wie sie mit IT-Unterstützung zu meistern sind.»

« Nach den Banken hat sich die Einsicht, dass ein professionelles Riskmanagement nötig sei, auch bei den Spitälern durchgesetzt. Fast jedes Spital hat heute einen RM-Verantwortlichen. »

Dr. med. Georg Sasse

Strategische Erfolgsfaktoren

Die Runde ist sich einig: Riskmanagement, IKS und erstklassige IT-Lösungen sind strategische Erfolgsfaktoren. Markus Goldschmid ist motiviert, diese Aufgabe organisatorisch und technisch anzupacken. Die Rechenzentren der HINT AG sind ISO- und FINMA-zertifiziert. Weitere Zertifizierungen sind für das Jahr 2012 geplant. Markus Goldschmid und die Spezialisten der HINT AG wissen, worauf es ankommt: «Wir setzen alles daran, dass unsere Kunden, die wir beraten oder für die wir ganz oder teilweise die IT als Outsourcing-Partner betreiben, ein qualifiziertes IT-Wissen aufbauen können. Wo zu geringe Inhouse-Kapazitäten bestehen, bündeln wir gemeinsam das nötige Know-how, damit eine positive kritische Masse entsteht, die für einen erstklassigen Betrieb sorgt. Eine der besten Voraussetzungen dafür ist, dass alle internen und externen Fachleute mit dem gleichen Fokus ans Werk gehen, damit insbesondere alle Aspekten der Sicherheit mit grösster Priorität behandelt werden.»
Text: Dr. Hans Balmer