INFORMATIONSSICHERHEIT IM KRANKENHAUS: Gestern, Heute und in Zukunft

Ein Interview mit Mike Zimmermann

Mike Zimmermann ist Informationssicherheitsbeauftragter im Universitätsklinikum Carl Gustav Carus in Dresden. Die Klinik ist seit 1999 eine Anstalt des öffentlichen Rechts des Freistaates Sachsen und gehört zu den größten führenden Kliniken in Deutschland. In unserem Exper*Site*-Interview berichtet er über die Herausforderungen der Digitalisierung im Gesundheitswesen, über die Veränderung seiner Position mit steigenden Sicherheitsanforderungen und wie er sich die Zukunft der Informationssicherheit im Gesundheitswesen vorstellt.

ExperSite *Herr Zimmermann, Sie sind seit 11 Jahren als Informationssicherheitsbeauftragter im Universitätsklinikum Carl Gustav Carus Dresden beschäftigt. Können Sie zusammenfassen, wie sich Ihre Position seitdem verändert hat? Vor welchen Herausforderungen standen Sie damals? Vor welchen Herausforderungen stehen Sie heute?*

Mike Zimmermann: Anfangs war ich noch mit dem Aufbau der operativen IT-Sicherheit beschäftigt. Natürlich hatten wir damals schon Firewalls oder Endpoint Protection Systeme im Einsatz, aber die Aufgabe bestand darin, die Klinik-Administratoren durch Zentralisierung und Standardisierung dieser sicherheitsrelevanten Systeme zu entlasten. In dieser Zeit war das Verständnis für IT-Sicherheit noch extrem gering und wurde eher als etwas Negatives empfunden, da zum Beispiel die Virenscanner im Verhältnis noch sehr viel Prozessorlast der IT-Systeme in Anspruch nahmen oder beim wöchentlichen Vollscann der Systeme nahezu nichts anderes mehr mit dem System gemacht werden konnte. Ich erinnere mich an viele Diskussionen mit den Anwendern und IT-Administratoren.

Mit den ersten Erkenntnissen zum damals neuen IT-Sicherheitsgesetz wurde ich dann zum ISB ernannt, klassischerweise nicht mehr in der IT angesiedelt, sondern direkt dem Vorstand unterstellt. Die Aufgaben wechselten sukzessive immer mehr von der operativen hin zu der strategischen IT-Sicherheit. Anfangs bestand die Herausforderung darin, das Verständnis, aber auch die Verantwortung für IT-Sicherheit in den Klinik- und Geschäftsbereichsleitungen zu etablieren. Es war nicht einfach, zumal es damals kaum öffentlich bekannte Angriffe gab und die wenigen Veröffentlichungen entweder sehr weit entfernt waren oder in der Regel kaum unsere Branche betrafen.

Ein wichtiges Merkmal meiner Arbeit heute besteht darin, nicht irgendwelche Verbote zu definieren, sondern ich versuche auch immer zu verstehen, warum Prozesse oder Praktiken so umgesetzt werden. Meiner Meinung nach fördern wir mit reinen Verboten nur die Kreativität der Benutzer:innen, um neue, andere, meistens nicht weniger gefährliche Wege zu finden, um ihre Arbeitsprozesse zu optimieren. Ich kann sie oftmals verstehen und im Dialog versuchen wir den schmalen Pfad zwischen Usability und IT-Sicherheit zu finden.

> „Wir können nur gemeinsam die aktuellen Herausforderungen meistern

> „Ein wichtiges Merkmal meiner Arbeit besteht darin zu verstehen, anstatt Verbote zu definieren.

MIKE ZIMMERMANN

Informationssicherheitsbeauftragter im Universitätsklinikum Carl Gustav Carus in Dresden

Aktuell gibt es für alle Krankenhäuser eine riesengroße finanzielle Herausforderungen aufgrund der Pandemie und dem Krieg in der Ukraine und den damit verbundenen teilweise enorm gestiegenen Beschaffungs- und Verbrauchskosten wie beispielsweise Energie. Ein wichtiges Credo unserer Universitätsklinik besteht darin, Prozesse nicht nur in unserem Hause zu formen, sondern auch in und vor allem für die Branche aktiv die Vorgaben mit zu definieren. Ein Beispiel sind die gemeinsamen Ausarbeitungen der ersten Handlungsempfehlungen für Krankenhäuser zum Aufbau von IT-Sicherheit im Rahmen des UP-KRITIS Branchenarbeitskreises „Medizinische Versorgung“. Heute bin ich in vielen externen Arbeitskreisen tätig und versuche nicht nur mitzugestalten, sondern vor allem auch die gemeinsame Bewältigung von Themen zu forcieren. Was somit einem weiteren wichtigen Credo unseres Hauses entspricht, dass wir gerne unsere Erfahrungen teilen wollen, um uns letztendlich gegenseitig in Bereichen zu helfen, in denen wir aus meiner Sicht mittelfristig nur gemeinsam erfolgreich die Herausforderungen bewältigen können!

ExperSite *Im Jahr 2015 ist das IT-Sicherheitsgesetz 2.0 (IT-SiG) in Kraft getreten. Im Jahr 2017 kam dann die KRITIS-Verordnung nach dem BSI-Gesetz (BSI-KritisV), durch die Ihr Haus als kritische Infrastruktur definiert wurde. Wie haben diese gesetzlichen Regelungen Ihre Tätigkeit als ISB verändert?*

>>>

Mike Zimmermann: Grundsätzlich haben die gesetzlichen Regulierungen einen sinnvollen Rahmen definiert. Ehrlich gesagt spart es auch viel interne Diskussionszeit, wenn ich auf Gesetze und Verordnungen verweisen kann und nicht argumentieren muss, ob denn nur wir Lösungen für Probleme suchen müssen. Ich würde mir aber wünschen, dass wir oftmals etwas mehr Zeit zwischen Gesetzes- bzw. Verordnungserlass und der Umsetzungsfrist hätten. Ein weiterer wichtiger Wunsch ist, dass der Gesetzgeber vor allem im Gesundheitssektor mit jeder Regulierung auch gleich die Finanzierung bestimmt. Es soll jetzt aber nicht der Eindruck entstehen, dass wir ohne Finanzierung keine IT-Sicherheitsmaßnahme durchsetzen wollen, aber wir müssen bei der besonderen Abrechnungsmethodik für Krankenhäuser immer wieder um jeden Euro kämpfen. Ich möchte auch gerne anregen, dass wir gelebte bzw. praktizierte Informationssicherheit fördern müssen, was sich zum Beispiel mit der Ermittlung eines Reifegrades und damit verbundenen Finanzierungstufen mittlerweile gut abbilden ließe. Sprich: Krankenhäuser erhalten je nach erreichtem Reifegrad Zulagen für die Finanzierung der IT-Sicherheit.

Insgesamt sind manche Anforderungen weniger verständlich und einzeln betrachtet sogar sinnlos, aber wie mittlerweile in allen Bereichen des Lebens, gibt es für die wenigsten Fragen nur noch ein einfaches Ja oder Nein. Die Komplexität wird immer weiter zunehmen und so müssen wir auch die Informationssicherheit ganzheitlich betrachten.

> Wir müssen gelebte Informationssicherheit in Krankenhäusern fördern

ExperSite *Schließlich wurde 2020 das Krankenhauszukunftsgesetz (KHZG) erlassen, das Krankenhäuser in die Lage versetzen soll, in moderne Notfallkapazitäten, die Digitalisierung und in IT-Sicherheit investieren zu können. Wie schätzen Sie den Erfolg des KHZG ein, wo sehen Sie Optimierungsbedarf?*

Mike Zimmermann: Das KHZG hat ursprünglich eine sehr gute Idee verfolgt und wir beschweren uns manchmal auf einem hohen Niveau. Es ist meines Erachtens das erste Förderprogramm, bei dem man nicht nur Investitionen abrechnen kann, sondern auch Dienstleistungen, Beratungen und vor allem auch Personalkosten für einen bestimmten Zeitraum. Die Gesamtfördersumme klingt erst einmal viel, aber geteilt durch alle Krankenhäuser und deren Digitalisierungs- und IT-Sicherheitsprojekte bleibt dann doch nicht mehr so viel übrig und wir haben sehr viel Nachholbedarf bei diesen beiden Themen in unserer Branche! Aber wie gesagt: 1 Million Euro sind besser als 0 Euro.

Kritisch sehe ich aber in der Tat zwei Probleme:
Zum einen wird es durch diesen enormen Investitionsschub für die Branche zunehmend schwieriger werden, Ressourcen zu finden, mit denen man diese Projekte zeitgerecht umsetzen kann, woran letztendlich die Qualität leiden wird.

Und zum anderen sehe ich wie bei allen Förderungen das Problem: Wie geht's weiter, nachdem die Gelder geflossen sind? In drei, spätestens fünf Jahren müssen erste Ersatzinvestitionen getätigt werden, oder wie sonst kann das jetzt finanzierte und qualitativ notwendige Personal gehalten werden? Vermutlich nicht nur die kleineren Häuser benötigen weitere Förderungen, um die Digitalisierungs- und Informationssicherheitsthemen auch dann noch weiter betreiben zu können.

> Das KHZG ist grundsätzlich eine sehr gute Idee. Aber wie geht es nach der Förderung weiter?

ExperSite *Unter anderem die Resilienz der IT-Systeme in KH steht immer wieder im Fokus, wenn es um zunehmende Digitalisierungsmaßnahmen geht. Wie setzen Sie das im Universitätsklinikum Carl Gustav Carus Dresden um?*

Mike Zimmermann: Zuallererst muss der Stellenwert der IT angepasst werden. Wenn ich Benutzer:innen dahingehend befrage, wird die IT immer noch häufig auf E-Mails und Internet beschränkt. Die jetzt schon vorhandene sehr hohe digitale Abhängigkeit wird vielen dann erst im weiteren Gesprächsverlauf bewusst.

Zusätzlich zeichnen sich unsere angebotenen IT-Services bisher durch eine sehr hohe Verfügbarkeit aus. Das führt zu der Erwartung, dass die IT oder auch die vernetzte Medizintechnik nicht ausfallen wird. Prinzipiell super, aber die Sensibilisierung hinsichtlich der Business Continuity bei Ausfall digitaler Prozesse steht dadurch natürlich nicht an erster Stelle.

Die IT ist sich der Wichtigkeit der IT-Resilienz bewusst, aber durch die Ressourcenknappheit in allen Belangen kann dies oftmals nicht vollumfänglich bewertet werden und steht somit unter enormen Druck. Es muss aber letztendlich jedem Klinik-Prozessverantwortlichen bewusst sein, dass auch dies in seiner Verantwortung steht.

> Die sehr hohe digitale Abhängigkeit ist vielen Benutzer:innen gar nicht bewusst

ExperSite *Immer wieder liest man auch von unklaren Verantwortlichkeiten, fehlenden personellen Ressourcen, einem mangelnden Verständnis für die Ernsthaftigkeit des Themas oder sogar der IT selbst, wenn es um Digitalisierungsmaßnahmen im Gesundheitswesen geht. Können Sie das bestätigen? Und wo erleben sie Schwachstellen und weiteren Handlungsbedarf?*

Mike Zimmermann: Die fehlenden Ressourcen und das damit verbundene fehlende Know-how ist aus meiner Sicht derzeit die größte Herausforderung bei der Digitalisierung. Oftmals werden analoge Prozesse eins zu eins digitalisiert, ohne dass eine umfassende Prozessprüfung stattfindet. Richtig frustrierend wird es dann für die Benutzer:innen, wenn es schon schlechte analoge Prozesse waren. Wichtig wie bei allen Prozessänderungen ist, dass wir die Benutzer:innen mitnehmen und auf ihre Bedarfe eingehen oder anders ausgedrückt: Die IT und die Informationssicherheit müssen begleiten, aber nicht die Prozesse federführend definieren.

> Das fehlende Know-how ist die größte Herausforderung in der Digitalisierung

ExperSite *Grundsätzlich geht es beim Business Continuity Management darum, die Aufrechterhaltung des Geschäftsbetriebes auch bei einer Störung sicherzustellen. Welche Prozesse mit welchen Maßnahmen stoßen Sie im Falle eines Cyberangriffs im UKDD an, um die Informationssicherheit weiterhin gewährleisten zu können?*

Mike Zimmermann: Wir haben als Krankenhaus viel Erfahrung mit Ausnahmesituationen wie Hochwasser oder der Versorgung von vielen Verletzten zur gleichen Zeit. Cyberangriffe waren vor Neuss und Düsseldorf noch so weit weg bzw. sehr abstrakt, aber spätestens seit dem Vorfall am UK Düsseldorf sind sich alle Verantwortlichen der möglichen Konsequenzen eines Informationssicherheitsvorfalles bewusst. Der vorhandene klinikumsweite Alarm- und Einsatzplan wurde angepasst und es wurden Strukturen geschaffen, die unter anderem durch die Erkenntnisse und Erfahrungen aus Düsseldorf entwickelt wurden. Zum Beispiel wurde das Lagezentrum für IT-Notfälle erweitert, sodass die IT integriert werden kann, inklusive mögliche externe IT-Unterstützung. Bei der Analyse eines möglichen IT-Totalausfalls an unserem Klinikum wurden mögliche Schwachstellen identifiziert und werden nun priorisiert bearbeitet. In der IT gibt es verschiedene Projekte zu Themen wie der Kommunikation im Notfall, dem Wiederanlauf oder auch der Forensik. Auch das regelmäßige Üben ist Bestandteil dieser Notfallkonzepte.

In den jeweiligen Kliniken und Geschäftsbereichen werden Notfallkonzepte entwickelt, um die Geschäftsfortführung der kritischen Dienstleistungen sicherzustellen. All diese Anforderungen kommen zusätzlich auf die betroffenen Bereiche dazu. Die Notwendigkeit ist allen bewusst, aber auch hier muss aufgrund der vorhandenen Ressourcen priorisiert werden. Für mich ist wichtig - wie bei allen anderen Informationssicherheitsthemen: Wir müssen uns stetig weiterentwickeln und besser werden.

ExperSite *Häufig merken wir bei DATATREE AG, dass die Sensibilisierung aller Mitarbeitenden ein wichtiger Bestandteil ist, um die Informationssicherheit in eine Organisation nachhaltig zu implementieren. „Die größte Schwachstelle in der IT ist der Mensch" ist ein Satz, der in diesem Zusammenhang gerne fällt, wenn es um IT-Security in Organisationen geht. Teilen Sie diese Meinung?*

Mike Zimmermann: Ja, selbstverständlich ist der Mensch die größte Schwachstelle.

Wir machen Fehler, was auch wichtig ist, um daraus zu lernen und uns weiterzuentwickeln. Leider sehe ich aber oftmals die falsche Fehlerkultur und man stürzt sich nach Vorfällen lieber auf den vermeintlichen Verursacher und kennt keine Gnade mit Vorwürfen, anstatt konstruktiv nach Lösungen zu suchen!

Oftmals werden uns nicht ausreichend Ressourcen zur Verfügung gestellt. Das Lernen und Ausprobieren sind sehr wichtig, um beispielsweise sichere Anwendungen zu entwickeln oder fit im Umgang mit der IT zu sein. Wir Menschen reagieren emotional und haben Ängste, die zu Reaktionen führen, die wir zu anderen Zeitpunkten so nicht getätigt hätten. Diese Eigenschaften werden ausgenutzt - im Positiven wie im Negativen! Auch für mich ist Sensibilisierung ein wichtiger Baustein in der Informationssicherheit. Die bisherige klassische regelmäßige Massen-„Grundbetankung“ der Benutzer:innen ist aber nicht sinnvoll. Wir müssen Awareness-Kampagnen erarbeiten, in denen zwar eLearning enthalten ist, aber durch viele anderen Medienformate und Inhalte ergänzt werden. Wir haben unterschiedliche Zielgruppen mit diversen Reifegraden. Der eine mag lieber eine spielende Vermittlung mit Gamification und andere lesen lieber einfache textbasierte Inhalte auf der Heimfahrt im Zug. Die Erfahrungen zeigen, dass Sensibilisierungen schnell wieder in Vergessenheit geraten oder gar schon bei der Schulung gelangweilt/genervt vom Thema sind. Gerade letztere Gruppe sind aus meiner Sicht auch die potenziell anfälligsten Benutzer:innen.

Es ist eine enorme Herausforderung und vor allem eine permanente Aufgabe User Awareness zu schaffen und nachhaltig zu etablieren! Wir müssen auch hier mit Emotionen arbeiten, natürlich nicht um Angst und Schrecken zu verbreiten, wie es Angreifer:innen tun, sondern im positiven Sinne. Erschwerend kommt noch dazu, dass Informationssicherheit im Krankenhaus nur ein kleiner Teil von vielen verpflichtenden Schulungen der Mitarbeitenden ist. Zusammengefasst bedeutet das: Sensibilisierung ist wichtig, als eine von vielen technischen und organisatorischen Bausteinen in der Informationssicherheit!

> Oft wird sich nach Vorfällen auf den/die vermeintlichen Verursachenden gestürzt, anstatt konstruktiv nach Lösungen zu suchen.

Exper*Site* *Ein Blick in die Zukunft aus Sicht eines Experten: An welcher Stelle steht Informationssicherheit in 10 Jahren? Welche Veränderungen / Trends erwarten und erhoffen Sie in Bezug auf Informationssicherheit in kritischen Infrastrukturen?*

Mike Zimmermann: Die grundlegende Methodik wird sich nicht ändern, sprich, wir werden immer wieder am besten möglichst zeitnah auf neue Bedrohungen reagieren müssen und es wird nie eine 100% Sicherheit geben! Wie immer werden neue Technologien sowohl positive als auch negative Veränderungen mit sich bringen. KI ist ein aktuelles, gutes Beispiel, obwohl ich oftmals unterstelle, dass mit KI geworben wird, obwohl sie letztendlich noch nicht drinsteckt. Aber es pusht das Thema derzeit enorm. KI wird uns sehr viel Positives bringen, selbstverständlich werden andererseits Angreifer:innen die KI auch für ihre Use Cases einsetzen.

Viele der bisherigen Prozesse werden aus meiner Sicht einer großen Transformation unterliegen und somit viele Veränderungen und Anpassungsbedarf mit sich bringen. Bisherige Ansätze der onPrem Datenhaltung werden zumindest zu hybriden cloud-/onPrem-basierten Umsetzungen führen.
Wir sind auf dem Weg zu einer datenzentrierten Infrastruktur, was die Voraussetzung für das erforderliche Teilen und Verschieben unseres wichtigsten Assets, den Daten sein wird. Nicht nur um die Sicherheit (Verfügbarkeit und Zuverlässigkeit) zu erhöhen, sondern auch um neue und absolut notwendige Use Cases durch das Verknüpfen dieser Daten zu erhalten. Gerade im Medizinsektor wünsche ich mir dadurch unter anderem Heilungschancen, die bisher noch nicht möglich sind.

Letztendlich wird es wichtig sein, dass die Informationssicherheit und der Datenschutz immer ein Bestandteil aller Krankenhausprozesse sein muss! Und wie schon seit eh und je werden wir uns rückblickend fragen, wie zeitintensiv - da ohne Automatisierung und deshalb kompliziert - haben wir früher nur analysiert? Was aber nicht bedeutet, dass man im Jetzt und Hier mehr Zeit für angenehmere Dinge haben wird!