ISMS AUFBAU UND BRANCHENVERGLEICH

Von ausbaufähig zu NIS-konform – das IT-Sicherheitssystem im Check

Die Vorschriften rund um die NIS-Richtlinie hinterlassen möglicherweise bei dem ein oder anderen IT-Sicherheitsverantwortlichen im Krankenhaus ein mulmiges Gefühl in der Magengrube. Ist mein Krankenhaus sicher genug? Wo stehen wir aktuell? Geht's noch besser? Und kann mir da wer helfen?

Mit der NIS-Richtlinie – der Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union – hat sich die Europäische Kommission zum Ziel gesetzt, die Netzwerk- und Informationssicherheit in der EU zu verbessern. Dem Richtlinienentwurf der EU im Jahre 2013 folgte im Juli 2015 ein deutsches Gesetz, wonach sich Betreiber ‚kritischer Infrastrukturen', wozu Krankenhäuser zählen, ihre für die Versorgung der Bevölkerung kritischen Prozesse nach dem Stand der Technik absichern und diese gegenüber dem Bundesamt für Sicherheit in der Informationstechnik nachweisen müssen. Vor allem Krankenhäuser ab 30.000 stationären Fällen pro Jahr sind seit diesem Zeitpunkt besonders gefordert ihre Systeme zu durchleuchten und an die Richtlinie anzupassen, um sich abzusichern.

Schnell Handeln
Früh genug erkannt hat dies ein süddeutsches Krankenhaus und mit dem Aufbau eines Informationssicherheitsmanagementsystems (ISMS) begonnen. Als Unterstützung beauftragte es den IT-Dienstleister x-tention mit dem umfassenden IT-Security Compliance Check.

Der IT-Leiter des Krankenhauses berichtet über den Anstoß für das Projekt mit x-tention: „Wir arbeiten mit x-tention in anderen Bereichen bereits seit Jahren zusammen. Da wir x-tention als äußerst zuverlässigen Partner kennengelernt haben, und uns das vorgelegte Konzept zum Aufbau eines ISMS überzeugt hatte, fiel die Wahl leicht."

x-tention ist IT-Sicherheitsexperte im Gesundheitswesen und selbst Betreiber kritischer Infrastruktur. „Die NIS-Richtlinie betrifft rund 100 Krankenhäuser in Deutschland. Für einige durften wir bereits ein ISMS aufbauen und sie bis zur NIS-Konformität und darüber hinaus begleiten" berichtet Bernhard Kronsteiner, Geschäftsführer von x-tention Deutschland.

ISO/IEC 27001 Compliance Check
Die ‚Begleitung' zum ISMS ist eigentlich ein umfangreiches methodisches Vorgehen, das strukturierte Prozessabschnitte durchläuft und eine intensive Zusammenarbeit zwischen dem x-tention Projektleiter und dem Kunden voraussetzt. „Die Zusammenarbeit mit x-tention verlief völlig reibungslos. Die Berater haben unsere Bedürfnisse verstanden, und uns optimal auf dem Weg zum ISMS begleitet", berichtet der IT-Leiter der betreuten Klinik.

Begonnen wird bei x-tention mit dem IT Security Health Check, der den Status Quo beim Kunden ermittelt und einen Überblick über die umgesetzten Informationssicherheitsmaßnahmen gibt. Hier wird in Erfahrung gebracht, welche Dinge bereits sehr gut funktionieren und wo noch Maßnahmen zu setzen sind, um die Informationssicherheit zu erhöhen. Am Anfang wird immer ein Gesamtbild

geschaffen; die Projektleiterin des ISO/IEC 27001 Compliance Checks bei der süddeutschen Klinik, Sabrina Würflinger, erklärt: „Der Kunde will wissen wo er denn sicherheitstechnisch überhaupt steht – diesen Überblick geben wir ihm." In einem zweiten Schritt wird die Compliance zur ISO/IEC 27001 sondiert und es erfolgt die Dokumentensichtung. Inspiziert wird, ob und inwieweit die vorhandenen Dokumente bereits den Normanforderungen entsprechen.

So richtig ans Eingemachte geht es bei der Prüfung der Kernanforderungen an das Managementsystem der Kapitel 4 bis 10 der ISO/IEC 27001. Die verschiedenen Themenbereiche werden genauestens durchleuchtet, u.a. Sicherheitsrichtlinien und -ziele, Rollen- und Verantwortlichkeitsdefinitionen, Awareness-Programm, interne Audits, Informationssicherheits-Risikomanagement, Kennzahlen und Management Review. Zusätzlich wird der Erfüllungsgrad der einzelnen Controls des Annex A bewertet. „Wir schauen uns alles individuell und sehr detailliert an. Im Falle dieses Krankenhauses waren wir zwei Tage vor Ort und haben die Gegebenheiten beurteilt und dokumentiert. Außerdem wurde eine Begehung des Serverraumes durchgeführt", berichtet Würflinger.

Sind alle Tests abgeschlossen, erhält der Kunde seinen Abschlussbericht und in einer Präsentation werden die Ergebnisse grafisch aufbereitet. Den Sicherheitsverantwortlichen der Klinik wurden hier bereits erste Handlungsempfehlungen und Maßnahmen nahegelegt. „Wir hatten bislang noch keinen Kunden, wo gänzlich alle Richtlinien erfüllt waren. Aber genau dazu sind wir ja da – wir decken die Verbesserungspotentiale auf", untermauert Kronsteiner den x-tention Part.

Doch der Job für x-tention ist hiermit keineswegs beendet. Ist es Wunsch des Kunden, werden die erforderlichen Maßnahmen auch umgesetzt und ein IT-Sicherheitsbeauftragter von x-tention zur Verfügung gestellt.

Kleinere Krankenhäuser ziehen nach

„Wir erkennen den Trend, dass jetzt schon Krankenhäuser nachziehen, die nicht unter die NIS-Richtlinie fallen", berichtet Kronsteiner über aktuelle Entwicklungen. Obwohl Krankenhäuser mit weniger stationären Fällen als 30.000 pro Jahr den Gesetzesdruck der NIS-Richtlinie noch nicht verspüren, haben bereits einige entschieden, mit einem Informationssicherheitsmanagementsystem für die Zukunft gerüstet sein zu wollen. Munkelt man doch bereits, dass die Regelung bald auch auf kleinere Institutionen ausgeweitet werden soll.

Immer aktueller Branchenvergleich

Nicht nur in der Wirtschaft ist der Wettbewerb groß, sondern auch Gesundheits- und Sozialeinrichtungen sind angehalten, sich attraktiv für Mitarbeiter und Patienten zu präsentieren. Wer genau wissen möchte, wo er hinsichtlich Informationssicherheit und Datenschutz im Vergleich zum Mitbewerb liegt, ist mit dem x-tention D-A-CH IT Security Benchmark gut beraten.

In den letzten zwei Jahren hat x-tention IT Security Health Checks bei mehr als 20 Trägern aus dem Gesundheits- und Sozialwesen, bestehend aus mehr als 150 Häusern und insgesamt 44.000 Betten durchgeführt. Alle Ergebnisse wurden im von x-tention entwickelten D-A-CH IT Security Benchmark zusammengeführt und bilden jetzt eine umfassende Datenbank, welche erlaubt, die IST-Situation eines Instituts der Branche gegenüberzustellen.

„Wir können damit die Frage, wie andere und vergleichbare Einrichtungen im Gesundheits- und Sozialwesen mit den Herausforderungen hinsichtlich Informationssicherheit und Datenschutz umgehen, sehr gut beantworten", bekräftigt x-tention CISO Michael Punz.

„Seit Anfang des Jahres bieten wir außerdem eine Weiterentwicklung des Benchmark-Tools an, bei dem unsere Kunden IT Security Health Checks nicht nur selbst durchführen können, sondern auch individuelle Auswertungen und sogar angepasste Fragenkataloge aus den Bereichen Informationssicherheit und Datenschutz dynamisch erstellen können. Dadurch kann eine größtmögliche Flexibilität und Anpassbarkeit an die Organisation unserer Kunden erreicht werden."

Software as a Service für Health Check und Benchmark
Unabhängigkeit und Aktualität sind die zwei großen Schlagworte des neuen x-tention Angebotes „Software as a Service für den D-A-CH IT Security Benchmark".

Unabhängigkeit deshalb, weil für Institutionen des Gesundheits- und Sozialwesens jederzeit die Möglichkeit besteht, für all ihre Häuser Security Checks durchzuführen. Durch den vordefinierten, modular aufgebauten Fragenkatalog mit 224 Fragen erhält der Kunde vergleichbare Ergebnisse. „Unsere Kunden können so z.B. fünf ihrer Standorte auditieren und in Vergleich zueinander setzen oder eine Auswertung in Vergleich zum Benchmark ziehen", erläutert Punz. Der Vergleich zum Benchmark erfolgt in einer der Kategorien „Krankenhaus", „Soziale Einrichtung", „Bildungs- und Forschungseinrichtung" oder „Sonstige".

Aktualität deshalb, weil jedes Health Check Ergebnis wiederum in die Gesamtauswertung im Benchmark miteinfließt. Auch die daraus resultierenden Handlungsempfehlungen erfolgen gemäß dem letzten Stand der Technik. Zugleich sind die Sicherheit und der Schutz der vertraulichen Kundendaten oberstes Gebot. Sämtliche Auswertungen werden anonymisiert aufbereitet, sodass nie ein Rückschluss auf einzelne Organisationen ermöglicht wird. Zudem wird der Benchmark-Service ausschließlich in dem seit 2011 durchgängig nach ISO/IEC 27001 zertifizierten Sicherheits-Rechenzentrum von x-tention in Österreich betrieben.

Alle Fragen wurden von x-tention entwickelt, jedoch stark an internationalen Normen wie der ISO/IEC 27001 und dem BSI IT-Grundschutz ausgerichtet. „Die Tatsache, dass x-tention selbst kritische Infrastruktur betreibt, jahrelange Erfahrung im Gesundheits- und Sozialwesen mitbringt und den Benchmark als Software as a Service anbietet, macht uns am deutschen Markt einzigartig", unterstreicht x-tention Geschäftsführer Bernhard Kronsteiner.

Kontakt

Bernhard Kronsteiner, bernhard.kronsteiner@x-tention.de
x-tention Informationstechnologie GmbH
Bürgermeister-Wegele-Str. 12, 86167 Augsburg, Deutschland
tel + 49 821 / 56747 430