KRITIS in Krankenhäusern – Wie sieht eine Prüfung in der Praxis aus und was sind die Lessons Learned?

Vortrag

Datum	Zeit	Ort
22. April 2020	10:50 - 11:10 Uhr	_Stage A, Halle 6.2

Digitalisierung, Vernetzung und neue Technologien für die medizinische Versorgung von Patienten sind noch immer eine Herausforderung für IT-Sicherheitspersonal in Kliniken. Die schiere Menge an IT-sicherheitsrelevanten Themen stellt in diesem Zusammenhang die wohl größte Herausforderung dar. Um ein Mindestmaß an IT-Sicherheit für Kliniken sicherzustellen, hat der Gesetzgeber mit dem IT-Sicherheitsgesetz einen Rahmen geschaffen. Knapp 2.000 deutsche Kraneknhäuser befanden und befinden sich immer noch in der Umsetzung dieses Gesetzes. Welche Lessons Learned aus der Umsetzung sowie aus der Prüfung der Kliniken gibt es?

Neue Technologien, Digitalisierung und Vernetzung in der Medizin eröffnen großartige Möglichkeiten, bergen bei genauerem Hinsehen jedoch auch erhebliche Gefahren. Die Zahl der Cyber-Angriffe sowie der Schadprogramme steigt durch die sich kontinuierlich fortentwickelten digitalen Innovationen und Treiber jährlich an. Cyber-Kriminalität ist mittlerweile in allen Branchen und für alle Unternehmensgrößen von Relevanz. Gerade für medizinische Einrichtungen jeglicher Art ist sie eine große Gefahr.

Im einfachsten und wahrscheinlichsten Fall entstehen finanzielle Schäden und/oder Reputationsverluste. Im schlimmsten Fall kommen Patienten zu Schaden. Die Bandbreite an potentiellen Szenarien ist groß: ob sorglose Nutzer von Krankenhaus-IT, unzureichend geschützte Netzwerke und Medizintechnik bis hin zu einer äußerst komplexen IT-Landschaft, die nicht mehr so einfach zu überblicken und zu steuern ist – alles sind Sicherheitslücken.

Um kritische Infrastruktur wie die von Krankenhäuser zu schützen, verabschiedete der Gesetzgeber bereits vor einigen Jahren das IT-Sicherheitsgesetz. Eine Rechtsverordnung regelt, was kritische Infrastrukturen in Deutschland sind. Ein weiteres Gesetz, das BSI-Gesetz, regelt die Prüfung jener kritischen Infrastrukturen.

Die erste Welle an sogenannten Nachweisprüfungen gem. §8a (3) BSIG sind bereits im Jahr 2018 durch die im Korb 1 befindlichen Sektoren und Branchen im BSI eingegangen. Die zweite Welle in diesem Jahr verpflichtete auch den kompletten Gesundheitssektor und die Branche der medizinischen Versorgung zur Umsetzung der gesetzlichen Vorgaben und damit das Einreichen einer o.g. Nachweisprüfung. Doch was sind die wesentlichen Erkenntnisse und Erfahrungen aus den Prüfungen. Ein Prüfer berichtet aus seinem Prüferalltag in deutschen Kliniken.

Folgende praktische Themen- und Fragestellungen ergeben sich für die Kliniken:

- Bin ich überhaupt betroffen?
- Wie lege ich den Geltungsbereich fest?
- Was ist ein B3S und warum ist er für die Prüfung von Bedeutung?
- Welche kritischen Prozesse und Systeme sind betroffen?
- Wie sieht der Ablauf der Nachweisprüfung in der Praxis aus?
- Welche Dokumente sind von Relevanz? Was ist besonders wichtig?
- Nach der Prüfung ist vor der Prüfung – was gilt es für die nächste Prüfung zu berücksichtigen?
- Was sind die TOP 10 der häufigsten festgestellten Sicherheitsmängel?

Das Ziel des Vortrages ist es, mit praxisnahen Beispielen und Erfahrungen aus dem Prüfungsalltag, dem Auditorium einen Einblick in die Welt der Nachweisprüfungen zu geben sowie wichtige Eckpunkte der Prüfung sowie häufig auftretende Feststellungen bzw. Sicherheitsmängel vorzustellen.

Der Vortrag wird dialogbasiert durchgeführt. Praxisbeispiele lockern die Ausführungen auf. Der Erkenntnisgewinn der Zuhörer wird durch eigene Fragestellungen und damit verbundene Antworten weiter erhöht.

Akteure

Speaker:

Marcel Kunze, Manager, Consulting – Cyber Security, KPMG AG Wirtschaftsprüfungsgesellschaft