

IT-Sicherheitsgesetz / UP-KRITIS

Welche Krankenhäuser sind betroffen?

Aktuell werden als KRITIS-Häuser nur Regel- und Maximalversorger sowie Unfallkrankenhäuser betrachtet. Der gesamte ambulante Sektor einschließlich MVZs bleibt außen vor. Es ist derzeit noch offen ob und wie psychiatrische Häuser aufgenommen werden. Auch die Labore und Blutbanken der Kliniken könnten vom Standard erfasst werden, wenn diese externe Dienstleistungen anbieten.

Die konkreten Kriterien werden aktuell noch definiert.

Nach aktuellem Stand wird folgendes Kriterium herangezogen: Die stationäre Fallzahl je Standort (gemäß Feststellungsbescheides des Gesundheitsministeriums). Dieses Kriterium hat auch die DKG befürwortet. Der finale Vorschlag wird Ende

Oktober 2016 erwartet.

Kurzfasit

- Die Benennung eines IT-Sicherheitsbeauftragten wird Zwang.
- Die Einführung eines ISMS wird gefordert
- Zur Vermeidung wirtschaftlicher Risiken benötigt der AK-IT die Rückmeldung der Geschäftsführung zum Scope
- Der AK-IT schlägt den Geschäftsführern vor, dass alle AKG-Häuser sich gemeinsam einen externen Partner für die Auditierungen auszusuchen
- Die voraussichtlichen Kosten und Personalressourcen sind zum heutigen Zeitpunkt nicht abschätzbar
- Zum heutigen Zeitpunkt gibt es keine Zusage zur Finanzierung

Scope

Der „Scope“ ist die stationäre Versorgungsleistung des Krankenhauses, die auch in kritischen Situationen erbracht werden muss. Für diese Bereiche müsste dann die Kritikalität der darin zum Einsatz kommenden IT-Systeme bestimmt werden und für die kritischen Systeme der Branchenstandard und die Auditierung Anwendung finden.

Daraus wird direkt der Aufwand für die Häuser ableitbar sein. Hier benötigt die AK-IT einen Rücklauf der Geschäftsführer wie der Scope definiert werden muss. Dieser Rücklauf wird kurzfristig für Berücksichtigung im Branchenarbeitskreis benötigt.

Zusammensetzung des Branchenarbeitskreises (BAK)

Der Branchenarbeitskreis ist ein vom BSI eingesetzter Arbeitskreis, der den Vorschlag für die Rechtsverordnung erarbeiten soll. Obwohl unterschiedliche Verbände und Krankenhausformen vertreten sind, ziehen derzeit alle am gleichen Strang und vertreten keine Partikulärinteressen.

Ein besseres Einwirken auf die Erstellung eines Branchenstandards im Sinne der Kliniken kann durch die Teilnahme weiterer KH im BAK erfolgen.

Branchenstandard

Der Branchenstandard (B3S), welcher vom Branchenarbeitskreis (BAK) erstellt wird, stellt die spezifischen Prüf- und Anforderungskriterien für die Gesundheitsversorgung dar. Das Ziel der KH-Vertreter im BAK ist es, die Anforderungen des B3S geringer zu halten als die sehr umfänglichen Standards BSI-Grundschrift und ISO 27000.

Der BAK ist vom BSI legitimiert worden, die Grunddefinitionen im Standard festzulegen. Hiervon wird direkt der Aufwand abhängen, welche die Kliniken einbringen müssen. Über die DKG wurde ein Budget für die Erarbeitung von Krankenhausvorschlägen eingestellt.

Auditierung

Künftig werden die Kliniken hinsichtlich des Branchenstandards alle 2 Jahre auditiert werden. Der vom Gesetz geforderte und verpflichtende Auditierungsnachweis wird nach aktuellem Stand nicht ganz so hoch angesetzt sein, wie der einer Zertifizierung nach z.B. IT-Grundschutz.

Im Rahmen der Auditierung werden auch die Anforderungen an die **prüfende Stelle definiert**. Es wird nicht möglich sein sog. Peer-Review's wie bei der QS im med. Bereich durchzuführen.

Es werden eher vgl. anderer Branchen kommerzielle Partner wie z.B. DEKRA und TÜV geben, welche die Audits ausführen. Hierzu benötigt die prüfenden Stellen Kompetenzen in den Bereichen: Audit, Sicherheit, IT und Branchenwissen, auf welche die Prüfverfahren des Branchenstandards angewandt werden müssen.

Zeitschiene

Bis Ende 2016	Rechtsverordnung (RV) geht in Ressortabstimmung.
Q1/2017	Abstimmung zur RV in den Gremien.
Q2/2017	Verabschiedung RV.
6 Monate ab Freigabe RV	In dieser Zeit müssen die Krankenhäuser welche die KRITIS Kriterien erfüllen eine sog. Selbstanzeige beim BSI durchführen.
2 Jahre ab Freigabe RV	Spätestens 2 Jahre nach Verabschiedung der Rechtsverordnung müssen die Häuser welche die B3S Kriterien für KRITIS erfüllen auditiert sein.
ca. Mitte 2017	Branchenstandard finalisiert Die Umsetzungszeit läuft unabhängig von der Freigabe der Branchenstandards ab Freigabe RV.

To-Dos / Entscheidungen GFs

- Die AK-IT will über einen Workshop Vorschläge zur Einreichung des Branchenstandards erarbeiten und beisteuern, um die Interessen unserer Kliniken bestmöglich zu vertreten. Der Vorschlag soll über die DKG eingestellt werden, welche über ein Projektbudget zur Ausarbeitung verfügt.
- Wir raten den Unternehmensleitungen in den Häusern dringend ein so genanntes **Informationssicherheit-Management-System (ISMS)** in 2017 zu etablieren. Hierfür sollte kurzfristig zumindest ein Team für die Erstaufnahme benannt und mit Ressourcen versehen werden. Der Umsetzungszeitrahmen nach der Freigabe RV ist mehr als ambitioniert. **Der Aufwand ist wegen fehlender Festlegung des Scopes zum heutigen Zeitpunkt nicht kalkulierbar.**
Der AK-IT wird das Thema ISMS im nächsten Jahr bearbeiten. Basis für das ISMS ist die Freigabe der sog. A0-Dokumentation (BSI), welche die Etablierung und organisatorische Integration regelt.
- Es wird dringend empfohlen, dass jede Klinik verbindlich Mitarbeiterressourcen freistellen muss und in die AG des AK-IT entsendet. Nur bei einer verbindlichen Zusage über die Geschäftsführung werden Synergieeffekte und Aufwandsreduktionen für alle erzielt werden können.
- Der AK-IT schlägt den Geschäftsführern konkret vor, dass alle AKG-Häuser sich gemeinsam einen externen Partner für die Auditierungen aussuchen. Ziel wäre, dass der AK-IT den Partner beim Aufbau von Branchenknowhow unterstützt und im Gegenzug erhalten die KH-Mitarbeiter eine Auditorenausbildung. Der externe Auditaufwand wird derzeit mit 20-30 Manntagen veranschlagt, weshalb hierdurch erhebliches Kosten-/Nutzenpotential für die Häuser entstehen kann.

Fazit:

Die Unternehmensführung und die IT stehen für diese Themen in der persönlichen Haftung und müssen in diesem Themenumfeld dringend konkrete Maßnahmen ergreifen.