WHITEPAPER

ENJOY SAFER TECHNOLOGY™

Cybersicherheit auch für Nicht-KRITIS: Was bringen IT-Sicherheitsgesetz 2.0, PDSG und KHZG?

ESET.DE | ESET.AT | ESET.CH

ENJOY SAFER TECHNOLOGY™

Cybersicherheit auch für Nicht-KRITIS: **Was bringen IT-Sicherheitsgesetz 2.0, PDSG und KHZG?**

EXECUTIVE SUMMARY

Die Schlagzahl der gesetzlichen Auflagen für IT-Sicherheit im Krankenhaus wird immer höher: 2015 wurde das erste IT-Sicherheitsgesetz verabschiedet, das die IT-Sicherheitsmaßnahmen für Krankenhäuser ab 30.000 vollstationären Fällen im Jahr regelte.

Im Oktober 2020 kam das Patientendaten-schutzgesetz (PDSG), das unter Einführung des §75c in das SGB V ähnlich strenge Auflagen auch für Kliniken unter der KRITIS-Grenze macht. Nach langer Vorbereitung und lebhafter Diskussion ist nun im April 2021 das IT-Sicherheitsgesetz 2.0 verabschiedet worden, das die Inhalte seines Vorgängers weiter verschärft.

Seit Anfang 2021 ist die finanzielle Förderung von Digitalisierungsprojekten in Kliniken nach dem Krankenhauszukunftsgesetz (KHZG) möglich, und auch hier spielt IT-Sicherheit eine wesentliche Rolle: Es ist eigener Fördertatbestand, aber auch „integraler Bestandteil aller Fördermaßnahmen".

Nicht zuletzt ist IT-Sicherheit, neben den gesetzlichen Vorgaben, auch essenziell, um den Betrieb und Fortbestand Ihres Hauses zu sichern. Seit Jahren ist das Gesundheitswesen Ziel von immer neuen Typen von Schadsoftware und anderen Angriffen. Finanzieller Schaden in Millionenhöhe, nachhaltige Rufschädigung und sogar Schäden an Leib und Leben von Patientinnen und Patienten waren bisher die Folgen.

Behörden und Gesetzgeber stellen aber nicht nur Ansprüche an Krankenhäuser, sondern bieten auch gewisse Hilfestellungen: Mit dem Branchenspezifischen Sicherheitsstandard (B3S) für die Gesundheitsversorgung im Krankenhaus werden Richtlinien vorgegeben, die pragmatischer umzusetzen sind als die sehr detaillierten und teils komplexen Vorgaben aus Informationssicherheitsmanagementsystemen (ISMS) wie der ISO 27001.

Zudem wurde endlich auch finanzielle Unterstützung für die Digitalisierung und Cybersicherheit von Krankenhäusern bereitgestellt, in Form des bereits genannten KHZG mit seinem Krankenhauszukunftsfonds (KHZF), der 3 Milliarden Euro aus Bundesmitteln enthält, die mit weiteren bis zu 1,3 Milliarden aus den Bundesländern ergänzt werden. Förderprojekte können über das jeweilige Bundesland für ein Krankenhaus beantragt werden, und zwar noch bis Ende 2021.

ESET als inhabergeführtes und EU-ansässiges Unternehmen mit über 30 Jahren Erfahrung für umfassende Sicherheitslösungen, die perfekt auf die Security-Anforderungen auch im Healthcare-Bereich abgestimmt sind, beantwortet Ihnen gern Ihre Fragen zum Fördertatbestand Cybersicherheit im KHZG. Mit unserem Produkt ESET PROTECT und unserer umfassenden Lösung ESET PROTECT Enterprise machen wir es Ihnen leicht, die Anforderungen des B3S für die Gesundheitsversorgung im Krankenhaus zu erfüllen und damit konform mit dem PDSG und mit dem ersten und zweiten IT-Sicherheitsgesetz zu handeln. Betriebsausfälle, Gefährdung der Patientensicherheit und Ihres guten Rufs sowie Haftungsrisiken werden reduziert. Ihr Haus wird zukunftssicher aufgestellt.

Vereinbaren Sie noch heute ein unverbindliches Beratungsgespräch, um die Erfüllung Ihrer gesetzlichen Pflichten und eine rechtzeitige Antragstellung für finanzielle Förderung nach KHZG bis Ende 2021 zu besprechen.

Wir stehen Ihnen zur Verfügung:

MAIK WETZEL

Strategic Business Development Director DACH

vertrieb@eset.de / www.eset.de/health

INHALTSVERZEICHNIS

KRANKENHÄUSER: DEUTSCHLANDS WICHTIGSTE INFRASTRUKTUR

Was braucht es, um das Alltagsleben in Deutschland komplett lahmzulegen?

Mit zunehmender Digitalisierung aller Arbeits- und Lebensbereiche lautet die Antwort: Nur einen effektiven Cyberangriff.

Von allen potenziellen Gefahren für Unternehmen und Einrichtungen in Deutschland nimmt die Bedrohung durch Cyberangriffe am stärksten zu, denn:

- Immer mehr Strukturen und Prozesse sind teilweise oder komplett digital – also angreifbar.
- Potenzielle Angreifer können nicht nur vor Ort, sondern von überall auf der Welt her zuschlagen.

Die Beeinträchtigung bestimmter Einrichtungen – etwa durch einen Cyberangriff – hätte fatale Folgen für Leib und Leben der Bevölkerung, weil es etwa zu Versorgungsengpässen oder Störungen der öffentlichen Sicherheit kommen würde. Diese Strukturen werden in Deutschland als Kritische Infrastrukturen (KRITIS) bezeichnet. Hierzu gehören etwa die Sektoren Energie, IT, Telekommunikation, Transport und Verkehr, Wasser, Ernährung sowie Finanz- und Versicherungswesen – und das Gesundheitswesen.

CYBERATTACKE KOSTET LUKAS-KRANKENHAUS EINE MILLION EURO

Krankenhäuser und Kliniken sind ganz klar eine der wichtigsten Infrastrukturen der Bundesrepublik. Ihr besonderer Schutzbedarf wurde spätestens durch die zahlreichen Ransomware-Attacken der letzten Jahre belegt.

Hohe Wellen schlug der Ransomware-Angriff auf das Lukaskrankenhaus in Neuss im Februar 2016. Den meisten IT-Verantwortlichen im Gesundheitswesen waren Cyberangriffe zuvor als theoretische Möglichkeit bekannt. Doch erst dieser bundesweit publizierte Vorfall schaffte ein Bewusstsein dafür, wie dringlich Investitionen in Cybersicherheit im Krankenhaussektor nötig waren und sind.

Eine Analyse der Neusser Ransomware-Attacke ein Jahr später ergab, dass sie das Krankenhaus eine Million Euro allein im Bereich der IT gekostet hatte[1] - die Rufschädigung und den tatsächlichen Schaden an Leib und Leben für Patienten sind schwerer zu beziffern und daher in dieser Zahl noch gar nicht berücksichtigt. Im September 2020 verstarb beispielsweise eine Patientin der Uniklinik Düsseldorf, die aufgrund von Betriebseinschränkungen wegen einer anderen Ransomware-Attacke verlegt werden musste.

1 Heise Medien GmbH & Co. KG: Trojaner im OP - wie ein Krankenhaus mit den Folgen lebt (https://www.heise.de/newsticker/meldung/Trojaner-im-OP-wie-ein-Krankenhaus-mit-den-Folgen-lebt-3617880.html, Aufruf 02.06.2021)

SCHÄDEN DURCH CYBERATTACKEN: MENSCHENLEBEN IN GEFAHR, GESCHÄFTSFÜHRER HAFTEN

Wichtig für alle Entscheidungsträger im Krankenhaus: Die Geschäftsführung haftet im Zweifelsfall für alle aus Cyberattacken resultierenden Schäden. Diese umfassen bei weitem nicht nur die Kosten für die Wiederherstellung des Systems: Hinzu kommen Umsatzeinbußen, Kosten für die Ursachenermittlung (Forensik) sowie die Zahlung von Bußgeldern und Schadenersatz.

Schadenersatzpflicht gegenüber Dritten im Fall eines Cyberangriffs kann gegenüber Lieferanten und Zuweisern bestehen, und ganz besonders natürlich gegenüber Patientinnen und Patienten. Hier wird zum einen die Vertraulichkeit personenbezogener Daten gefährdet, zum anderen die körperliche Unversehrtheit und gar das Überleben. Zudem können Bußgelder nach Art. 82 und 83 der DSGVO anfallen, die mit bis zu 20 Millionen Euro oder 4% des weltweiten Jahresumsatzes eines Unternehmens (es gilt der höhere Betrag) extrem schmerzhaft sind. Und selbst bei nachgewiesen fahrlässigem Verhalten von Mitarbeiterinnen und Mitarbeitern kann ein Rückgriff auf diese, abhängig vom Grad der Fahrlässigkeit, nur in geringem Umfang möglich sein.

All diese Haftungsrisiken können nur vermieden werden, wenn die Geschäftsführung klar nachweisen kann, dass die IT-Sicherheit zum Zeitpunkt des Angriffs auf dem Stand der Technik war.

Die aus den Schlagzeilen bekannte Ransomware ist nur ein möglicher Angriff auf ein Krankenhausnetz. Es gibt zahlreiche weitere Arten von bösartigen Programmen (Malware), und darüber hinaus andere, gezieltere Attacken auf Rechnernetze. Es genügt daher nicht, eine Klinik immer nur gegen einzelne Gefahren oder bekannte Sicherheitslücken abzusichern: Eine übergreifende Strategie und ein umfassendes Management der IT-Sicherheit müssen her.

Wie man ein solches einrichtet, das geben sogenannte IT-Sicherheits-Management-Systeme oder ISMS vor. Ein weit verbreitetes und sehr umfassendes Modell ist etwa das ISMS nach DIN EN ISO 27001.

KRANKENHÄUSER: KRITISCHE INFRASTRUKTUR ODER NICHT?

Die Einrichtung und Pflege eines ISMS ist eine der wichtigsten Pflichten, die das erste IT-Sicherheitsgesetz KRITIS-Krankenhäusern auferlegt hat.

Dem Gesetz nach werden allerdings nicht alle Krankenhäuser und Kliniken zu den KRITIS gezählt, sondern nur solche, die mindestens 30.000 vollstationäre Fälle pro Jahr behandeln. Sie stellen innerhalb des Gesundheitswesens die Branche Medizinische Versorgung dar. Darüber hinaus gelten die Vorschriften auch für die Branchen Labore und Pharma im KRITIS-Sektor Gesundheitswesen.

Die Betreiber solcher großen Kliniken müssen seit dem ersten IT-Sicherheitsgesetz (verabschiedet 2015) folgende Auflagen erfüllen:

- Sie müssen alle zwei Jahre nachweisen, dass sie in Bezug auf IT-Sicherheit auf dem „Stand der Technik“ sind. Dieser Nachweis kann durch Zertifizierung und Rezertifizierung eines Informationssicherheitsmanagementsystems (ISMS) nach ISO 27001 erfolgen. Eine andere Möglichkeit ist der Nachweis der Einhaltung des Branchenspezifischen Sicherheitsstandards (B3S) für das Gesundheitswesen.
- Sie müssen die IT-Sicherheitsvorfälle, die die Funktionsfähigkeit der KRITIS beeinträchtigen können, an das Bundesamt für Sicherheit in der Informationstechnik (BSI) melden und einen konkreten Ansprechpartner für das BSI benennen.

Gesetze, die durch das erste IT-Sicherheitsgesetz geändert und ergänzt wurden, sind insbesondere das BSI-Gesetz, das Energiewirtschaftsgesetz, das Telemediengesetz und das Telekommunikationsgesetz.

UPDATE FÜR IT-SICHERHEIT IN KRITIS: IT-SICHERHEITSGESETZ 2.0

Aber IT-Sicherheit und deren gesetzliche Regulierung sind nie ganz „fertig" – IT-Fachleute und Gesetzgeber auf der einen Seite und Angreifer auf der anderen Seite befinden sich in einem steten Wettlauf.

Im April 2021 hat der Bundestag daher nach langer Vorbereitungszeit das IT-Sicherheitsgesetz 2.0 verabschiedet. Was bringt es Neues?

- Ab sofort müssen Betreiber von KRITIS auch ein Angriffserkennungssystem (Intrusion Detection System) zur automatisierten Erkennung von Angriffen aus dem Netz vorhalten.
- Das BSI wird gestärkt und erhält neue Befugnisse: Die Behörde darf jetzt auch aktiv nach Schwachstellen an fremden Servern suchen, etwa mit Portscans.

Auch das IT-Sicherheitsgesetz 2.0 regelt also die Sicherheit von Kliniken im KRITIS-Bereich. Zudem gilt es auch für Unternehmen von „erheblicher volkswirtschaftlicher Bedeutung", also voraussichtlich für große (etwa börsennotierte) Klinik-Ketten, deren Kliniken einzeln betrachtet nicht die KRITIS-Grenze von 30.000 Fällen erreichen. Konkret wird dies aber noch durch eine Rechtsverordnung festgelegt werden.

Das bedeutet allerdings nicht, dass es kleinen Kliniken freigestellt bleibt, ob und wie sie sich gegen Cyberattacken absichern. Im Oktober 2020 trat das Patientendatenschutzgesetz (PDSG) in Kraft, dessen Vorgaben alle Krankenhäuser in Deutschland betreffen.

PATIENTENDATENSCHUTZGESETZ (PDSG): IT-SICHERHEIT AUCH FÜR NICHT-KRITIS-KLINIKEN EIN MUSS

Mit dem PDSG wurde im Sozialgesetzbuch V (SGB V) der neue §75 c geschaffen. Er schreibt vor, dass zum 1. Januar 2022 alle Krankenhäuser „nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen" zum Schutz ihrer IT-Infrastruktur treffen und mindestens alle zwei Jahre aktualisieren müssen.

Ausdrücklich weist §75 c darauf hin, dass die Krankenhäuser dieser Pflicht genügen können, indem sie den durch das BSI zugelassenen Branchenspezifischen Sicherheitsstandard (B3S) umsetzen, der auch in KRITIS-Kliniken angewendet wird.

Das Fazit aus dem PDSG und §75 c SGB V: Ab dem 1. Januar 2022 gelten für Nicht-KRITIS-Kliniken fast genauso strenge Vorgaben in Bezug auf Cybersicherheit wie für KRITIS-Kliniken.

B3S: PRAGMATISCH UND BASIEREND AUF ISO-NORMEN

Der Branchenspezifische Sicherheitsstandard (B3S) für die Gesundheitsversorgung im Krankenhaus wurde von der Deutschen Krankenhausgesellschaft (DKG) erarbeitet und durch das BSI zertifiziert. Die jeweils aktuelle Fassung findet sich auf den Webseiten der DKG (www.dkgev.de).

Anstoß für die Entwicklung des B3S war zwar das erste IT-Sicherheitsgesetz – er wurde also ausgehend von den Verhältnissen in KRITIS-Krankenhäusern erstellt. Mit der Erwähnung im PDSG werden diese Verhältnisse jetzt jedoch auf alle anderen Krankenhäuser übertragen.

Grundlage für den B3S für die Gesundheitsversorgung im Krankenhaus ist die schon oben erwähnte Norm ISO 27001, die weltweit zur Zertifizierung von ISMS angewandt wird.

Zusätzlich fließt die Norm ISO 27799 Medizinische Informatik – Sicherheitsmanagement im Gesundheitswesen mit ein. Für den Bereich des Risikomanagements in den B3S wird außerdem die ISO 80001 „Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten" hinzugezogen.

Es wurden aus diesen Normen aber nur diejenigen Anforderungen mit in den B3S aufgenommen, die für die Zielgruppe Krankenhäuser relevant sind. Eine ISO-Zertifizierung eines ISMS ist ausdrücklich nicht notwendig, damit ein Krankenhaus die Umsetzung der B3S für die Gesundheitsversorgung im Krankenhaus nachweisen kann.

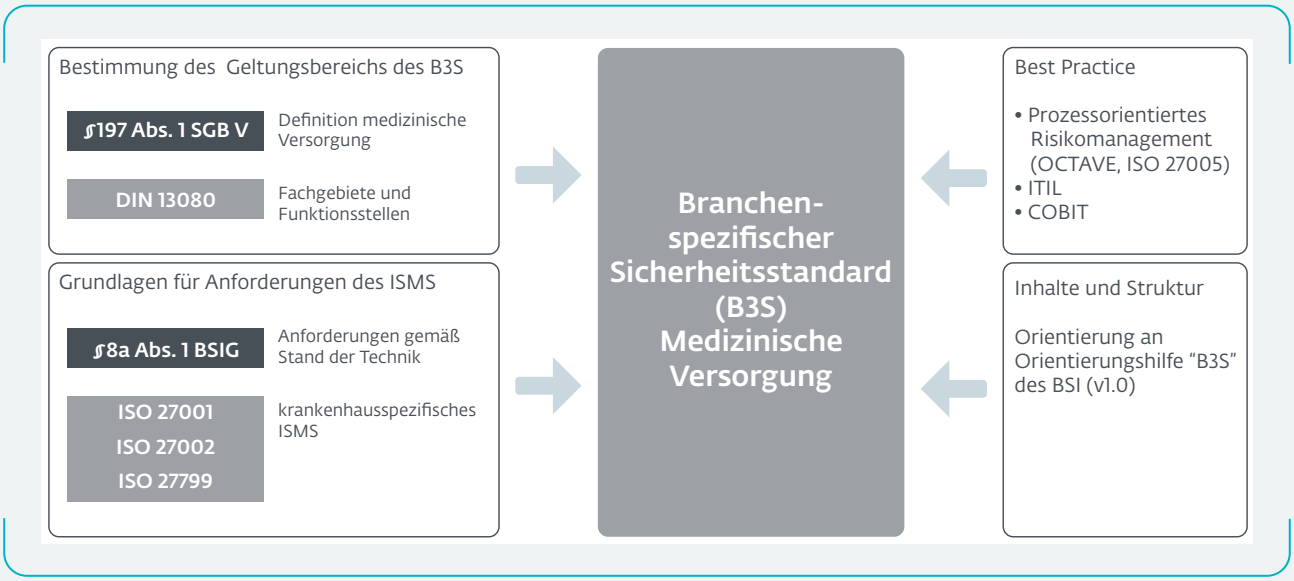

Abbildung 1: Quellen und Grundlagen des B3S (Deutsche Krankenhausgesellschaft e. V.)[2]

2 Deutsche Krankenhausgesellschaft e. V.: Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus, v1.1, S. 9 (https://www.dkgev.de/fileadmin/default/Mediapool/2_Themen/2.1_Digitalisierung_Daten/2.1.4._IT-Sicherheit_und_technischer_Datenschutz/2.1.4.1._IT-Sicherheit_im_Krankenhaus/B3S_KH_v1.1_8a_geprueft.pdf, Aufruf 02.06.2021)

KRITISCHE DIENSTLEISTUNG: STATIONÄRE MEDIZINISCHE VERSORGUNG

Mit den B3S soll stets die sogenannte kritische Dienstleistung (kDL) einer Branche abgesichert werden. Für die B3S für die Gesundheitsversorgung im Krankenhaus ist dies die stationäre medizinische Versorgung. Hierzu legt der B3S folgende Schutzziele fest:

- Verfügbarkeit
- Integrität
- Authentizität
- Vertraulichkeit
- Patientensicherheit
- Behandlungseffektivität

Neben den bekannten Schutzzielen der Informationssicherheit kommen also Patientensicherheit und Behandlungseffektivität als für die medizinische Versorgung spezifische Ziele hinzu.

Patientensicherheit im Sinne der B3S ist die Freiheit von unvertretbaren Risiken einer physischen Verletzung oder eines Schadens an der Gesundheit von Menschen, einschließlich nachhaltiger psychischer Belastungen.

Behandlungseffektivität im Sinne der B3S stellt die wirksame Behandlung des Patienten unter Benutzung von Informationen und wirksamen Therapiemaßnahmen sicher, wenn notwendig auch auf Basis eines Informationsaustausches zwischen unterschiedlichen verantwortlichen Organisationseinheiten.

BRANCHENSPEZIFISCHE GEFÄHRDUNGEN MANAGEN

Der entscheidende Vorteil von B3S gegenüber branchenneutralen ISMS wie ISO 27001: In Bezug auf branchenspezifische Gefährdungen muss das Rad nicht neu erfunden werden. Um die Umsetzung des B3S zu vereinfachen, sind diese von den Autoren der DKG bereits festgelegt worden, etwa im Kapitel „Branchenspezifische Gefährdungslage".

Solche Branchenspezifische Gefährdungen in der medizinischen Versorgung sind beispielsweise:

- Nichtverfügbarkeit wichtiger, medizinisch relevanter Daten
  - in der Diagnostik
  - in der Therapie
  - in der Pflege
  - im Entlassungsprozess
- Manipulation von wichtigen, medizinisch relevanten Daten
  - in der Diagnostik
  - in der Therapie
  - in der Pflege
  - im Entlassungsprozess
- Fremdsteuerung/Manipulation von Medizingeräten

und so weiter.

Zudem weist der B3S darauf hin, welche Technik- und Softwaresysteme für die Branche medizinische Versorgung in der Regel kritisch sind: etwa das Krankenhausinformationssystem (KIS), das Laborinformationssystem (LIS), das radiologische Informationssystem (RIS), die Medizintechnik (insbesondere die vernetzte), die Transportlogistik und andere.

Als nächstes wird festgelegt, wie das Informationssicherheitsmanagement einer Klinik aussehen muss, um mit diesen Bedrohungen umzugehen.

Die Benennung und Bestellung eines Informationssicherheitsbeauftragten wird dabei in den B3S ausdrücklich als notwendig herausgestellt.

Die B3S geben zusammenfassend schon konkrete Maßnahmen der Informationssicherheit vor, und zwar als MUSS-, SOLL- und KANN-Maßnahmen:

MUSS-Maßnahmen sind verpflichtend, auf SOLL-Maßnahmen kann nur in begründeten Ausnahmefällen verzichtet werden, KANN-Maßnahmen sind lediglich empfehlenswert.

Da sich vor allem hier der Stand der Technik abbildet, werden die B3S regelmäßig aktualisiert, voraussichtlich alle zwei Jahre. In der nächsten Version sollen der Umgang mit innovativen Untersuchungs- und Behandlungsverfahren sowie die Differenzierung von Anforderungen an Informationstechnik bzw. Medizintechnik in den Fokus rücken.

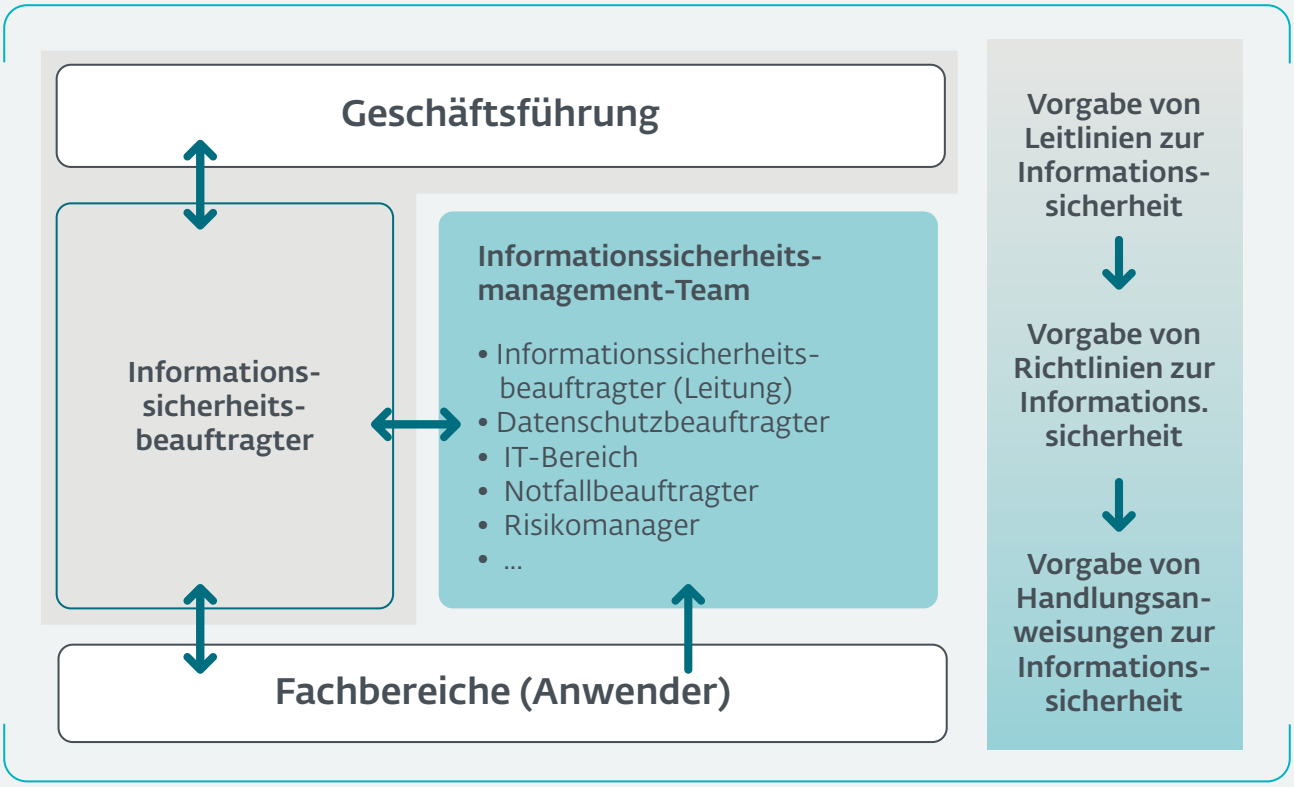

Abbildung 2: Management der Informationssicherheit im Krankenhaus (Deutsche Krankenhausgesellschaft e. V.)[3]

3 Deutsche Krankenhausgesellschaft e. V.: Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus, v1.1, S. 59 (https://www.dkgev.de/fileadmin/default/Mediapool/2_Themen/2.1_Digitalisierung_Daten/2.1.4._IT-Sicherheit_und_technischer_Datenschutz/2.1.4.1._IT-Sicherheit_im_Krankenhaus/B3S_KH_v1.1_8a_geprueft.pdf, Aufruf 02.06.2021)

KRANKENHAUSZUKUNFTSGESETZ (KHZG): 4,3 MRD. EUR FÜR DIGITALISIERUNG UND CYBERSICHERHEIT

Entscheidungsträger aus dem Gesundheitswesen haben die Politik immer wieder zu Recht darauf hingewiesen, wie schwer die Umsetzung angemessener IT-Sicherheitsmaßnahmen mit den begrenzten finanziellen und personellen Ressourcen der meisten Krankenhäuser ist. Die Mittel des alten Krankenhausstrukturfonds waren hierzu unzureichend und bei weitem nicht für alle Häuser zugänglich. Hinzu kommt aktuell die außerordentliche Belastung von Menschen und Strukturen im Gesundheitswesen durch die Corona-Pandemie.

Die Mahnungen haben Wirkung gezeigt, und es gibt nun Abhilfe seitens des Gesetzgebers: Im Krankenhauszukunftsgesetz (KHZG) wird ein Finanzierungstopf – der Krankenhauszukunftsfonds oder KHZF – des Bundesamtes für Soziale Sicherung (BAS) von 3 Milliarden Euro zur Verfügung gestellt, gewissermaßen als Krankenhausstrukturfonds 2.0.

CYBERSICHERHEIT: TEIL JEDES FÖRDERTATBESTANDES DES KHZG

Diese Mittel des KHZF können durch Projekte abgerufen werden, die die Modernisierung der Krankenhäuser zum Ziel haben. In erster Linie sind das natürlich Maßnahmen der Digitalisierung und damit verknüpft auch der Cybersicherheit, denn diese muss bei jeder Digitalisierungsmaßnahme von Anfang an mitgedacht werden.

So schreibt das BAS selbst, der Schwerpunkt der Fördermaßnahmen liege „auf der Digitalisierung der Ablauforganisation, Dokumentation und Kommunikation sowie der Verbesserung der Telemedizin, Robotik und Hightech-Medizin“, alles zum Zwecke einer Verbesserung der Patientenversorgung. Und: „Integraler Bestandteil aller Fördermaßnahmen sind Investitionen in die Informationssicherheit“.

Somit werden Fördermittel für die IT-Sicherheit in Krankenhäusern nicht nur in dedizierten IT-Sicherheitsprojekten vom BAS zur Verfügung gestellt, sondern im Prinzip als Teil jedes Förderprojekts, das beim BAS aus dem KHZF beantragt wird.

FÖRDERPROJEKT NACH KHZG RECHTZEITIG BEANTRAGEN

Die Antragstellung beim BAS für Förderung von Projekten nach KHZG ist seit Anfang 2021 möglich. Genau genommen erfolgt sie nicht durch das Krankenhaus selbst, denn Antragsteller können laut KHZG nur Bundesländer sein. Das Krankenhaus mit einer innovativen Idee und entsprechendem Bedarf sendet vielmehr eine Bedarfsmeldung an das Bundesland. Wie die Meldungen der Krankenhäuser bewertet und priorisiert werden, liegt in der Verantwortung des einzelnen Bundeslandes.

Das jeweilige Bundesland muss auch 30% des beantragten Fördervolumens für das Projekt als eigene Investition tragen. Trotzdem sind ausdrücklich auch länderübergreifende Projekte möglich und gewünscht.

Der Erfolg der Förderprojekte wird anhand einer digitalen Reifegradmessung ermittelt, die im Abstand von zwei Jahren den digitalen Reifegrad des Krankenhauses vor und nach Durchführung des Projektes ermittelt. Auch wenn ein Krankenhaus hier wenig Fortschritt zu verzeichnen hat, ist keine Rückforderung von Fördermitteln geplant – denn nicht alle Erfolge schlagen sich immer im digitalen Reifegrad nieder. Zurückgefordert werden können allerdings nicht verwendete Fördermittel.

Antragstellung für Förderprojekte nach KHZG ist noch bis Ende des Jahres 2021 möglich.

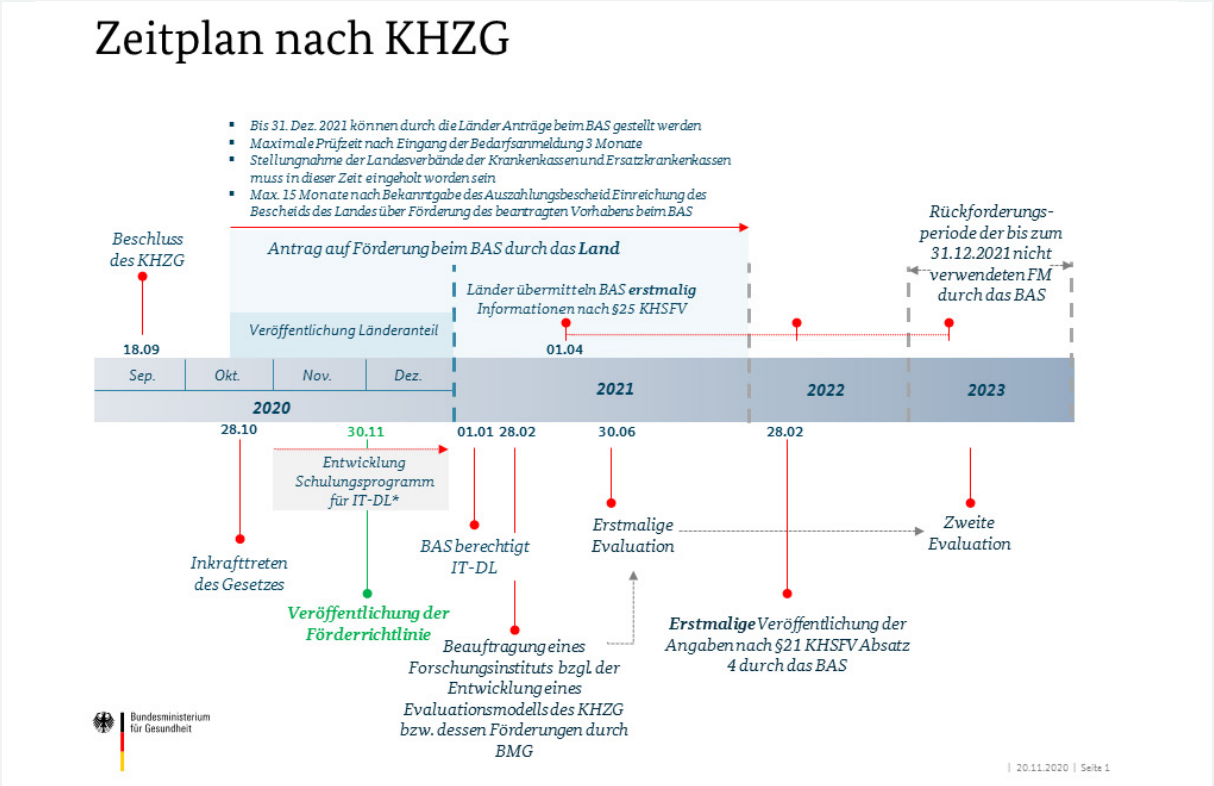

Abbildung 3: Zeitplan des KHZF (Bundesministerium für Gesundheit)[4]

4 Bundesministerium für Gesundheit: Krankenhauszukunftsgesetz für die Digitalisierung von Krankenhäusern (https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/GuV/K/Krankenhauszukunftsfonds_Zeitplanung.png, Aufruf 02.06.2021)

ESET: CYBERSICHERHEIT FÜR IHR KRANKENHAUS AUS EINER HAND

Im Angesicht dieser Herausforderungen stellt sich vor allem für Nicht-KRITIS-Kliniken die Frage, wie Lösungen aussehen können, die sowohl gesetzeskonform als auch effektiv und effizient sind – also die Klinik auch auf lange Sicht vor Bußgeldern und Haftungsrisiken bewahren und gleichzeitig auf schlanke Art und Weise wirksam die Patientenversorgung und das Vertrauen von Patienten und Beschäftigten sichern.

Unter dem derzeitigen Personal- und Ressourcendruck – noch einmal verschärft durch die Pandemie – lässt sich dies für kaum ein Haus aus eigenen Kräften stemmen. Hier kommt ESET ins Spiel: Seit über 30 Jahren entwickeln wir umfassende Sicherheitslösungen, die perfekt auf die Security-Bedürfnisse auch im Healthcare-Bereich abgestimmt sind. Als inhabergeführtes und EU-ansässiges Unternehmen legen wir besonderen Wert auf hochwertigen und fachlich qualifizierten deutschsprachigen Support, so dass Sie mit unseren Lösungen nie allein dastehen.

ESET PROTECT: NUTZERFREUNDLICH, UMFASSEND, B3S-KONFORM

Ganz oben auf unserer Prioritätenliste stehen Nutzerfreundlichkeit und Automatisierung: Wir wollen Ihnen und Ihren Mitarbeitern den Alltag so einfach und stressfrei wie möglich machen. Das erreichen wir mit der Integration unserer Werkzeuge in eine umfassende Management-Konsole ESET PROTECT, die für Echtzeit-Übersicht aller Endpoints und kinderleichte Verwaltung durch Ihre Administratoren sorgt, auch über mehrere Standorte hinweg.

Die meisten unserer Kunden im Gesundheitswesen entscheiden sich für die Lösung ESET PROTECT Enterprise. Diese sichert alle Server und Geräte in Ihrem Netzwerk durch mehrschichtige Sicherheitstechnologien ab und bietet dank der cloudbasierten Sandbox-Technologie einen besonders starken Schutz gegen Ransomware. Sensible Patientendaten bleiben durch Festplattenverschlüsselung auch bei Geräteverlust geschützt, sowohl unter Windows als auch macOS.

Durch die übersichtliche Darstellung des Sicherheitsstatus in ESET PROTECT lassen sich die in Ihrem Hause getroffenen Schutzmaßnahmen gegen Branchenspezifische Gefährdungen laut B3S für die Gesundheitsversorgung im Krankenhaus und damit die Konformität Ihres Hauses mit den Vorschriften des PDSG belegen.

IHR KOSTENLOSES BERATUNGSGESPRÄCH

Kontaktieren Sie uns noch heute, um sich unverbindlich zur Erfüllung Ihrer gesetzlichen Pflichten beraten zu lassen und von der finanziellen Förderung bis Ende 2021 zu profitieren:

MAIK WETZEL

Strategic Business Development Director DACH

vertrieb@eset.de / www.eset.de/health

ENJOY SAFER TECHNOLOGY™

Über ESET

Als europäischer Hersteller mit mehr als 30 Jahren Erfahrung bietet ESET ein breites Portfolio an Sicherheitslösungen für jede Unternehmensgröße. Wir schützen betriebssystemübergreifend sämtliche Endpoints und Server mit einer vielfach ausgezeichneten mehrschichtigen Technologie, unterstützen Ihren Datenschutz mit Hilfe von Multi-Faktor-Authentifizierung und zertifizierten Verschlüsselungsprodukten oder halten Ihr Netzwerk mit Hilfe von Cloud-Sandboxing frei von Zero-Day-Bedrohungen. Unsere Endpoint Detection and Response Lösungen und Frühwarnsysteme wie Threat Intelligence Services ergänzen das Angebot im Hinblick auf gezielte Cyberkriminalität, APTs und Forensik. Dabei setzt ESET nicht nur allein auf Next-Gen-Technologien wie KI oder Machine Learning, sondern kombiniert Erkenntnisse aus dem eigenen LiveGrid (Reputationssystem) mit Machine Learning und menschlicher Expertise, um Ihnen den besten Schutz zu gewährleisten.

ZUFRIEDENE KUNDEN

BVB 09 Champion Partner

Allianz Suisse

T

MHB Marienhospital Bottrop gGmbH

kohlpharma

Med360°

BEWÄHRT

Secur|Ty made in EU
Trust Seal www.teletrust.de/itsmie

ESET wurde das Vertrauenssiegel „IT Security made in EU" verliehen

CERTIFIED ISO 9001:2015 COMPANY

CERTIFIED ISO 27001:2013 COMPANY

Unsere Lösungen sind nach Qualitätsstandards zertifiziert

ESET IN ZAHLEN

110+ Mio.
Nutzer weltweit

400k+
Business-Kunden

200+
Länder & Regionen

13
Forschungs- und Entwicklungs-zentren weltweit

welivesecurity™ BY ESET

ESET Deutschland GmbH | Spitzweidenweg 32 | 07743 Jena | Tel.:+49 3641 3114 200

ESET.DE | ESET.AT | ESET.CH