Rödl & Partner

8 PRAXISTIPPS FÜR EINE ERFOLGREICHE KRITIS-PRÜFUNG

WIE SIE DIE HÄUFIGSTEN FEHLER ZUR NACHWEISERBRINGUNG VERMEIDEN

EINLEITUNG

Nachdem die KRITIS-Prüfung 2019 für die Betreiber Kritischer Infrastrukturen beendet sein dürfte (Abgabefrist für den Prüfnachweis war der 30. Juni 2019), beginnt nun die Zeit der Nacharbeiten und Beseitigung festgestellter Mängel.

Bei der medizinischen Versorgung war durch die späte Veröffentlichung des B3S in Version 1.0 die Prüfung sowohl auf Seiten des Betreibers der kritischen Dienstleistung (kDL) als auch bei der prüfenden Stelle durch Ressourcenknappheit geprägt: Die Betreiber mussten sich inhaltlich mit dem B3S und den Änderungen zur vorherigen Version auseinander setzen, die Umsetzung der einzelnen Anforderungen beschreiben und ggf. noch Maßnahmen ergreifen um Lücken zu schließen. Dies führte dazu, dass sich die Prüfungen sehr stark in Richtung des Stichtages verlagerten und zu einem Engpass der ohnehin wenigen geeigneten prüfenden Stellen mit der geforderten Branchenkenntnis. Prüfungshandlungen und die Erstellung der Nachweise wurden somit auf beiden Seiten unter Zeitdruck erstellt.

Mit den folgenden Tipps möchten wir Sie bei der Vorbereitung auf die nächste KRITIS-Runde unterstützen, so dass sie für alle Beteiligten reibungslos ablaufen kann.

DIE 8 PRAXISTIPPS

I. *Festgestellte Mängel frühzeitig angehen*

Je nach Art des Mangels kann die Behebung von Mängeln sowohl Zeit- als auch kostenintensiv sein. Oftmals erfordert es aber auch die Erstellung von neuen Konzepten, die erst noch erarbeitet werden müssen. Man sollte sich daher frühzeitig mit den Feststellungen auseinander setzen, angemessene Lösungsansätze suchen und umsetzen und die Zeit bis zur Erstellung des kommenden Nachweises an das BSI nicht untätig vergehen lassen. Wir empfehlen die folgenden Schritte:

– Maßnahmen definieren und Budgets beschaffen
– Verantwortlichkeiten und Zeitpläne/Fristen für die Mängelbeseitigung festlegen
– Personalressourcen ausreichend einplanen und ggf. externe Berater dazu holen

Oftmals ist es schwer neben der normalen Tätigkeit ausreichend personelle Ressourcen für die Umsetzung der Maßnahmen vorzuhalten, aus diesem Grund ist eine klassische Projektstruktur mit Projektzeiträumen und Meilensteinen für größere Maßnahmen sinnvoll.

2. *Beschreibung der Umsetzung der Anforderungen des B3S erstellen*

Der B3S definiert MUSS- und SOLL-Anforderungen aus unterschiedlichen Bereichen der Informationssicherheit. Im Rahmen der Prüfung muss sich die prüfende Stelle damit auseinander setzen, welche Maßnahmen zur Erfüllung der Anforderungen umgesetzt wurden. Es sollte daher vom kDL-Betreiber eine Beschreibung der Umsetzung erstellt und regelmäßig aktualisiert werden. Dies beinhaltet die folgenden Vorteile:

– Hilft zur eigenen Überwachung der Umsetzung und als Nachweis gegenüber dem BSI
– Prüfer kann ggf. auf die Aufbauprüfung verzichten und direkt in die Funktionsprüfung einsteigen
– Etwaige Lücken im Control Set könnten leichter festgestellt werden
– Nachweislicher Review von relevanten Unterlagen, der Schutzbedarfsanalyse etc.. Damit ist gleichzeitig ein Qualitätssicherungssystem für regelmäßig durchzuführende Tätigkeiten im Rahmen der KRITIS-Anforderungen geschaffen

Eine Dokumentation der Umsetzung von Anforderungen kann folgendermaßen aussehen.

Anforderung	Klassifikation	Beschreibung	Umsetzung	Ansprechpartner	Dokumente
ANF-MN 8	MUSS	Es MUSS mindestens eine Person als Beauftragter für die Informationssicherheit (Informationssicherheitsbeauftragter, Chief Information Security Officer) im B3S-Geltungsbereich benannt werden.	Als ISB wurde Herr Peter Petersen bestellt. Seine Stellvertreterin ist Erika Mustermann.	Hr. Peter Petersen	U:\...\Bestellungsurkunden.pdf
ANF-MN9	MUSS	...	...	...	...

DIE 8 PRAXISTIPPS

3. *Frühzeitig um den Prüfer kümmern*

Für einige Betreiber war es schwer unter Einhaltung des Stichtags 30. Juni 2019 eine prüfende Stelle zu finden. Wir empfehlen daher frühzeitig nach einem Prüfer für das Jahr 2021 zu suchen. Dies hätte u.a. die folgenden Vorteile:

- Planungssicherheit mit verfügbarem Prüfer
- Sicherstellung der Einhaltung der Abgabefrist
- Frühzeitiger Prüfungsbeginn und so ggf. Puffer zur Nachbesserung
- Frühzeitige Kommunikation mit dem Prüfer für die Prüfungsplanung und -inhalte – die Kommunikation muss sich nicht auf die Prüfzeiträume vor Ort beschränken
- Enge Abstimmung der Mängelbeseitigung intern und mit dem Prüfer – Welche Maßnahmen können wann umgesetzt werden? Sind die neuen Maßnahmen überhaupt angemessen oder bleibt ein Mangel bestehen?

Dies bringt Ihnen Planungssicherheit und stellt eine angemessene Darstellung der Prüfung und Maßnahmenumsetzung gegenüber dem BSI sicher.

4. *Kompetenz der Prüfer sicherstellen*

Das Gesundheitswesen unterscheidet sich deutlich von typischen Industriebetrieben. Um nicht Äpfel mit Birnen zu vergleichen und tatsächlich beurteilen zu können, wie wichtig ein System ist oder inwiefern sich ein festgestellter Mangel auf die Verfügbarkeit, Verfügbarkeit, Integrität und Authentizität der Dienstleistung auswirken kann (wovon am Ende die Kritikalität des Mangels abhängt), ist ein erfahrenes Team mit ausreichend Branchenerfahrung notwendig. Wir empfehlen bei der Auswahl der prüfenden Stelle auf folgende Punkte zu achten:

- Prüfteam sollte bei der Angebotspräsentation bereits bekannt sein und vorgestellt werden können
- Kompetenz der Prüfer nachweisen lassen (Prüfverfahrens-Kompetenz nach §8a BSIG, Auditkompetenz, Informationssicherheits-Kompetenz, Branchenerfahrung)
- Empfehlungsschreiben aus durchgeführten Prüfungen anfordern, im Idealfall personenbezogene Referenzen und nicht allgemein für das Unternehmen

DIE 8 PRAXISTIPPS

5. *Verwendung des Prüfnachweisplaner-Tools*

Je nach prüfender Stelle kann sich das Vorgehen im Rahmen der Prüfung unterscheiden (Vollprüfung, Stichprobenprüfung, Dokumentenprüfung...). Daraus können sich große Varianzen in den Kosten und auch der Qualität der Prüfung ergeben. Durch Nutzung des Prüfnachweisplaner-Tools (https://www.kh-it.de/downloads.html) ergeben sich Vorteile bei der Vergleichbarkeit von Angeboten und der Prüfungstiefe. Dies ist insbesondere hinsichtlich der Vergleichbarkeit zu anderen Betreibern kritischer Infrastrukturen der Branche sinnvoll.

6. *Klare Termine für Prüfungsdurchführung definieren*

Sobald die prüfende Stelle gefunden ist, sollte ein fester Zeitplan für die Prüfung vereinbart werden. Es muss ausgehend von der Abgabefrist zurückgerechnet werden, wann welche Schritte notwendig sind, um am Ende rechtzeitig den Prüfnachweis in den Händen zu halten. Aus unserer Sicht sollte mit der Abgabe auch nicht bis zum letztmöglichen Zeitpunkt gewartet werden. Ein angemessener Zeitplan berücksichtigt insbesondere die notwendige Zeit zur Abstimmung der Mängelliste. Dies beinhaltet die Abstimmung der Mängel mit dem Prüfer als auch die interne Abstimmung der Maßnahmenplanung zur Behebung schwerwiegender Mängel.

DIE 8 PRAXISTIPPS

7. *Stand der Technik verfolgen*

Betreiber kritischer Infrastrukturen, welche bei der letzten Prüfung keine schwerwiegenden Mängel aufgezeigt bekommen haben mögen nun denken, dass sie entspannt bis zur nächsten KRITIS-Runde die Füße hochlegen können. Doch dem ist nicht so – zum einen verändert sich der Stand der Technik und somit auch der technische „Standard“, der dringend umzusetzen ist. Zum anderen kann eine Verlagerung von Prüfungsschwerpunkten zu weitergehenden Erkenntnissen und somit auch zu schwerwiegenden Abweichungen der geforderten Maßnahmen führen.

8. *IT-Sicherheitsgesetz 2.0*

Im März 2019 wurde ein Referentenentwurf des IT-Sicherheitsgesetz 2.0 veröffentlicht, der die Umsetzung des Stands der Technik zumindest im Bereich Vorfallerkennung konkretisiert. Hierbei wird nun explizit eine Pflicht zum Einsatz von Systemen zur Angriffserkennung genannt. Ein Security Incident & Event Management (SIEM) System wird damit obligatorisch.

Zudem sollen die Hersteller von Betreibern kritischer Infrastrukturen stärker in die Pflicht genommen werden, indem Hersteller für sogenannte Kernkomponenten der kritischen Dienstleistung zukünftig ein IT-Sicherheitskennzeichen umsetzen. Dieses besteht aus einer Selbstauskunft des Herstellers, sowie weitergehenden dynamischen Sicherheitsinformationen des BSI. Damit soll verständlich und transparent aufgezeigt werden, inwiefern IT-Sicherheitsmaßnahmen erfüllt werden und worauf zu achten ist. Auch kann die Mitwirkung der Hersteller bei Störungen und Ausfall der von Ihnen betreuten IT-Systeme verlangt werden.

Für die Umsetzung angemessener technischer und organisatorischer Maßnahmen wird mit Verabschiedung des Gesetzes eine weitere Motivation geschaffen. Die Bußgeldvorschriften wurden insgesamt überarbeitet und Bußgelder erhöht. Damit werden Verstöße auf das Niveau der DSGVO gehoben. Sanktionen können damit also bis zu 4 % des weltweiten Umsatzes oder 20 Millionen Euro, je nachdem welcher Wert höher ist, ausmachen.

Auch wenn der Entwurf sicher noch diskutiert und angepasst wird, so ist klar der eingeschlagene Weg zu erkennen. Eine frühzeitige Auseinandersetzung mit den Themen ist ganz klar empfehlenswert.

IHRE ANSPRECHPARTNER

Jürgen Schwestka

Diplom-Kaufmann, CISA, Zertifizierter IT-Security-Auditor, IT-Auditor[IDW], Leiter DigitalGRC Süd

T +49 911 9193 3508
E juergen.schwestka@roedl.com

Konrad Klein

Bachelor of Science, CISA, IT-Auditor[IDW]

T +49 911 9193 3686
E konrad.klein@roedl.com

Gerne stehen wir für weitergehende Fragen zur Verfügung!

Für weitere Informationen zum Thema KRITIS besuchen Sie uns doch auf www.roedl.de/wen-wir-beraten/gesundheit-sozialwirtschaft/kritis

MEHR INFOS GEFÄLLIG?

Informative Whitepaper hilfreiche Checklisten und viele Flyer

zu den verschiedensten Themen der Gesundheits- und Sozialwirtschaft

Jetzt kostenfrei herunterladen: www.roedl.de/downloadcenter-gesundheit-sozialwirtschaft

Kennen Sie schon unsere fachspezifischen Newsletter?

Der E-Mail Newsticker Kompass Gesundheit und Soziales und der Newsletter Fokus Gesundheits- und Sozialwirtschaft.

Jetzt kostenfrei abonnieren: http://www.roedl.de/medien/publikationen/newsletter/