AG KRITIS

Arbeitsgruppe Kritische Infrastrukturen

Stellungnahme zum Referentenentwurf der C5-Äquivalenz-Verordnung vom 19.12.2024

Version 1.0 – zuletzt editiert am 23.01.2025

1 Arbeitsgruppe Kritische Infrastrukturen

Dieses Dokument wurde von Mitgliedern der unabhängigen Arbeitsgruppe Kritische Infrastrukturen (AG KRITIS) erstellt.

Wir haben uns im Frühjahr 2018 erstmals zusammengefunden, um Ideen und Anregungen zur Erhöhung der Resilienz und Sicherheit kritischer Dienstleistungen von Betreibern kritischer Infrastrukturen im Sinne des Gemeinwohls zu entwickeln. Unser Ziel ist es, die Versorgungssicherheit der deutschen Bevölkerung zu erhöhen, indem wir die Bewältigungskapazitäten des Staates zur Bewältigung von Großschadenslagen, die durch Cyberangriffe hervorgerufen wurden, ergänzen und erweitern wollen. Unsere Arbeitsgruppe ist unabhängig von Staat, Verwaltung oder wirtschaftlichen Interessen.

Die AG KRITIS besteht aus ca. 42 Fachleuten und Experten, die sich mit Kritischen Infrastrukturen (KRITIS) gemäß § 2 (Abs 10) BSI-Gesetz [1] und gemäß § 10 BSIG zugehöriger *Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz* [2] (BSI-Kritisverordnung - BSI-KritisV) beruflich beschäftigen, zum Beispiel durch Planung, Aufbau, Betrieb sowie Beratung, Forschung oder Prüfung der beteiligten Systeme und Anlagen. Unser Engagement ist getrieben von der Motivation, unabhängig von wirtschaftlichen Interessen eine nachhaltige Verbesserung der Sicherheit jener Anlagen kooperativ mit allen Beteiligten herbeizuführen und damit im Katastrophenfall die öffentliche Sicherheit zu verbessern. Wir sind kein Wirtschaftsverband oder Unternehmen und haben daher auch und insbesondere keine Sponsoren.

Uns eint, dass wir durch unsere Arbeit unabhängig voneinander zu dem Schluss gekommen sind, dass die Ressourcen der Bundesrepublik Deutschland zur Bewältigung von Großschadenslagen auf Grund von informations- und operationstechnischen Vorfällen im Bereich der Kritischen Infrastrukturen nicht ausreichen. In der Folge sind resultierende Krisen oder Katastrophen nicht oder kaum zu bewältigen. Es sollen daher Wege gefunden werden, das Eintreten gravierender Folgen dieser Vorfälle durch schnelles und kompetentes Handeln zu verhindern oder zumindest abzuschwächen und eine Regelversorgung in kürzest möglicher Zeit wieder sicherzustellen.

[1] www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html
[2] www.gesetze-im-internet.de/bsi-kritisv/BJNR095800016.html

2 Einleitung

Im Gesundheitswesen werden besonders schützenswerte Daten verarbeitet. Um den dafür angemessenen Schutz auch beim Einsatz cloudbasierter Informationssysteme sicherzustellen, in denen Gesundheits- oder Sozialdaten verarbeitet werden, wurde durch das Digital-Gesetz der § 393 des Fünften Buches Sozialgesetzbuch (SGB V) neu eingeführt. Damit wurde ein verpflichtend einzuhaltender Mindeststandard eingeführt: der durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelte „Kriterienkatalog C5 (Cloud Computing Compliance Criteria Catalogue)“. Durch die Anforderung einer C5 Zertifizierung der informationstechnischen Systeme soll die Resilienz der Einrichtungen im Gesundheitswesen gesteigert werden.

Um die Organisationen nicht zu überfordern und ihnen den Zugang zu modernen Cloudservices zu ermöglichen, soll durch die C5-Äquivalenz-Verordnung für eine Übergangszeit der Nachweis der Einhaltung eines zum C5-Kriterienkatalog äquivalenten Sicherheitsniveaus durch alternative Zertifikate und Testate erlaubt werden. Eine stufenweise Migration der internen Sicherheitskontrollen auf den C5-Standard ist obligatorisch.

Die Verarbeitung von personenbezogenen Gesundheits- oder Sozialdaten soll ohne ein C5-Testat möglich sein, wenn ein Testat oder Zertifikat nach einem der folgenden drei Standards oder Frameworks vorliegt:

1. DIN EN ISO/IEC 27001:2022
2. ISO 27001 auf der Basis von IT-Grundschutz durch das Bundesamt für Sicherheit in der Informationstechnik (BSI)
3. Cloud Controls Matrix Version 4.0 (CCM)

Damit ist für den Einsatz des Cloud-Computing-Dienstes, der Cloud-Systeme und der Cloud-Technik ein zum C5-Standard vergleichbares oder höheres Sicherheitsniveau aber noch nicht sichergestellt. Zusätzlich muss ein Maßnahmenplan vorliegen, welcher für die Einsichtnahme der zuständigen Aufsichtsbehörden zusammen mit dem Testat oder Zertifikat vorzuhalten ist. Der Maßnahmenplan muss folgendes enthalten:

- Gap-Analyse zu den Basiskriterien des C5-Kriterienkatalogs
- Dokumentation der individuellen technischen und organisatorischen Vorkehrungen, um die Gaps zum C5-Katalog zu schließen
- Roadmap über die geplanten Maßnahmen, die eine Zeitraum von 12 Monaten ab der Erstellung der Meilensteinplanung nicht überschreitet
- eine Dokumentation von Maßnahmen zur Erlangung eines C5-Typ-1-Testats (spätestens nach 18 Monaten ab Erstellung der Meilensteinplanung), vertragliche Vereinbarungen mit Auditoren oder die Aufnahme von Vertragsverhandlungen genügen.

3 Stellungnahme

Der C5 Katalog integriert die Anforderungen von ISO/IEC 27001, IT-Grundschutz und CCM, um eine umfassendes Sicherheitsniveau speziell für Cloud-Dienste zu bieten. Außerdem ist C5 exakt auf Deutschland zugeschnitten, die Basisanforderungen übersteigen die Anforderungen der ISO 27001, des IT-Grundschutzes oder des CCM.

Aus unserer Sicht ist nicht nachvollziehbar, dass ein **C5-Testat ausschließlich durch Wirtschaftsprüfer erstellt** werden darf und dass **nicht auf das bewährte Verfahren der Erteilung von Zertifikaten zurückgegriffen** wird.

Mit der Äquivalenzverordnung soll Rechtssicherheit bezüglich eines vergleichbaren Sicherheitsniveaus hergestellt werden. Dies ist zu begrüßen.

C5 hat nicht das gleiche Sicherheitsniveau wie ISO 27001, IT-Grundschutz und CCM. Deshalb ist die Vorgehensweise nach C5-Äquivalenz-Verordnung § 1 Absatz (2) aus unserer Sicht geeignet, nach einem angemessenen Übergangszeitraum das erforderliche Sicherheitsniveau zu erreichen.

Die C5-Äquivalenz-Verordnung bezieht sich auf Typ1-Testate, die nach SGB V §393 Absatz (4) nur noch bis zum 30. Juni 2025 als aktuell gelten. Die in § 1 Absatz (2) der C5-Äquivalenz-Verordnung benannten Fristen bis zur Erlangung eines Typ1-Testats überschreiten diesen Termin auch bei der geplanten rückwirkenden Inkraftsetzung zum 1. Juli 2024. Somit entsteht eine Rechtsunsicherheit für einen Cloud-Anbieter, der ein C5-Testat nach vorgelegtem Meilensteinplan erst später erreichen wird, obwohl die Fristen im Meilensteinplan eingehalten werden.

Problematisch wäre die Ausweitung der C5-Äquivalenz-Verordnung auch auf Typ2-Testate nach C5-Kriterienkatalog. Dadurch würde eine dauerhafte Abschwächung des Sicherheitsniveaus entstehen, weil neue Cloud-Anbieter zunächst mit einem niedrigeren Sicherheitsniveau die Verarbeitung beginnen könnten.

Daher ist die Begrenzung der Gültigkeit der Äquivalenzverordnung auf Typ1-Testate beizubehalten.