bvitg-Positionierung

Sichere Cloud.
Starke Wirtschaft.

C5 praxisnah betrachtet

Kontakt:
Tom Lühmann

Referent eHealth
tom.luehmann@bvitg.de

bvitg

Sichere Cloud. Starke Wirtschaft.
C5 praxisnah betrachtet.

Cloud-basierte Technologien sind ein zentraler Baustein der digitalen Transformation im Gesundheitswesen. Der Bundesverband Gesundheits-IT – bvitg e. V. begrüßt ausdrücklich die fortschreitende Standardisierung und Zertifizierung dieser Technologien. Einheitliche, transparente und vertrauenswürdige Kriterien schaffen Sicherheit im Markt, stärken die Resilienz in einem herausfordernden geopolitischen Umfeld und bilden eine wesentliche Grundlage für Innovationen.
Als Verband stehen wir hinter diesen Zielen und bringen uns aktiv in den Diskurs um eine tragfähige, harmonisierte Strategie für Cloud-Zertifizierungen ein. Dabei stehen wir für einen risikobasierten Ansatz ein.

Zielklarheit und Ausgewogenheit der Anforderungen

Bei der Ausgestaltung des Cloud Computing Compliance Criteria Catalogue (C5), welcher Mindeststandards an sicheres Cloud Computing definiert, müssen Zielsetzung und praktische Ausgestaltung des C5 konsequent aufeinander abgestimmt sein. Der derzeitige C5 Kriterienkatalog lässt an einigen Stellen eine klare und ausgewogene Gewichtung unterschiedlicher regulatorischer, technischer und wirtschaftlicher Interessen vermissen. Um wirksam und praxistauglich zu sein, braucht es eindeutige Zuständigkeiten und Verantwortlichkeiten, nachvollziehbare Rollenverteilungen sowie Kriterien, die proportional zum angestrebten Sicherheitsgewinn ausgestaltet sind. Mehrfachaufwände sind zu vermeiden. Zudem muss sichergestellt werden, dass die Vorgaben von allen Marktteilnehmenden korrekt verstanden und Interpretationsspielräume eliminiert werden. Dies gilt nicht nur für das C5-Testat, sondern grundsätzlich für alle Testate und Zertifizierungen, welche im Gesundheitswesen notwendig sind.

Im Markt, d.h. bei den Anwender:innen von Cloud-basierten Lösungen, wird häufig nicht hinreichend zwischen einer neutralen, unabhängigen Bestandsaufnahme (Testat) und einer kontinuierlichen Prozessüberwachung (Zertifizierung, z. B. nach ISO/IEC 27001) differenziert. Häufig werden diese beiden Nachweisformen fälschlicherweise gleichgesetzt und die daraus resultierenden Implikationen auf Seite der Leistungserbringenden sind nicht bekannt.

Zur Vermeidung von Mehrfachaufwänden ist eine eindeutige Trennung der Assurance-Logik erforderlich: **Testate (punktuelle Bestandsaufnahme)** und **Zertifizierungen (kontinuierlicher Systembetrieb mit Überwachung)** sind in Aussagekraft und Verwendung klar zu differenzieren. Missverständnisse führen in der Praxis zu additiven Prüfanforderungen ohne Sicherheitsgewinn.

Abgrenzung von und Verzahnung mit bestehenden Standards

Ein zentrales Anliegen des bvitg ist die stärkere Anbindung des C5 an bestehende international etablierte Standards wie ISO 27001 und vergleichbare. Zahlreiche Anforderungen überschneiden sich bereits heute, werden in der C5-Testierung jedoch erneut abgeprüft. Dies führt zu vermeidbaren Mehrfachprüfungen, erhöhten Kosten und verlängerten Zertifizierungsprozessen.

Das verlängert in der Folge Innovationszyklen für Cloud-basierte Produkte, hemmt Innovationsentscheidungen und schwächt letztendlich den Wirtschaftsstandort Deutschland.
Wir plädieren für ein verbindliches Anerkennungs- und Substitutionsprinzip: Anforderungen, die durch international etablierte Zertifizierungen (insb. ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018) oder einschlägige Branchenstandards bereits nachweislich abgedeckt sind, dürfen im Rahmen der C5-Testierung nicht erneut geprüft werden. Stattdessen ist ein standardisiertes Mapping (*Crosswalk*) und eine Abweichungsanalyse vorzusehen, die ausschließlich verbleibende Lücken adressiert.

Zudem spricht der bvitg sich dafür aus, eine positive Prüf- und Berichtskultur zu fördern, die vorhandene Ergebnisse z.B. aus einem C5 Testat der genutzten Cloud Plattform nutzt, um den Prüfaufwand zu reduzieren. Dies kann im Prüfbericht dokumentiert werden, ohne die Potentiale des C5 zu beschädigen (aktive Nutzung der Carve Out Methode).
Konkret plädieren wir daher für:

- eine **deutliche Abgrenzung** der Bereiche, die durch folgende weitere Nachweise abgedeckt sind:
  - ISO27001
    - ISO 27017
    - ISO 27018
  - AI Act (B II)
  - B3S Medizinische Versorgung
  - B3S GKV/GPV
- eine **verzahnte Prüfarchitektur**, die Mehrfachaufwände systematisch reduziert. Hierfür eignet sich insbesondere die Carve-Out Methode, bei welcher bereits abgeprüfte Anforderungen (auch solche von Dienstleistern, Plattformen o.ä.) in einem weiteren Testierungs- oder Zertifizierungsverfahren nicht erneut geprüft werden.
- eine **klare Zuordnung** von Verantwortlichkeiten und Prüfumfängen.

Diese Weiterentwicklungen würden Leistungserbringende und Anbieter mit bestehenden Zertifizierungen entlasten, ohne Abstriche bei der Sicherheit zu machen.

Praktikabilität und Auswirkungen auf den Markt

Mit der zunehmenden Detaillierung von Anforderungen steigt der operative Aufwand für Testierung und Dokumentation erheblich. In der Praxis droht dadurch ein strukturelles Nadelöhr, dessen Folgen bereits heute absehbar sind:

- **erschwerter Marktzugang,** speziell für Cloud-Lösungen. Das wirkt sich hemmend auf die Entscheidung für den deutschen Markt aus
- **verlängerte Innovationszyklen**,
- **steigende Kosten** für Testierung, Zertifizierung und Compliance,
- **besondere Belastung für mittelständische Unternehmen**, die Gefahr laufen, aus dem Markt verdrängt zu werden.

Wenn innovative Cloud-Lösungen aufgrund restriktiver Vorgaben den deutschen Markt nicht erreichen, wird eine strukturelle Benachteiligung der Patientenversorgung in Kauf genommen. Damit entsteht ein Risiko für eine schleichende Marktbereinigung, die Innovationskraft und Vielfalt im Gesundheitswesen verringert.

Lehren aus anderen Regulierungsverfahren und Europäische Perspektive

Um negative Markteffekte wie bei der Einführung der MDR, etwa steigende Zertifizierungskosten und Innovationshemmnisse, im Cloud-Sektor zu vermeiden, mahnt der bvitg zur Proportionalität und Vermeidung von Mehrfachstrukturen. Ziel muss eine konsequente europäische Harmonisierung sein: Perspektivisch sollte ein europäisches *Cloud Certification Scheme und* nationale Standards wie C5 vollständig integrierbar sein, d.h. C5 vor einem europäischen Zertifikat als gleichwertig anerkannt werden. Nur durch eine widerspruchsfreie Verzahnung von C5, MDR, AI Act und EU-Vorgaben lassen sich Planungssicherheit schaffen und die internationale Anschlussfähigkeit des deutschen Gesundheitsmarktes sichern.

Das C5 Testat kann außerdem als etablierter und praxiserprobter Baustein für Anforderungen an europäische digitale Cloud-Souveränität dienen. Vor dem Hintergrund des deutsch-französischen Souveränitätsgipfels im November 2025 in Berlin und der angekündigten Wiederaufnahme europäischer Verhandlungen zur Cloud-Souveränität, etwa zum EUCS, sollte sich der deutsche Gesetzgeber auf europäischer Ebene dafür einsetzen, C5 auch als anerkannten Nachweis für Cloud-Souveränität zu verankern. Dies würde eine Zersplitterung der Anforderungen vermeiden und deutschen Unternehmen den Marktzugang im europäischen digitalen Binnenmarkt erleichtern. Im Rahmen europäischer Initiativen, etwa des Digitalen Omnibus, sollten zudem weder neue Öffnungsklauseln noch nationale Insellösungen geschaffen werden. Entscheidend ist, dass weder über den EUCS noch über andere europäische Regelwerke zusätzliche, strengere Zertifizierungsanforderungen in nationales Recht eingeführt werden, die das C5 faktisch ersetzen oder entwerten.

Schlussbemerkung

Eine sinnvolle Anwendung und Weiterentwicklung des Cloud Computing Compliance Criteria Catalogue sollte in den Mittelpunkt regulatorischer Anforderungen an den Cloud-Einsatz im Gesundheitswesen gestellt werden. Der Fokus muss dabei gleichermaßen auf der kontinuierlichen Weiterentwicklung des Kriterienkatalogs wie auf seinem konkreten Nutzen für Anwender und Anbieter liegen. Ziel sollte es sein den hohen Sicherheitsstandard beizubehalten und gleichzeitig regulatorische Aufwände deutlich zu reduzieren. Abstriche dürfen nicht zulasten von Sicherheit, Transparenz und Vertrauenswürdigkeit gehen - eine stärkere Berücksichtigung der Auswirkungen auf den Markt als bisher ist jedoch dringend erforderlich. Mit dem vorliegenden Papier machen wir eine ganze Reihe an konkreten Vorschlägen zu Weiterentwicklung und Verbesserung des C5: Eine stärkere Bündelung und Anerkennung bestehender Nachweise kann mit erheblich geringerem Aufwand das Sicherheitsniveau beim Betrieb von Cloud-Lösungen im Gesundheitswesen erreichen. Dies schafft Planungssicherheit, fördert Wettbewerb und Innovation und wirkt sich insgesamt positiv auf den Markt aus, indem

Markteintrittsbarrieren gesenkt und Investitionen in sichere, souveräne Cloud-Infrastrukturen begünstigt werden.

Der bvitg e. V. steht jederzeit für einen konstruktiven Austausch bereit, um die Anwendung des C5 im Gesundheitswesen praxisnah, innovationsfreundlich und sicher mitzugestalten. Wir freuen uns darauf, den weiteren Prozess aktiv zu begleiten.