KritisVO - DORA

27.22.2024 FFM BecN Meeting (CH)

DORA richtet sich an alle **Finanzinstitute** in der EU, die digitale Dienste anbieten, und verlangt von ihnen, ihre **digitale Resilienz** und **Cybersicherheit** zu verbessern.
Diese Verordnung ist vor allem auf **Betriebsstabilität** im Finanzsektor ausgerichtet, insbesondere bei **Cyberangriffen** und **IT-Ausfällen**.

KritisV betrifft nur **Betreiber kritischer Infrastrukturen**, die für die **Wirtschaft und Gesellschaft** von zentraler Bedeutung sind. Zahlungsinstitute, die als Betreiber einer **kritischen Finanzinfrastruktur** gelten (z.B. zentrale Zahlungssysteme), müssen zusätzlich zur DORA auch die Anforderungen der KritisV erfüllen.

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Bundesamt für Sicherheit in der Informationstechnik, 53175 Bonn

Bundesverband der electronic cash
Netzbetreiber (BecN) e.V.
Herrn Christian Hessel
c/o Hogan Lovells International LLP
Große Gallusstraße 18
60312 Frankfurt am Main

Dr. Timo Hauschild
Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189
53175 Bonn
Postanschrift:
Postfach 20 03 63
53133 Bonn
Tel. +49 228 99 9582-6166
Fax +49 228 99 10 9582-6166
Kritis-buero@bsi.bund.de
www.bsi.bund.de

De-Mail-Adresse:
poststelle@bsi-bund.de-mail.de

Betreff: Feststellung der Eignung eines Branchenspezifischen Sicherheitsstandards

Bezug: Ihr Antrag auf Feststellung der Eignung des branchenspezifischen Sicherheitsstandards vom 04.08.2023
Verfahrensnummer: 040_B3S_BeCN_Version 2.1
Datum: 24.08.2023
Seite 1 von 5

Eignungsfeststellung

gemäß § 8a Absatz 2 BSIG

„Branchenspezifischer Sicherheitsstandard des Bundesverbands der electronic cash-Netzbetreiber BecN“

Version 2.1 vom 07.07.2023

ist zur Gewährleistung der Anforderungen gemäß § 8a Absatz 1, 1a BSIG geeignet.

Zustell- und Lieferanschrift: Bundesamt für Sicherheit in der Informationstechnik, Godesberger Allee 185-189, 53175 Bonn

Sehr geehrte Damen und Herren,

gemäß Ihrem Antrag vom 04.08.2023 ergeht folgender

Eignungsfeststellungsbescheid:

1. Es wird festgestellt, dass der branchenspezifische Sicherheitsstandard unter dem Titel „Branchenspezifischer Sicherheitsstandard des Bundesverbands der electronic cash-Netzbetreiber BecN“ in der Version 2.1 vom 07.07.2023 zur Gewährleistung der Anforderungen des § 8a Abs. 1, 1a BSIG geeignet ist.
2. Das Bundesamt ist unverzüglich darüber zu informieren, wenn sich Anforderungen, die Auswirkungen auf die vollständige oder teilweise Eignung des B3S haben können, ändern.
3. Das Bundesamt behält sich vor, die Feststellung der Eignung zu widerrufen.
4. Die Eignungsfeststellung des unter 1. bezeichneten B3S wird auf zwei Jahre ab Bekanntgabe befristet.
5. Der Kostenbescheid ergeht mit gesondertem Schreiben.

31.August.2025
Brief wurde 31.08.23 zugestellt

Begründung

I.

Der Bundesverband der electronic cash Netzbetreiber (Antragsteller) hat dem BSI am 04.08.2023 einen branchenspezifischen Sicherheitsstandard (B3S) zur erneuten Eignungsprüfung vorgelegt.

Die Eignungsfeststellung wurde auf Grundlage der folgenden vom Antragsteller eingereichten Unterlagen vom 04.08.2023 vorgenommen:

- „Branchenspezifischer Sicherheitsstandard des Bundesverbands der electronic cash-Netzbetreiber BecN“ Version 2.1 vom 07.07.2023

Die Eignung wurde in Zusammenarbeit mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) beurteilt.

II.

zu 1.:
Dieser Bescheid ergeht aufgrund von § 8a Absatz 2 Satz 2 BSIG.

Das BSI ist nach § 3 Nummer 17; § 8a Absatz 2 Satz 1 BSIG zuständig für die Feststellung der Eignung branchenspezifischer Sicherheitsstandards, hier für den durch den Bundesverband der electronic cash Netzbetreiber am 04.08.2023 eingereichten branchenspezifischen Sicherheitsstandard (B3S) unter dem Namen „Branchenspezifischer Sicherheitsstandard des Bundesverbands der electronic cash-Netzbetreiber“ (Verfahrensnummer 040_B3S_BeCN_Version 2.1).

Das BSI kommt zu dem Ergebnis, dass der branchenspezifische Sicherheitsstandard (B3S) zum Zeitpunkt der Ausstellung dieses Bescheides zur Gewährleistung der Anforderungen gemäß § 8a Absatz 1, 1a BSIG für den KRITIS-Sektor Finanz- und Versicherungswesen, hier nur den Bereich der „Finanzdienstleister“, geeignet ist.

DORA ersetzt Kritis?

- Art. 2 Abs. 1 lit. a bis t Verordnung (EU) 2022/2554 (DORA) regelt, welche Unternehmen als Finanzunternehmen unter dieser Verordnung gelten.
- Sollte dies für das eigene Unternehmen der Fall sein, wäre die Regelungen des § 28 Abs. 5 BSIG-E anwendbar.
- Diese befreit ggf. von der Pflicht zur Abgabe von Nachweisen gem. § 39 BSIG-E
- BSIG-E noch nicht ein geltendes Gesetz
- Befindet sich derzeit im parlamentarischen Verfahren

- Das aktuelle BSIG gilt in der aktuellen Form weiter, bis es mit Inkrafttreten des NIS2-UmsCG durch die neue Fassung des BSIG ersetzt wird.

- BSIG wann? – derzeit offen

Aspekt	DORA	KritisV
Zielgruppe	Alle Finanzmarktakteure in der EU (einschließlich Zahlungsinstitute)	Betreiber von kritischen Infrastrukturen in Deutschland (inkl. kritischer Finanzinfrastruktur)
Fokus	**Digitale Resilienz und Cybersicherheit** im Finanzsektor	**Schutz kritischer Infrastrukturen** und Gewährleistung der **Versorgungssicherheit**
Meldung von Vorfällen	Meldung von IT-Vorfällen	Meldung von IT-Vorfällen
Geografische Reichweite	EU-weite Regelung für Finanzinstitute	Nationale Regelung in Deutschland für Betreiber kritischer Infrastrukturen
Umsetzungspflicht	Gilt für alle Finanzinstitute, die digitale Finanzdienstleistungen anbieten	Gilt nur für Unternehmen, die als Betreiber kritischer Infrastrukturen eingestuft sind
Forderungen zur Auslagerung	Anforderungen an **Drittanbieter** und die Auslagerung von IT-Diensten	Keine speziellen Auslagerungsanforderungen, jedoch generelle Sicherheitsvorgaben


WHAT'S
NEXT?

Cyber Resilience Act (CRA)

BSI-Präsidentin Claudia Plattner: „Künftig müssen Hersteller über den gesamten Lebenszyklus ihrer Produkte und Anwendungen die Verantwortung für deren Cybersicherheit übernehmen. Damit wird die Sicherheit digitaler Produkte und auch das Vertrauen in die Digitalisierung erheblich gestärkt. Davon profitieren alle Anwenderinnen und Anwender und letztlich auch die Hersteller, denn ihre Produkte werden qualitativ hochwertiger und sicherer.„

EU Cyber Resilience Act | Shaping Europe’s digital future

- Die **Cyberresilienz-Verordnung** (CRV) ist eine Verordnung der Europäischen Union, mit der die Regeln zur Cybersicherheit von Produkten mit digitalen Elementen EU-weit vereinheitlicht werden. Dadurch soll ein hohes Cybersicherheitsniveau in der Union sichergestellt und der freie Verkehr von Produkten mit digitalen Elementen im europäischen Binnenmarkt gewährleistet werden.
- Die Verordnung wurde am 12. März 2024 vom Europäischen Parlament und am 10. Oktober 2024 vom Rat der Europäischen Union beschlossen. Sie gilt ab dem 11. Dezember 2027.
- Sie ergänzt die Datenschutz-Grundverordnung und die NIS-2-Richtlinie.

- Die Regulierung gilt insbesondere auch für freie und Open-Source-Produkte, sofern sie in kommerziellen Produkten eingesetzt werden

Quelle: Cyberresilienz-Verordnung – Wikipedia

SOTEU_factsheet_CRA_update_20231201_cpHkdiLLl9BJxoY291IZs0Jz5Pw_89528.pdf

Nächste Schritte

- B3S?
- Abfrage an BecN Mitglieder wann nächster Kritis Audit ansteht
- Q2/25 Status Gesetzgebung prüfen ggf. B3S erneuern

- CRA?
- Frage an Verband der Terminalhersteller
- Terminalhersteller einzeln befragen