ILNAS

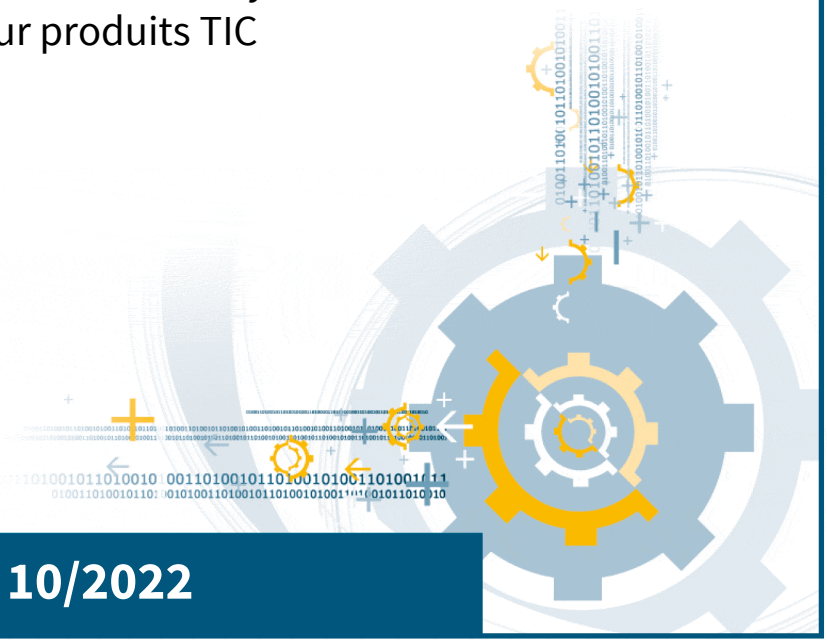
Institut luxembourgeois de la normalisation
de l'accréditation, de la sécurité et qualité
des produits et services

ILNAS-EN 17640:2022

Zeitlich festgelegte Cybersicherheitsevaluationsmethodologie für IKT-Produkte

Fixed-time cybersecurity evaluation methodology for ICT products

Méthode d'évaluation de la cybersécurité pour produits TIC



10/2022

Nationales Vorwort

Diese Europäische Norm EN 17640:2022 wurde als luxemburgische Norm ILNAS-EN 17640:2022 übernommen.

Alle interessierten Personen, welche Mitglied einer luxemburgischen Organisation sind, können sich kostenlos an der Entwicklung von luxemburgischen (ILNAS), europäischen (CEN, CENELEC) und internationalen (ISO, IEC) Normen beteiligen:

- Inhalt der Normen beeinflussen und mitgestalten
- Künftige Entwicklungen vorhersehen
- An Sitzungen der technischen Komitees teilnehmen

https://portail-qualite.public.lu/fr/normes-normalisation/participer-normalisation.html

EUROPÄISCHE NORM
EUROPEAN STANDARD
NORME EUROPÉENNE

EN 17640

Oktober 2022

ICS 35.030

Deutsche Fassung

Zeitlich festgelegte Cybersicherheitsevaluationsmethodologie für IKT-Produkte

Fixed-time cybersecurity evaluation methodology for ICT products

Méthode d'évaluation de la cybersécurité pour produits TIC

Diese Europäische Norm wurde vom CEN am 15. August 2022 angenommen.

Die CEN und CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC-Management-Zentrum oder bei jedem CEN und CENELEC-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN und CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN- und CENELEC-Mitglieder sind die nationalen Normungsinstitute und elektrotechnischen Komitees von Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, der Republik Nordmazedonien, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.

CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

Inhalt

Europäisches Vorwort

Dieses Dokument (EN 17640:2022) wurde vom Technischen Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ erarbeitet, dessen Sekretariat von DIN gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis April 2023, und etwaige entgegenstehende nationale Normen müssen bis April 2023 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Liste dieser Institute ist auf den Internetseiten von CEN abrufbar.

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die Republik Nordmazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Serbien, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Einleitung

Die Grundlage für eine fundierte Produktzertifizierung ist eine zuverlässige, transparente und wiederholbare Evaluationsmethodologie. Es gibt mehrere produkt- oder systemabhängige Evaluationsmethodologien. Der Rechtsakt zur Cybersicherheit (CSA, en: Cybersecurity Act) [1] wird zur Schaffung neuer Schemata führen, die wiederum (neue) Methodologien zur Evaluierung der Cybersicherheitsfunktionalitäten von Produkten erfordern. Diese neuen Methodologien werden benötigt, um die im CSA definierten Evaluierungsaufgaben zu beschreiben. Diese Methodologie fügt auch ein Konzept hinzu, das unabhängig von den Anforderungen der CSA ist, nämlich die Evaluierung innerhalb einer festen Zeit. Bestehende Evaluationsmethodologien zur Cybersicherheit (z. B. EN ISO/IEC 15408 in Kombination mit EN ISO/IEC 18045) sind nicht ausdrücklich zum Einsatz innerhalb einer festen Zeit ausgelegt.

Schemaentwickler werden ermutigt, die Evaluationsmethodologie in ihren Schemata umzusetzen. Dies kann bei Schemata für allgemeine Zwecke oder bei speziellen (vertikalen) Schemata durch die Auswahl von Aspekten für die Selbstbewertung auf der CSA-Vertrauenswürdigkeitsstufe „niedrig“ oder für Bewertungen durch Dritte geschehen. Die Selbstbewertung darf auf der CSA-Vertrauenswürdigkeitsstufe „niedrig“, die Drittparteien-Evaluierungen dürfen auf der CSA-Vertrauenswürdigkeitsstufe „niedrig“, „mittel“ oder „hoch“ durchgeführt werden. Und die Evaluierungskriterien sowie die Methodologie unterliegen möglicherweise einer zusätzlichen Anpassung je nach den Anforderungen des einzelnen Schemas. Diese Evaluationsmethodologie für die Cybersicherheit deckt alle diese Anforderungen ab. Diese Methodologie wurde so gestaltet, dass sie an die Anforderungen des jeweiligen Schemas angepasst werden kann (und muss).

Schemaentwickler werden ermutigt, die Evaluationsmethodologie für den vorgesehenen Verwendungszweck des Schemas umzusetzen, die für allgemeine Zwecke oder in speziellen (vertikalen) Domänen anwendbar ist, indem sie die Aspekte auswählen, die für die Selbstbewertung auf der CSA-Vertrauenswürdigkeitsstufe „niedrig“ oder die Drittparteien-Evaluierung auf jeder vom Schema geforderten CSA-Vertrauenswürdigkeitsstufe erforderlich sind.

Dieses Dokument enthält das Mindestmaß an Evaluierungsaufgaben, die im CSA definiert sind, um die gewünschte CSA-Vertrauenswürdigkeitsstufe zu erreichen, sowie optionale Arbeitsaufgaben, die im Rahmen des Schemas erforderlich sein könnten. Die Auswahl der verschiedenen optionalen Arbeitsaufgaben wird von Leitlinien begleitet, damit die Schemaentwickler die Auswirkungen ihrer Entscheidungen abschätzen können. Eine weitere Anpassung an die Risikosituation im Schema kann durch die Auswahl der verschiedenen in der Methodologie definierten Evaluierungsaufgaben oder durch die Verwendung der Parameter der Evaluierungsaufgaben, z. B. die Anzahl der Tage für die Durchführung bestimmter Arbeitsaufgaben, erreicht werden.

Wenn Schemaentwickler Arbeitsaufgaben wählen, die nicht in dieser Evaluationsmethodologie definiert sind, liegt es in der Verantwortung des Schemaentwicklers, eine Reihe begleitender Anforderungen zu definieren oder eine anwendbare Evaluationsmethodologie wiederzuverwenden.

Nichtsdestotrotz wird erwartet, dass die einzelnen Schemata die allgemeinen Anforderungen, die in dieser Evaluationsmethodologie dargelegt sind, instanziieren und den Herstellern (und allen anderen Parteien) umfassende Leitlinien zu den konkreten Anforderungen, die innerhalb des Schemas zu erfüllen sind, geben.

Evaluatoren, Prüfer und Zertifizierer können diese Methodologie verwenden, um die Beurteilung, Prüfung oder Evaluierung der Produkte durchzuführen und die eigentliche Evaluierung/Zertifizierung nach den von einem bestimmten Schema aufgestellten Anforderungen durchzuführen. Es sind auch Anforderungen an den Qualifikations- und Wissensstand der Evaluatoren enthalten, und daher wird das Schema auch von **Akkreditierungsstellen** oder **nationalen Zertifizierungsstellen für Cybersicherheit** bei der Akkreditierung oder ggf. Befugniserteilung und Überwachung von Konformitätsbewertungsstellen verwendet.

Hersteller und **Entwickler** finden die allgemeine Art von Nachweisen, die für jede Evaluierungsaufgabe erforderlich sind, in der Evaluationsmethodologie aufgeführt, um sich auf die Beurteilung oder Bewertung vorzubereiten. Die Nachweis- und Evaluierungsaufgaben sind unabhängig davon, ob die Evaluierung durch den Hersteller/Entwickler (d. h. Erstpartei) oder durch eine andere Person (Zweit-/Drittpartei) durchgeführt wird.

Benutzer von zertifizierten Produkten (Regulierungsbehörden, Benutzerverbände, Regierungen, Unternehmen, Verbraucher usw.) dürfen dieses Dokument ebenfalls nutzen, um sich über die Vertrauenswürdigkeit zu informieren, die sich aus bestimmten Zertifikaten ergibt, die diese Bewertungsmethode verwenden. Auch hier wird erwartet, dass die Schemaentwickler zusätzliche, auf die Domäne des Schemas zugeschnittene Informationen über die durch Evaluierungen/Beurteilungen nach dieser Methodologie gewonnene Vertrauenswürdigkeit bereitstellen.

Darüber hinaus ist diese Methodologie dazu gedacht, Schemaentwickler in die Lage zu versetzen, Schemata zu erstellen, die versuchen, den Aufwand für den Hersteller so weit wie möglich zu reduzieren (was einen zusätzlichen Aufwand für das Prüflabor und die Zertifizierungsstelle bedeutet).

ANMERKUNG In diesem Dokument wird der Begriff „Konformitätsbewertungsstelle“ (KBS) für KBS, die die Evaluierung durchführen, verwendet. Andere mögliche Rollen für KBS werden in diesem Dokument nicht berücksichtigt.

Es sollte beachtet werden, dass dieses Dokument nicht „eigenständig“ verwendet werden kann. Jede Domäne (Schema) muss domänenspezifische Cybersicherheitsanforderungen („technische Spezifikationen“) für die zu evaluierenden/zertifizierenden Objekte bereitstellen. Diese Methodologie ist das zu gedacht, in Verbindung mit den betreffenden technischen Spezifikationen verwendet zu werden, die solche Cybersicherheitsanforderungen enthalten. Die Beziehung zwischen der in diesem Dokument dargestellten Methodologie und den Aufgaben in der Produktkonformitätsbewertung ist in Bild 1 dargestellt.

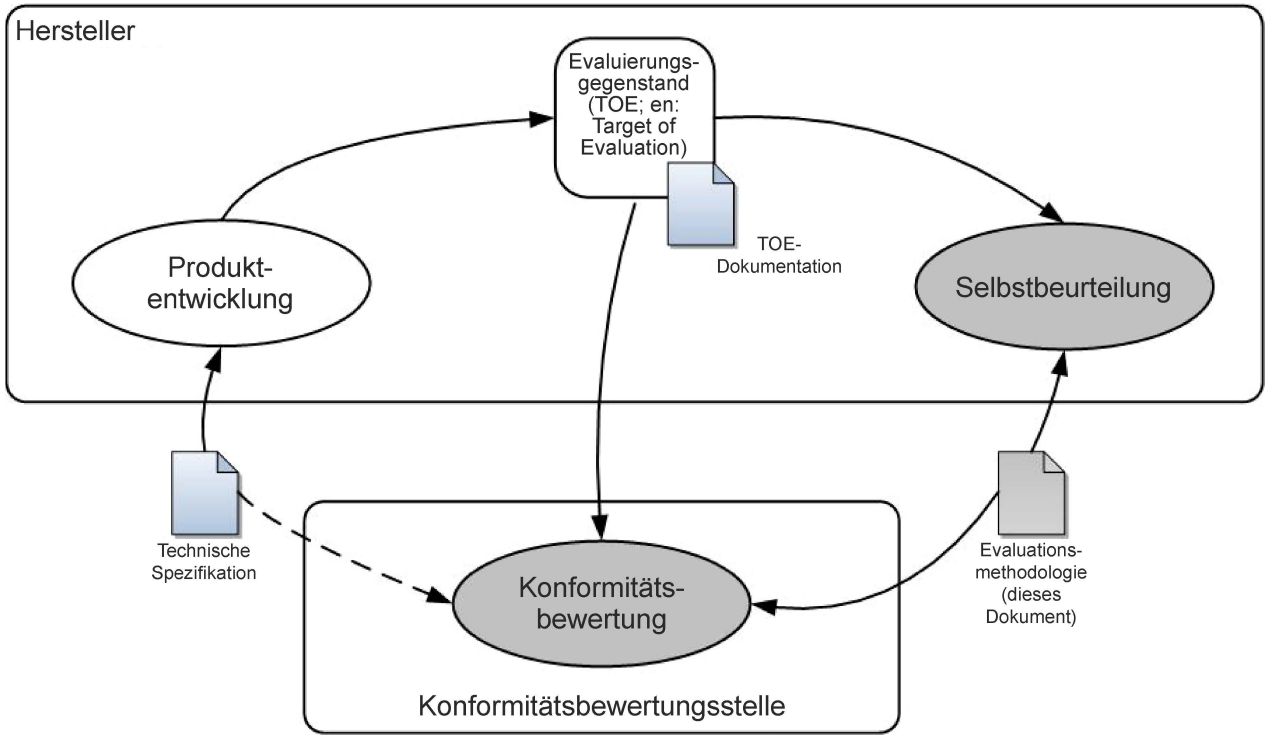


Bild 1 — Beziehung dieses Dokuments zu den Aufgaben in der Produktkonformitätsbewertung