BESCHREIBUNG DES ZERTIFIZIERUNGSVERFAHRENS EUCC

INHALT

Haben Sie Fragen zu der Leistungsbeschreibung? Wir helfen Ihnen gern weiter.

Sie erreichen uns per Mail info.tncert@tuev-nord.de oder persönlich von Montag bis Freitag zwischen 07:30 Uhr und 18:00 Uhr unter 0800 – 2457457.

TÜV NORD CERT GmbH
Am TÜV 1
45307 Essen
www.tuev-nord-cert.de

TÜVNORD

BESCHREIBUNG DES ZERTIFIZIERUNGSVERFAHRENS EUCC

1. ZWECK

Diese Leistungsbeschreibung definiert das Verfahren zur Cybersicherheitszertifizierung von Produkten der Informations- und Kommunikationstechnologie (IKT) und Schutzprofilen gemäß dem auf den Gemeinsamen Kriterien beruhenden europäischen System (EUCC), welches auf der Verordnung (EU) 2019/881 (Cybersecurity Act) sowie der Durchführungsverordnung (EU) 2024/482 basiert. Die Zertifizierungsstelle der TÜV NORD CERT GmbH ist eine benannte Stelle für die Vertrauenswürdigkeitsstufe „mittel“ (substantial) für die IKT-Produkttypen S1-S7, N1-N9 und C1.

Das auf den Common Criteria beruhende europäische System für die Cybersicherheitszertifizierung (EUCC) dient der formalen Bestätigung, dass Produkte der Informations- und Kommunikationstechnologie (IKT) spezifische Sicherheitsanforderungen erfüllen. Dieses Verfahren basiert auf der Verordnung (EU) 2019/881 (Cybersecurity Act) sowie der Durchführungsverordnung (EU) 2024/482. TÜV NORD CERT bietet als benannte Stelle Zertifizierungen für die Vertrauenswürdigkeitsstufe „mittel “ (substantial) an, was den Schwachstellen-Evaluierungsstufen AVA_VAN.1 oder 2 entspricht. Ziel ist der Schutz der Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten über den gesamten Lebenszyklus eines Produkts.

2. ZERTIFIZIERUNGSVERFAHREN UND -GEGENSTAND

Das Verfahren stellt durch eine unparteiische Evaluierung durch Dritte sicher, dass ein Evaluationsgegenstand (Target of Evaluation, TOE) festgelegte Sicherheitsanforderungen erfüllt.

Zertifizierungsgegenstand sind IKT-Produkte sowie deren Dokumentation. Ein Produkt kann ein Einzelgerät, ein Teil eines Produkts oder eine Technologie sein, die im Rahmen der Evaluierung als Evaluierungsgegenstand (Target of Evaluation, TOE) definiert wird. Zusätzlich können Schutzprofile (Protection Profiles, PP) zertifiziert werden, welche herstellerunabhängige Sicherheitsanforderungen für spezifische Produktkategorien festlegen.

3. ÜBERBLICK ÜBER DEN ZERTIFIZIERUNGSPROZESS

Die methodische Grundlage für den Prozess bilden die internationalen Normen ISO/IEC 15408 (Common Criteria) und ISO/IEC 18045 (CEM). Der Ablauf gliedert sich in mehrere Phasen von der Anfrage bis zur Zertifikatserteilung.

3.1. Angebotsanfrage und Zertifizierungsvereinbarung

Interessenten richten ihre Anfrage an die Zertifizierungsstelle, welche Informationsmaterial und Formulare bereitstellt. Für die Angebotserstellung liefert der Kunde eine Beschreibung des TOE-Umfangs (Scope). TÜV NORD CERT prüft die generelle Zertifizierbarkeit und erstellt auf Basis eines Kalkulationstools ein Angebot. Mit Unterzeichnung der Zertifizierungsvereinbarung und Anerkennung der Allgemeinen Zertifizierungsbedingungen EUCC wird der Auftrag formal erteilt.

3.2. Vorbereitung der Evaluierung

Seitens der Zertifizierungsstelle wird ein kompetenter und unparteiischer Veto-Manager benannt. In einem Kick-off-Meeting mit dem Kunden, dem Entwickler und dem Prüflabor (ITSEF) werden der Zeitplan und die Verfügbarkeit der Nachweise bestätigt. Der Kunde stellt die erforderlichen Entwicklernachweise bereit, insbesondere die Sicherheitsvorgaben (Security Target, ST), welche für die Stufe „substanziell“ zwingend Anforderungen zur Schwachstellenbewertung (AVA_VAN) und zu unabhängigen Tests (ATE_IND) enthalten müssen.

3.3. Evaluierung

Die technische Prüfung wird von einer unabhängigen, akkreditierten und für das EUCC-System autorisierten Einrichtung zur Evaluierung der IT-Sicherheit (ITSEF) durchgeführt. Die Evaluierung für die Vertrauenswürdigkeitsstufe „mittel“ umfasst Methoden wie Dokumentenprüfung, unabhängige Funktionstests sowie eine Schwachstellenanalyse auf Basis öffentlich bekannter Informationen. Das Prüflabor verifiziert dabei, dass das Produkt gegen Angreifer mit „Basis-Angriffspotenzial“ resistent ist.

3.4. Evaluierungsbericht

Nach Abschluss der Prüftätigkeiten erstellt die ITSEF einen formalen technischen Evaluierungsbericht (ETR). Der Veto-Manager der Zertifizierungsstelle überprüft den ETR auf Übereinstimmung mit den Nachweisen und die korrekte Anwendung der Evaluierungsnormen. Er kann bei Bedarf Klarstellungen oder zusätzliche Informationen von der ITSEF einfordern.

3.5. Zertifikaterteilung

Basierend auf dem validierten ETR erstellt die Zertifizierungsstelle einen Zertifizierungsbericht. Bei positivem Ergebnis trifft der TIC-Manager die formale Zertifizierungsentscheidung und stellt das EUCC-Zertifikat aus. Im Falle einer Ablehnung wird der Kunde schriftlich unter Angabe der Gründe informiert; gegen diese Entscheidung kann innerhalb von 4 Wochen Widerspruch eingelegt werden. Zertifizierte Produkte werden in einer öffentlichen Liste geführt und die Ergebnisse an die ENISA gemeldet.

4. ZERTIFIKATSLAUFZEIT UND ÜBERWACHUNG

Das EUCC-Zertifikat hat eine Gültigkeitsdauer von maximal fünf Jahren. Während dieser Zeit ist der Inhaber verpflichtet, ein Schwachstellenmanagement zu betreiben und Informationen über neue Sicherheitslücken aktiv zu überwachen. Die Zertifizierungsstelle führt eine Überprüfung durch, die durch Beschwerden, direkte Anfragen der nationalen Behörden (NCCA) oder Informationen über Schwachstellen ausgelöst werden kann. Jährlich erfolgt zudem eine stichprobenartige Überprüfung der Konformität (mindestens 4 % der Zertifikate) durch die NCCA.

5. ÄNDERUNGEN IN DER ZERTIFIZIERUNG

Sicherheitsrelevante Änderungen am Produkt oder der Umgebung erfordern ein Verfahren zur Gewährleistung der Kontinuität der Vertrauenswürdigkeit (Assurance Continuity). Der Inhaber muss hierzu einen Auswirkungsanalysebericht (Impact Analysis Report, IAR) vorlegen.

- Geringfügige Änderungen: Die Zertifizierungsstelle validiert die Analyse und ergänzt den ursprünglichen Bericht um einen Aufrechterhaltungsbericht.
- Erhebliche Änderungen: Eine erneute (Teil-)Evaluierung durch die ITSEF ist erforderlich, wobei gültige Ergebnisse der Vorbewertung wiederverwendet werden können. Zudem kann ein zertifiziertes Patchverwaltungsverfahren genutzt werden, um Updates strukturiert in das zertifizierte Produkt zu übernehmen.

6. REZERTIFIZIERUNGSEVALUIERUNG

EUCC-Zertifikate haben eine maximale Geltungsdauer von fünf Jahren. Eine Verlängerung erfordert eine Neubewertung (Re-assessment), bei der insbesondere das aktuelle Bedrohungsumfeld und die Lebenszyklusprozesse erneut geprüft werden.

7. ERWEITERUNGSEVALUIERUNG

Soll der Anwendungsbereich oder die Vertrauenswürdigkeitsstufe eines bestehenden Zertifikats geändert werden, führt dies zum Widerruf des alten und zur Ausstellung eines neuen EUCC-Zertifikats mit angepasstem Geltungsbereich.

8. ÜBERNAHME VON ZERTIFIZIERUNGEN

Innerhalb der EU ausgestellte EUCC-Zertifikate werden in allen Mitgliedstaaten verbindlich anerkannt. Evaluierungsergebnisse früherer Zertifizierungen können unter bestimmten Bedingungen (z. B. Bericht jünger als 2 Jahre, gleiche ITSEF) teilweise wiederverwendet werden.