TeleTrusT-Mitgliederkonferenz

TeleTrusT – Bundesverband IT-Sicherheit e.V.

Berlin, 29.11.2018

TeleTrusT Prüfschema für Produkte nach IEC 62443-4-2

Tobias Glemser, secuvera

secuvera

BSI-zertifizierter IT-Sicherheitsdienstleister und Prüfstelle

TeleTrusT- Mitgliederkonferenz

TeleTrusT Pioneers in IT security.

Prüfschema für IEC 62443-4-2

Berlin, 29. November 2018

- Drei Beratungsfelder
  - BSI-Prüfstelle für Common Criteria (Produktzertifizierungen)
  - Penetrationstests/Webanwendungsprüfungen
  - BSI-Grundschutz/ISO 27001
- BSI-zertifizierter IT-Sicherheitsdienstleister
  - Kompetenzfeststellung durch das Bundesamt für Firma und Berater

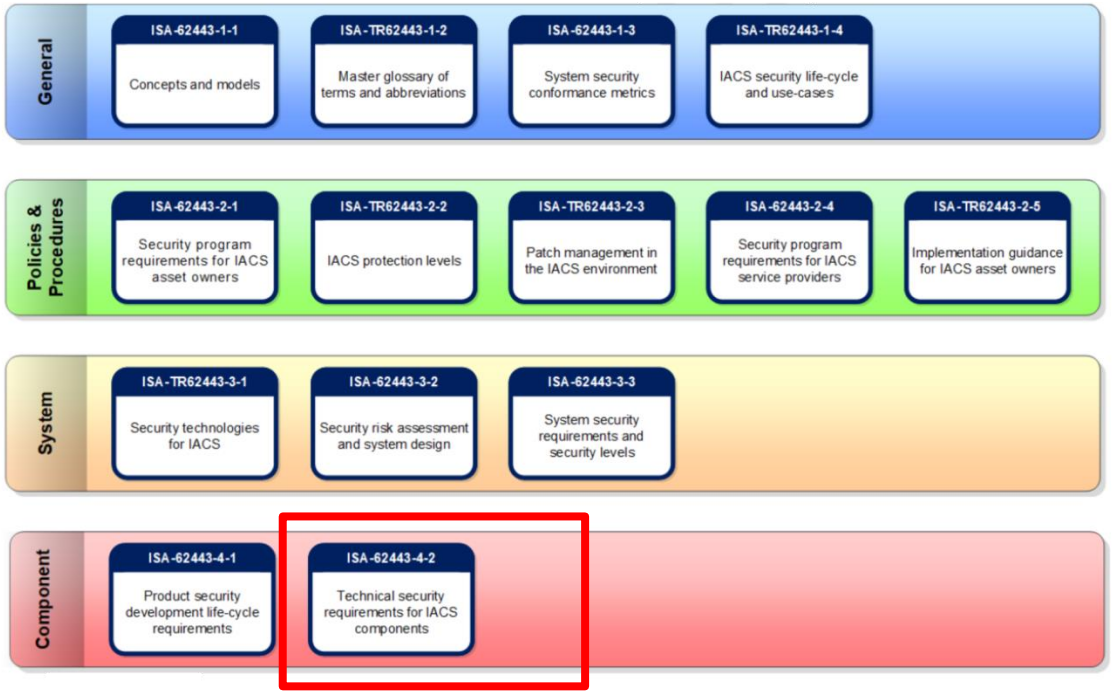
- Prüfstelle

  auch anerkannt als Prüflabor bei TÜV NORD CERT
  für Prüfungen nach IEC 62443

IEC 62443

relevanter Ausschnitt

- Aufbau der ISA/IEC 62443



Quelle: ISA99 Committee

- Bewertung einer Komponente
  - Embedded
    - z. B. PLC, Sensoren, SIS (Safety Instrumented Systems), Controller, DCS (Distributed Control System) Controller
  - Host
    - z. B. Notebooks oder PC Workstations
  - Network
    - z. B. Industrial Router
  - Applications
    - z. B. Konfigurations-Software, Historisierungssoftware

- Bewertung einer Komponente

  Ansätze:

  – Bewertung des Entwicklungsprozesses (62443-4-1)
  – Bewertung des Produktes (62443-4-2)

  wichtig: hier nur Prüfschema für 62443-4-2

  – Feststellung der technische Fähigkeiten (Capabilities) einer Komponente

- Bewertung des Produktes nach IEC 62443-4-2
  - Fokus Automatisierungs-Komponente
  - Feststellung der technische Fähigkeiten (Capabilities)
    - SL-C = Security-Level-Capability
    - SL = Security Level (zentrales Konzept der IEC 62443)

- Organisation der IEC 62443-4-2
  - Strukturebene
    - Katalog an Anforderungen
    - Foundational Requirements (FR) (Anzahl: 7)
  - Detailebene
    - je FR strukturiert
    - Component Requirements (CR)
    - entsprechen i.d.R. den System Requirements (SR) (Teil 3-3)

secuvera

Warum ein Prüfschema?

secuvera

Security Zertifikat

Security-Audit Januar 2018

Auditprozess:	NIST SP800-115 (adaptiert) & OSSTMM.
Konzeptaudit:	BSI Grundschutz-Katalog, IEC 62443-3-3, IEC62443-4-2 Draft.
Komponentenaudits:	Vulnerability-Analyse, Angriffe mit Standardwerkzeugen, Fuzzing über Ethernetport, Prüfung des Signierungsverfahrens für Firmware, Analyse der Kommunikationsverfahren.
Systemaudit:	Securityprüfung anhand eines Referenz-Aufbaus (Ende zu Ende), Schwachstellenanalyse der Komponenten von Drittherstellern mittels CVEs, OWASP Top 10 Bedrohungsanalyse.

- 62443-4-2 definiert Anforderungen an das Produkt
  - aber aus Standard lassen sich
    - Detailgrad der CR häufig nicht ausreichend
    - keine konkreten Tests ableiten
    - ergeben sich keine Vorgaben für Bewertung
    - CRs decken Bedrohungsaspekt nicht ab
  - im Ergebnis: Prüfstellen/Zertifizierungsstellen gehen
  - mit Standard sehr unterschiedlich um

- Prüfschema definiert Vorgaben für Prüflabore
  - Existiert derzeit nicht
  - Bedarf am Markt gegeben
  - Weitgehende Einheitlichkeit des Prüfrahmens
    - d.h. Klarheit für Hersteller
  - Ohne Vorgaben: keine Vergleichbarkeit von Zertifikaten
    - schlecht für Leser der Zertifikate
    - schlecht für Hersteller
    - schlecht für Prüfe

- Idee: Ein Branchenverband definiert Prüfschema
  - Feedback durch andere Verbände
  - Notwendigkeit: einer muss vorlegen…
  - entwickelt vom Tele-TrusT
  - kommentiert über VDMA, ZVEI, DKE, …

- zur Prüfung benötigt
  - Scoping (Kompontenspezifikation)
    - Komponenten-Kategorie:
      - Application, Embedded, Host, Network
    - Schnittstellen
    - Verwendungszweck (intended use)
    - Sicherheitsfunktionalität
      - z. B. Trennung zwischen Plattform und Anwendung
    - Dokumentation
    - Abgrenzung
      - z. B. Sensoren/Aktoren nicht betrachten bei Fernwartung

- Inhalt Prüfschema
  - Konformitätsbehauptung
    - entweder nur über SL-Stufe
      - definiert Component Requirements (CR) und Angreifertyp
    - oder detaillierter
      - Auswahl von CRs,
      - und Angreifertyp über SL-Stufe
  - Warum Differenzierung?
    - Komponentenhersteller mit offenem Markt, oder
    - System-Hersteller für konkrete Anwendungen

- Inhalt Prüfschema
  - Prüfschritte
    1. Prüfung des Verwendungszwecks
    2. Dokumentation (Design/Prüfung)
    3. Dokumentation (Anwender)
    4. Konformitätsprüfung
    5. Schwachstellenanalyse

- Inhalt Prüfschema
  - Prüfschema für SL-2 und SL-3
    - unter-/oberhalb aktuell nicht relevant
  - Zu jeder CR werden Konformitätstests durch das Prüflabor definiert
  - Jeder Test muss mit pass/fail beantwortbar sein

- Inhalt Prüfschema
  - Prüfung des Verwendungszwecks, Dokumentation (Design/Prüfung), Dokumentation (Anwender)
  - zunehmende Tiefe mit zunehmender SL-Stufe

Auszug:

SL-Stufe / Angreifertyp	Geforderte Design-Dokumentation
SL-2 / gering	Schnittstellenbeschreibung, u.a.: alle kabelgebundenen und funkbasierten Kommunikationsschnittstellen sowie elektrische Schnittstellen mit Beschreibung der Funktionalität und Konfigurationsmöglichkeiten, z. B. eine Schnittstelle zur Gerätekonfiguration mit technischer Beschreibung des Protokolls und aller Konfigurationsparameter, zusätzlich detaillierte Informationen zu eingesetzter Software mit 3rd-Party-Libraries und exakter Version
SL-3 / mittel	zusätzlich internes Design, u.a.: Nennung von Subsystemen und Modulen mit Funktionalität und Konfigurationsmöglichkeiten

- Inhalt Prüfschema
  - Konformitätsprüfung
  - Prüfschema beinhaltet im Anhang Akzeptanzkriterien
    - accept / not accept
    - Abhängigkeiten für Szenario/Verwendungszweck
    - flexibel über Prüfschema fortschreibbar
  - Aufgabe Prüfstelle
    - zu jeder CR 1..n konkrete Konformitätstests definieren
    - jeden Test mit pass/fail bewertbar

- Inhalt Prüfschema
  - Konformitätsprüfung: Beispiel
  - FR 1 - Identification and Authentication Control
    - CR 1.12 - System use notification: "When a component provides local human user access/HMI, it shall provide the capability to display a system use notification message before authenticating.

- Inhalt Prüfschema
  - *Acceptance Criteria*

    SL-1 requirements

    Accept:

    - *capability to display a system use notification message before authenticating to the local user interface*
    - *capability to configurable the message by authorized user*
  - *Test:*
    - *Is a System Use Notification displayed at the HMI?*
    - *Is the System Use Notification configurable?*

- Inhalt Prüfschema
  - Schwachstellenanalyse
    - Nicht alle notwendigen Analysen können direkt aus Anforderungen (CRs) abgeleitet werden
    - Beispiel: OpenSSH (3rd party library)
      - Suche nach öffentlich bekannten Schwachstellen in OpenSSH-X.X
      - Verwundbar gegenüber CVE-2017-XXXXX
      - Nicht direkt aus einer Component Requirement ableitbar
      - ➔ Schwachstellenanalyse erforderlich

- Inhalt Prüfschema
  - Bewertung nach „Vulnerability Assessment (AVA)" Methodik
    - definiert in ISO/IEC 18045 / Common Evaluation Methodology, Anhang B
    - Diskussion des kompletten Angriffs

- Abgrenzung
  - Zertifizierung
    - Prüfschema definiert nur die technische Prüfung
    - nicht anwendbar (not applicable, N/A)
      - Aufgabe der Zertifizierer
    - auch nicht im Fokus Zertifizierungsumfang
      - IEC 62443-4-2 oder nur kombiniert IEC 62443-4-1/-2

- weitere Anwendungsfälle
  - technische Assessments in Lieferanten-Auftragnehmer-Beziehungen
  - interne Prüfung der technischen Fähigkeiten/Resistenz der eigenen Produkte durch eine interne Prüfer

- Kritikpunkte in der Kommentierung (Auszug)
  - 4-1 ➔ sicheres Produkt
    - Man muss zur Prüfung auf Prüfstand rollen
  - Schwachstellenprüfung nur intern
    - Externer Blick ➔ andere Ergebnisse und Erkenntnisgewinn
  - Anforderungen an Produkt (z. B. Firewall) kann doch die Umgebung abdecken
    - Nein, das Ziel ist eine sichere Komponente, die den Anforderungen genügt

- Roadmap
  - Vorstellung Tele-TrustT-Vorhaben bei Verbänden ✓
  - Erstellung Draft Schema bis zum Sommer ✓
  - Feedbackrunde ✓
  - Veröffentlichung vorab zur it-sa 2018 ✓
  - Diskussion in DKE/TBKON-Cybersecurity ✓
  - Anfang Januar Editing Session im DKE, parallel Übersetzung
  - Angestrebt: In IECEE WG31 "Cyber Security" einbringen
  - Anwendung jetzt möglich

secuvera

BSI-zertifizierter IT-Sicherheitsdienstleister und Prüfstelle

Vielen Dank