IEC 62443-1-1
Industrielle Kommunikationsnetze - IT-Sicherheit für Netze und Systeme

Teil 1-1: Begriffe und Modelle

Die IEC/TS 62443-1-1:2009 "Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models" (Industrielle Kommunikationsnetze - IT-Sicherheit für Netze und Systeme) ist eine Technische Spezifikation, die von der IEC veröffentlicht wurde. Sie legt die Terminologie, Konzepte und Modelle für die IT-Sicherheit in der Automatisierungstechnik fest.

Im Unterabschnitt 1.2 "Behandelte Funktionalität" wird klargestellt, dass der Anwendungsbereich der Normenreihe IEC 62443 nicht nur Anlagen der industriellen Automatisierungstechnik umfasst, sondern auch solche in kritischen Infrastrukturen, wie z.B. in der elektrischen Energieübertragung und in Gas- und Wassernetzen.

Die sogenannten grundlegenden Anforderungen werden im Unterabschnitt 5.3 eingeführt:

a) Identifizierung und Authentifizierung (identification and authentication control IAC): den Zugriff von Nutzern (Menschen, Geräten oder Softwareprozesse) auf das Automatisierungssystem regeln;
b) Nutzung kontrollieren (use control UC): die Nutzung ausgewählter Geräte, Informationen oder beides überwachen, um vor nicht autorisiertem Betrieb des Gerätes oder unerlaubter Informationsverwendung zu schützen;
c) Systemintegrität (system integrity SI): die Integrität des industriellen Automatisierungssystems sicherstellen und nicht autorisierte Manipulation verhindern;
d) Datenvertraulichkeit (data confidentiality DC): Vertraulichkeit von Daten in Kommunikationskanälen und Datenbeständen sicherstellen, um deren nicht autorisierte Offenlegung zu verhindern;
e) eingeschränkter Datenfluss (restricted data flow, RDF): das Automatisierungssystem in Zonen und Conduits aufteilen, um einen unnötigen Datenfluss zu verhindern;
f) auf Ereignisse schnell reagieren (timely response TRE): auf Verletzungen der IT-Sicherheit durch Benachrichtigung der zuständigen Stellen rechtzeitig reagieren, die notwendige Sicherung von Beweisen anfordern und automatisch und rechtzeitig in für den Erfolg des Systems kritischen oder sicherheitskritischen Situationen Korrekturmaßnahmen veranlassen;
g) Verfügbarkeit der Mittel und Ressourcen (resource availability RA): die Verfügbarkeit aller Netzwerkressourcen sicherstellen, um so vor Denial-of-Service-Angriffen zu schützen.

Weitere durch diese Publikation eingeführte Konzepte sind die gestaffelte Verteidigung (defense in depth), die Bedrohungs-Risikobeurteilung, die Reife eines IT-Sicherheitsprogramms, IT-Sicherheitsleitlinien, Zonen und Conduits (zur Aufteilung des betrachteten Systems) sowie Security-Level (SL).

Diese beschreiben abgestuft den Einsatz, mit dem ein erwarteter Angreifer vorgehen wird:

- SL 1: zufällige Fehlanwendung,

- SL 2: absichtliche Versuche mit einfachen Mitteln,
- SL 3: wie SL2, aber mit Kenntnissen und entsprechenden Mitteln,
- SL 4: wie SL 3 aber mit erheblichen Mitteln.

Je nach der Position im Lebensweg, auf den sich der SL bezieht, wird unterschieden zwischen:

- SL-T (SL target): dieser zu erzielende SL ist ein Ergebnis der Bedrohungs-Risikoanalyse,
- SL-C (SL capable): SL, den ein Gerät oder System erreichen kann, wenn es richtig eingesetzt und konfiguriert wird,
- SL-A (SL achieved): der im Gesamtsystem erreichte und messbare SL.

Ingo Rolle, im November 2015