



Bild: Pixabay

Durch die permanente Verbindung von verschiedensten Systemen sind Sicherheitskontrollen unumgänglich.

ISO 27400:2022 – Sicherheit für IoT-Geräte

Internet of Things (IoT) ist heutzutage nicht mehr wegzudenken. In vielen Maschinen, Geräten, Lampen, Kühlschränken, usw. sind heute vernetzte Computer-Elemente enthalten. IoT-Systeme stellen damit eine besondere Herausforderung für die Informationssicherheit dar, da sie hochgradig verteilt sind und eine grosse Anzahl unterschiedlicher Einheiten umfassen. Dies bedeutet eine grosse Angriffsfläche damit auch eine Herausforderung angemessene Sicherheitskontrollen für das gesamte System anzuwenden und aufrechtzuerhalten. Ende Juni 2022 wurde die ISO 27400 veröffentlicht, welche die IoT-Sicherheit und den Datenschutz adressiert.

Wie gewohnt definieren ISO-Normen der 27000er zuerst den Umfang und geben normati-

ve Referenzen, bevor im Kapitel 3 Begriffe und Definitionen folgen. Diesmal sind es acht Begriffe rund um Cloud und IoT. Die Norm definiert auch acht zusätzliche Abkürzungen.

Das Kapitel 5 stellt IoT-Konzepte vor. Da es wenig Sinn macht alle Anwendungen zu beschreiben, werden Gemeinsamkeiten beschrieben, wie dass IoT-Geräte spezifische Hardware- und Software besitzen, mit dem Netzwerk

verbunden sind und damit Daten senden und empfangen können, in der Regel über Sensorfunktionen verfügen, können aktionsfähig sein, das heisst, sie können Steuerdaten empfangen, um physische Aktionen auszulösen, umfassen IoT-Anwendungen und Betriebskomponenten sowie unterstützen menschliche oder digitale Nutzer.

Bei IoT-Geräten ist die Preisgestaltung ein wichtiges Merkmal, weshalb niedrige Kosten für Herstellung und Betrieb von IoT-Geräten wichtig sind. Industrielle IoT-Systeme können industrielle Anlagen und Steuerungssysteme ersetzen oder in Verbindung mit ihnen eingesetzt werden und unterliegen daher ähnlichen Anforderungen wie hoher Verfügbarkeit oder Sicherheit. In Fahrzeugen

eingesetzte IoT-Systeme werden im Zusammenhang mit Zuverlässigkeits- oder sicherheitsrelevanten Funktionalitäten verwendet. Viele IoT-Dienste funktionieren (nur) mit einem entsprechenden Cloud-Dienst. Daher sollten Nutzer sicherstellen, dass der Cloud-Dienst über angemessene Sicherheitskontrollen verfügt.

Die Norm definiert im Kapitel 5.3 die Interessengruppen. Dazu gehören Dienstleister, Entwickler und Benutzer. Die Abhängigkeiten zwischen den Anbietern, den Entwicklern und den Nutzern im Zusammenhang mit der Sicherheit und dem Schutz der Privatsphäre in einem IoT-System bezeichnet die Norm als Ökosystem. Dies wird in verschiedene Lebenszyklen abgebildet. Ein IoT-Dienst wird von einem IoT-Dienstentwickler und einem IoT-Geräteentwickler entwickelt, die von einem IoT-Dienstanbieter bereitgestellt und die von IoT-Nutzern verwendet werden. Diese Schritte werden im Detail beschrieben. An dieser Stelle wird nicht weiter darauf eingegangen.

Risiko-Quellen

Bei IoT-Systemen sind viele Quellen für Risiken vorhanden. Das Kapitel 6 geht detaillierter auf dies ein. Als Methode wird auf andere Normen wie die ISO 31000 oder ISO 27005 verwiesen.

Folgende Kategorien werden aufgeführt:

- Schwachstelle des IoT-Systems
- mangelnde Kenntnisse und Fähigkeiten der Personen, die bei der Bereitstellung oder Nutzung eine Rolle spielen
- menschliches Versagen von Personen, die an der Bereitstellung oder Nutzung beteiligt sind
- Personen, die böswillige Absicht haben, das IoT-System anzugreifen
- Qualität des IoT-Systems und seiner Komponenten
- Vorhandensein von externen Systemen und Geräten, die für

ZUM AUTOR

Andreas Wisler, Dipl. Ing FH
goSecurity AG
Schulstrasse 11
CH-8542 Wiesendangen
T +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch

Anzeige



elesa.com

Discover our products !



An Elessa Company

MOZAIR **elesa**

STANDARD MACHINE ELEMENTS WORLDWIDE

Angriffe auf das IoT-System missbraucht werden können

- Naturereignisse (Blitzschlag, Überschwemmung und Erdbeben)
- fehlende organisatorische Governance bei den involvierten Akteuren

Im Gegensatz zu vielen anderen ISO-Normen zeigt die ISO 27400 sehr viele Beispiele von Risikoquellen. Im Bereich Sensorik und Kontrolle sind es beispielsweise 11, in den Bereichen Betrieb und Management, Anwendung und Dienstleistung sowie Benutzer sind es jeweils sechs und beim Ressourcenzugang und Datenaustausch vier. Im Anhang A.1 wird als Beispiel eine Risiko-Bewertung einer IoT-Überwachungskamera durchgeführt.

Zusätzlich werden Risikoquellen ausserhalb der IoT-Domänen aufgezeigt, dazu gehören Hacker, für einen Missbrauch anfällige Systeme und Geräte, Naturereignisse, die Abhängigkeit von Strom und Netzdiensten oder der Komplexität. Auch der Datenschutz wird immer wichtiger und wird adressiert. Für die Anwender ist es schwierig die Architektur der IoT-Produkte und die von den IoT-Sensoren über ihn gesammelten Daten zu verstehen, da die Einzelheiten der erfassten Daten entweder nicht von den Geräteherstellern weitergegeben werden. IoT-Geräte können miteinander kommunizieren und so Profile von Nutzern erstellen und das Nutzerverhalten durch Datenaggregation, Re-Identifizierung und Analysemethoden erfassen, um daraus beispielsweise geschäftliche Vorteile zu ziehen, was ohne das Wissen oder die Zustimmung des Nutzers geschehen könnte. So kann beispielsweise ein digitaler Eindruck unseres täglichen Lebens durch die Überwachung von intelligenten Geräten zu Hause, die Verfolgung des Standorts unserer intelligenten Autos, die Überwachung unserer Gesundheitsparameter durch intelligente Gesundheitsgeräte oder die Verfolgung unserer Gespräche mit intelligenten Geräten, die für einen anderen Zweck bestimmt sind, entstehen.

Sicherheitskontrollen

Als Ergänzung zu den Kontrollen aus der ISO 27002 werden 45 Si-

cherheitskontrollen für IoT-Dienstentwickler und IoT-Dienstleister empfohlen. Aufgebaut sind sie nach dem Schema:

- Zweck: erklärt den Zweck der Kontrolle
- Zielgruppe: nennt die beteiligten Akteure, die über die Kontrolle informiert werden sollen
- IoT-Domäne: listet die Domänen auf, auf die sich die Kontrolle bezieht
- Leitfaden: liefert Informationen zur Durchführung

Sie teilen sich in Informationssicherheit (1-28) und Datenschutz (29-45) auf.

Nachfolgend werden die Sicherheitskontrollen kurz vorgestellt:

- 01: Politik für IoT-Sicherheit
- 02: Organisation der IoT-Sicherheit
- 03: Informationsverwaltung
- 04: Ausrüstung und Werte, die sich ausserhalb physisch gesicherter Bereiche befinden
- 05: Sichere Entsorgung oder Wiederverwendung von Geräten
- 06: Aus Sicherheitsvorfällen lernen
- 07: Grundsätze der sicheren IoT-Systemtechnik
- 08: Sichere Entwicklungsumgebung und -verfahren
- 09: Sicherheit von IoT-Systemen zur Unterstützung der Sicherheit
- 10: Sicherheit bei der Verbindung verschiedener IoT-Geräte
- 11: Verifizierung von IoT-Geräten und Systemdesign
- 12: Überwachung und Protokollierung
- 13: Schutz von Protokollen
- 14: Nutzung geeigneter Netzwerke für die IoT-Systeme
- 15: Sichere Einstellungen und Konfigurationen bei der Bereitstellung von IoT-Geräten und -diensten
- 16: Benutzer- und Geräteauthentifizierung
- 17: Bereitstellung von Software- und Firmware-Updates
- 18: Austausch von Informationen über Schwachstellen
- 19: Sicherheitsmassnahmen, die an den Lebenszyklus von IoT-Systemen und -diensten angepasst sind
- 20: Anleitung für IoT-Nutzer zur ordnungsgemässen Nutzung von IoT-Geräten und -diensten

- 21: Festlegung von Sicherheitsrollen für die Beteiligten
- 22: Verwaltung von gefährdeten Geräten
- 23: Management von Lieferantenbeziehungen im Bereich IoT-Sicherheit
- 24: Sichere Weitergabe von Informationen über die Sicherheit von IoT-Geräten
- 25: Kontakte und Support-Service
- 26: Grundeinstellungen von IoT-Gerät und -Dienst
- 27: Deaktivierung von nicht verwendeten Geräten
- 28: Sichere Entsorgung oder Wiederverwendung von IoT-Geräten
- 29: Prävention von in die Privatsphäre eingreifenden Ereignissen
- 30: IoT-Datenschutz als Standard
- 31: Bereitstellung eines Datenschutzhinweises
- 32: Verifizierung der IoT-Funktionalität
- 33: Berücksichtigung von IoT-Nutzern
- 34: Verwaltung von IoT-Datenschutzkontrollen
- 35: Eindeutige Geräteidentität
- 36: Ausfallsichere Authentifizierung
- 37: Minimierung der indirekten Datenerfassung
- 38: Mitteilung der Datenschutzpräferenzen
- 39: Überprüfung der automatisierten Entscheidung

- 40: Rechenschaftspflicht gegenüber den Beteiligten
- 41: Schutz personenbezogener Daten
- 42: Austausch von Informationen über Massnahmen zum Schutz von personenbezogenen Daten bei IoT-Geräten
- 43: Zustimmung des Benutzers
- 44: Zweckmässige Nutzung zur Verbindung mit anderen Geräten und Diensten
- 45: Zertifizierung/Validierung des Schutzes von personenbezogenen Daten

Fazit

Zusammenfassend ist die ISO 27400 ein umfassendes Nachschlagemittel, wenn es um die Sicherheits- und Datenschutzanforderungen von IoT-Geräten geht. Verschiedene Risiken werden aufgezeigt und beschrieben. Das Beispiel Risikoszenario einer IoT-Überwachungskamera hilft ein Verständnis dafür zu bekommen. Die 45 Sicherheitskontrollen zu den Themen Informationssicherheit und Datenschutz helfen, geeignete Massnahmen zum Schutz der Systeme und Daten zu bekommen.

■ Anzeige



Führend in additiver Fertigung

Wir fertigen Ihre Serienbauteile

- additiv
- in hoher Qualität
- wirtschaftlich
- **nachhaltig & seit 20.04.23 STI-gelistet**

prodartis AG
Zielstrasse 38
9050 Appenzell
info@prodartis.ch
www.prodartis.ch





SUSTAINABLE DEVELOPMENT GOALS



SWISS triple impact