Bundesamt
für Sicherheit in der
Informationstechnik

SYS.4.4 Allgemeines IoT-Gerät

1. Beschreibung

1.1. Einleitung

Geräte mit Funktionen aus dem Bereich Internet of Things (IoT) sind, im Gegensatz zu klassischen Endgeräten, vernetzte Geräte oder Gegenstände, die zusätzliche „smarte“ Funktionen besitzen. IoT-Geräte werden in der Regel drahtlos an Datennetze angeschlossen. Die meisten Geräte können auf Informationen im Internet zugreifen und darüber erreicht werden. Hierdurch können sie Auswirkungen auf die Informationssicherheit des gesamten Informationsverbunds haben.

IoT-Geräte, wie Smartwatches oder andere Wearables, können in Institutionen gelangen, indem sie durch Mitarbeitende oder Externe am Körper getragen werden. In vielen Institutionen werden aber auch IoT-Geräte beschafft und betrieben, darunter etwa Brand-, Gas- und andere Warnmelder, Kaffeemaschinen oder Elemente der Gebäudesteuerung wie Kameras und HVAC (Heating, Ventilation and Air Conditioning).

Generell kann zwischen direkt adressierbaren IoT-Geräten und IoT-Geräten, die eine zentrale Steuereinheit voraussetzen, unterschieden werden. Direkt adressierbare Geräte werden in der Regel mit einer eigenen IP-Adresse an das LAN angeschlossen oder haben einen eigenen direkten Netzanschluss, z. B. mittels Mobilfunk, und können autark agieren oder durch eine zentrale Steuereinheit verwaltet werden. Daneben gibt es IoT-Geräte, die ausschließlich direkt mit Steuereinheiten kommunizieren, z. B. über Funknetze wie Bluetooth oder ZigBee, und somit nicht direkt an bestehende Datennetze angeschlossen werden.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, IoT-Geräte so abzusichern, dass über diese weder die Informationssicherheit der eigenen Institution noch die von Außenstehenden beeinträchtigt wird. Daher sollte sowohl ein unautorisierter Datenabfluss als auch die Manipulation der Geräte verhindert werden, speziell mit Blick auf Angriffe durch Dritte.

1.3. Abgrenzung und Modellierung

Der Baustein SYS.4.4 *Allgemeines IoT-Gerät* ist auf jedes Gerät mit Funktionalitäten aus dem Bereich Internet of Things (IoT) anzuwenden.

Dieser Baustein beschäftigt sich allgemein mit IoT-Geräten und soll für ein großes Spektrum unterschiedlicher IoT-Geräte anwendbar sein. Auf dedizierte Sicherheitseigenschaften, etwa von

Bedien- und Anzeigesystemen oder spezifischen Hard- und Software-Architekturen, wird nicht näher eingegangen.

Je nach Ausprägung der IoT-Geräte sind die Übergänge zu industriellen Steuerungssystemen (ICS-Systemen) oder eingebetteten Systemen fließend. Anforderungen an Geräte, die im Bereich Produktion und Fertigung eingesetzt werden, sind in den Bausteinen der Schicht IND *Industrielle IT* zu finden.

Eingebettete Systeme hingegen sind informationsverarbeitende Systeme, die in ein größeres System oder Produkt integriert sind, dort Steuerungs-, Regelungs- und Datenverarbeitungsaufgaben übernehmen und dabei oft nicht direkt von den Benutzenden wahrgenommen werden. Für diese Systeme ist der Baustein SYS.4.3 *Eingebettete Systeme* umzusetzen.

Anforderungen an die häufig im Zusammenhang mit IoT-Geräten eingesetzten Funkstrecken befinden sich in den Bausteinen der Schicht NET.2 *Funknetze*.

Die im betrachteten Informationsverbund eingesetzten IoT-Geräte sind im Identitäts- und Berechtigungsmanagement zu berücksichtigen. Hierfür ist der Baustein ORP.4 *Identitäts- und Berechtigungsmanagement* umzusetzen.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein SYS.4.4 *Allgemeines IoT-Gerät* von besonderer Bedeutung.

2.1. Ausspähung über IoT-Geräte

Bei der Entwicklung von IoT-Geräten wird der Aspekt der Informationssicherheit typischerweise nicht oder nur nachrangig beachtet. Das sorgte in der Vergangenheit dafür, dass IoT-Geräte immer wieder dazu missbraucht wurden, um Informationen über die Benutzenden oder den Einsatzbereich zu sammeln. So sind immer wieder Vorfälle mit vernetzten bzw. IP-basierten Überwachungskameras eingetreten:

- 2021 wurden Überwachungskameras durch erneute Registrierung der Kamera-ID gehackt. Es konnte so die Steuerung übernommen werden.
- 2022 wurden Videostreams von Babymonitoren durch eine fehlende Authentisierung bei einem Angriff auf andere Server umgeleitet. Aufgrund der fehlenden Authentisierung war es sogar möglich die Steuerung zu übernehmen.

Ende September 2016 wurde bekannt, dass einige Modelle von Überwachungskameras und Raumsensoren mit Hintertüren ausgestattet sind, die Spionage ermöglichen. Dies betraf insbesondere Überwachungskameras, die in Rechenzentren und Serverräumen eingesetzt wurden. Die Hintertüren ermöglichten offenbar, dass auf die Bild- und Videodaten der Kameras zugegriffen werden konnte und dass diese Daten auf Server im Internet kopiert werden konnten. Auf diese Weise konnten z. B. Kennwörter von Benutzenden oder Administrierenden kompromittiert werden oder Gerätekonfigurationen, Infrastrukturdetails und sonstige vertrauliche Informationen Dritten zugänglich werden. Dies erleichterte weitergehende Angriffe, indem die Gewohnheiten der Mitarbeitenden ausgenutzt wurden.

2.2. Verwendung von UPnP

In LANs integrierte IoT-Geräte bauen oftmals selbstständig eine Verbindung zum Internet auf, indem sie Router im Netz per UPnP (Universal Plug and Play) so konfigurieren, dass eine Portweiterleitung entsteht. Die Geräte können dann nicht nur ins lokale Netz kommunizieren, sondern sind auch außerhalb des LANs sicht- und erreichbar. Wenn dann eine Schwachstelle im IoT-Gerät durch einen

Angreifer ausgenutzt wird, könnte dieses Gerät Teil eines Botnetzes werden. Außerdem könnte weitere Schadsoftware in den Informationsverbund eingeschleust werden. Diese Sicherheitslücke kann zu einem späteren Zeitpunkt auch für weitere missbräuchliche Aktivitäten ausgenutzt werden.

2.3. Übernahme in ein Botnetz

Wenn IoT-Geräte nicht regelmäßig gepatcht werden, bleiben bekannte Schwachstellen offen und können für umfangreiche Angriffe ausgenutzt werden. Ein Ziel eines Angriffs könnte sein, die IoT-Geräte in ein Botnetz zu integrieren. In diesem Fall könnten sie beispielsweise dazu missbraucht werden, um DDoS-Angriffe (Distributed Denial of Service) auszuführen und die Verfügbarkeit von Diensten einzuschränken.

Häufig werden dazu Botnetze benutzt, die zu großen Teilen aus IoT-Geräten bestehen. Mit der Schadsoftware "Mirai", die es bereits seit 2016 gibt, werden beispielsweise Webcams, Kameras, digitale Videorecorder, Router und Drucker in ein Botnetz integriert. Sie scannen dann selbstständig das Internet nach weiteren Geräten, um sie mit Schadsoftware zu infizieren und dem Botnetz hinzuzufügen. Zusätzlich gibt es auch weitere Varianten einer solchen Schadsoftware wie "Mozi" oder "BotenaGo", die 2019 und 2021 eine ähnliche Vorgehensweise anwendeten.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.4.4 *Allgemeines IoT-Gerät* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rolle
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Beschaffungsstelle, Haustechnik

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderung

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

SYS.4.4.A1 Einsatzkriterien für IoT-Geräte (B)

IoT-Geräte MÜSSEN Update-Funktionen besitzen. Die herstellenden Unternehmen MÜSSEN einen Update-Prozess anbieten. Die Geräte MÜSSEN eine angemessene Authentisierung ermöglichen. Es DÜRFEN KEINE fest codierten oder herzuleitenden Zugangsdaten in den Geräten enthalten sein.

SYS.4.4.A2 Authentisierung (B)

Eine angemessene Authentisierung MUSS aktiviert sein. IoT-Gerate MÜSSEN in das Identitäts- und Berechtigungsmanagement der Institution integriert werden.

SYS.4.4.A3 ENTFALLEN (B)

Diese Anforderung ist entfallen.

SYS.4.4.A4 ENTFALLEN (B)

Diese Anforderung ist entfallen.

SYS.4.4.A5 Einschränkung des Netzzugriffs (B)

Der Netzzugriff von IoT-Geräten MUSS auf das erforderliche Minimum eingeschränkt werden. Dies SOLLTE regelmäßig kontrolliert werden. Dazu SOLLTEN folgende Punkte beachtet werden:

- Bei Verkehrskontrollen an Netzübergängen, z. B. durch Regelwerke auf Firewalls und Access Control Lists (ACLs) auf Routern, DÜRFEN NUR zuvor definierte ein- und ausgehende Verbindungen erlaubt werden.
- Die Routings auf IoT-Geräten und Sensoren, insbesondere die Unterdrückung von Default-Routen, SOLLTE restriktiv konfiguriert werden.
- Die IoT-Geräte und Sensoren SOLLTEN in einem eigenen Netzsegment betrieben werden, das ausschließlich mit dem Netzsegment für das Management kommunizieren darf.
- Virtual Private Networks (VPNs) zwischen den Netzen mit IoT-Geräten und Sensor-Netzen und den Management-Netzen SOLLTEN restriktiv konfiguriert werden.
- Die UPnP-Funktion MUSS an allen Routern deaktiviert sein.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

SYS.4.4.A6 Aufnahme von IoT-Geräten in die Sicherheitsrichtlinie der Institution (S)

In der allgemeinen Sicherheitsrichtlinie der Institution SOLLTEN die Anforderungen an IoT-Geräte konkretisiert werden. Die Richtlinie SOLLTE allen Personen, die IoT-Geräte beschaffen und betreiben, bekannt und Grundlage für deren Arbeit sein. Die Umsetzung der in der Richtlinie geforderten Inhalte SOLLTE regelmäßig überprüft und die Ergebnisse sinnvoll dokumentiert werden.

SYS.4.4.A7 Planung des Einsatzes von IoT-Geräten (S)

Um einen sicheren Betrieb von IoT-Geräten zu gewährleisten, SOLLTE im Vorfeld geplant werden, wo und wie diese eingesetzt werden sollen. Die Planung SOLLTE dabei nicht nur Aspekte betreffen, die klassischerweise mit dem Begriff Informationssicherheit verknüpft werden, sondern auch normale, betriebliche Aspekte, die Anforderungen im Bereich der Sicherheit nach sich ziehen. Alle Entscheidungen, die in der Planungsphase getroffen wurden, SOLLTEN geeignet dokumentiert werden.

SYS.4.4.A8 Beschaffungskriterien für IoT-Geräte (S) [Beschaffungsstelle]

Der oder die ISB SOLLTE bei allen Beschaffungen von IoT-Geräten mit einbezogen werden. Bevor IoT-Geräte beschafft werden, SOLLTE festgelegt werden, welche Sicherheitsanforderungen diese erfüllen müssen. Bei der Beschaffung von IoT-Geräten SOLLTEN Aspekte der materiellen Sicherheit ebenso wie Anforderungen an die Sicherheitseigenschaften der Software ausreichend berücksichtigt werden. Eine Anforderungsliste SOLLTE erstellt werden, anhand derer die am Markt erhältlichen Produkte bewertet werden.

SYS.4.4.A9 Regelung des Einsatzes von IoT-Geräten (S)

Für jedes IoT-Gerät SOLLTE eine zuständige Person für dessen Betrieb benannt werden. Die Zuständigen SOLLTEN ausreichend über den Umgang mit dem IoT-Gerät informiert werden.

SYS.4.4.A10 Sichere Installation und Konfiguration von IoT-Geräten (S)

Es SOLLTE festgelegt werden, unter welchen Rahmenbedingungen IoT-Geräte installiert und konfiguriert werden. Die IoT-Geräte SOLLTEN nur von autorisierten Personen (Zuständige für IoT-Geräte, Administrierende oder vertraglich gebundene Dienstleistende) nach einem definierten Prozess installiert und konfiguriert werden. Alle Installations- und Konfigurationsschritte SOLLTEN so dokumentiert werden, dass die Installation und Konfiguration durch sachkundige Dritte anhand der Dokumentation nachvollzogen und wiederholt werden kann.

Die Grundeinstellungen von IoT-Geräten SOLLTEN überprüft und nötigenfalls entsprechend den Vorgaben der Sicherheitsrichtlinie angepasst werden. Falls möglich, SOLLTEN IoT-Geräte erst mit Datennetzen verbunden werden, nachdem die Installation und die Konfiguration abgeschlossen sind.

SYS.4.4.A11 Verwendung von verschlüsselter Datenübertragung (S)

IoT-Geräte SOLLTEN Daten nur verschlüsselt übertragen.

SYS.4.4.A12 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.4.4.A13 Deaktivierung und Deinstallation nicht benötigter Komponenten (S)

Nach der Installation SOLLTE überprüft werden, welche Protokolle, Anwendungen und weiteren Tools auf den IoT-Geräten installiert und aktiviert sind. Nicht benötigte Protokolle, Dienste, Anmeldekennungen und Schnittstellen SOLLTEN deaktiviert oder ganz deinstalliert werden. Die Verwendung von nicht benötigten Funkschnittstellen SOLLTE unterbunden werden.

Wenn dies nicht am Gerät selber möglich ist, SOLLTEN nicht benötigte Dienste über die Firewall eingeschränkt werden. Die getroffenen Entscheidungen SOLLTEN so dokumentiert werden, dass nachvollzogen werden kann, welche Konfiguration für die IoT-Geräte gewählt wurden.

SYS.4.4.A14 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.4.4.A15 Restriktive Rechtevergabe (S)

Die Zugriffsberechtigungen auf IoT-Geräte SOLLTEN möglichst restriktiv vergeben werden. Wenn dies über die IoT-Geräte selber nicht möglich ist, SOLLTE überlegt werden, dies netzseitig zu regeln.

SYS.4.4.A16 Beseitigung von Schadprogrammen auf IoT-Geräten (S)

Der IT-Betrieb SOLLTE sich regelmäßig informieren, ob sich die eingesetzten IoT-Geräte mit Schadprogrammen infizieren könnten und wie Infektionen beseitigt werden können. Schadprogramme SOLLTEN unverzüglich beseitigt werden. Kann die Ursache für die Infektion nicht behoben bzw. eine Neuinfektion nicht wirksam verhindert werden, SOLLTEN die betroffenen IoT-Geräte nicht mehr verwendet werden.

SYS.4.4.A17 Überwachung des Netzverkehrs von IoT-Geräten (S)

Es SOLLTE überwacht werden, ob die IoT-Geräte oder Sensor-Systeme nur mit IT-Systemen kommunizieren, die für den Betrieb der IoT-Geräte notwendig sind.

SYS.4.4.A18 Protokollierung sicherheitsrelevanter Ereignisse bei IoT-Geräten (S)

Sicherheitsrelevante Ereignisse SOLLTEN automatisch protokolliert werden. Falls dies durch die IoT-Geräte selber nicht möglich ist, SOLLTEN hierfür Router oder Protokollmechanismen anderer IT-Systeme genutzt werden. Die Protokolle SOLLTEN geeignet ausgewertet werden.

SYS.4.4.A19 Schutz der Administrationsschnittstellen (S)

Abhängig davon, ob IoT-Geräte lokal, direkt über das Netz oder über zentrale netzbasierte Tools administriert werden, SOLLTEN geeignete Sicherheitsvorkehrungen getroffen werden. Der Zugriff auf die Administrationsschnittstellen von IoT-Geräten SOLLTE wie folgt eingeschränkt werden:

- Netzbasierte Administrationsschnittstellen SOLLTEN auf berechtigte IT-Systeme bzw. Netzsegmente beschränkt werden.
- Es SOLLTEN bevorzugt lokale Administrationsschnittstellen am IoT-Gerät oder Administrationsschnittstellen über lokale Netze verwendet werden.

Die zur Administration verwendeten Methoden SOLLTEN in der Sicherheitsrichtlinie festgelegt werden. Die IoT-Geräte SOLLTEN entsprechend der Sicherheitsrichtlinie administriert werden.

SYS.4.4.A20 Geregelte Außerbetriebnahme von IoT-Geräten (S)

Es SOLLTE eine Übersicht darüber geben, welche Daten wo auf IoT-Geräten gespeichert sind. Es SOLLTE eine Checkliste erstellt werden, die bei der Außerbetriebnahme von IoT-Geräten abgearbeitet werden kann. Diese Checkliste SOLLTE mindestens Aspekte zur Datensicherung weiterhin benötigter Daten und dem anschließenden sicheren Löschen aller Daten umfassen.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

SYS.4.4.A21 Einsatzumgebung und Stromversorgung (H) [Haustechnik]

Es SOLLTE geklärt werden, ob IoT-Geräte in der angedachten Einsatzumgebung betrieben werden dürfen (Schutzbedarf anderer IT-Systeme, Datenschutz). IoT-Geräte SOLLTEN in der Einsatzumgebung vor Diebstahl, Zerstörung und Manipulation geschützt werden.

Es SOLLTE geklärt sein, ob ein IoT-Gerät bestimmte Anforderungen an die physische Einsatzumgebung hat, wie z. B. Luftfeuchtigkeit, Temperatur oder Energieversorgung. Falls erforderlich, SOLLTEN dafür ergänzende Maßnahmen bei der Infrastruktur umgesetzt werden.

Wenn IoT-Geräte mit Batterien betrieben werden, SOLLTE der regelmäßige Funktionstest und Austausch der Batterien geregelt werden.

IoT-Geräte SOLLTEN entsprechend ihrer vorgesehenen Einsatzart und dem vorgesehenen Einsatzort vor Staub und Verschmutzungen geschützt werden.

SYS.4.4.A22 Systemüberwachung (H)

Die IoT-Geräte SOLLTEN in ein geeignetes Systemüberwachungs- bzw. Monitoringkonzept eingebunden werden. Der Systemzustand und die Funktionsfähigkeit der IoT-Geräte SOLLTEN laufend überwacht werden. Fehlerzustände sowie die Überschreitung definierter Grenzwerte SOLLTEN an das Betriebspersonal gemeldet werden. Es SOLLTE geprüft werden, ob die verwendeten Geräte die Anforderung an die Verfügbarkeit erfüllen. Alternativ SOLLTE geprüft werden, ob weitere Maßnahmen, wie das Einrichten eines Clusters oder die Beschaffung von Standby-Geräten, erforderlich sind.

SYS.4.4.A23 Auditierung von IoT-Geräten (H)

Alle eingesetzten IoT-Geräte SOLLTEN regelmäßig auditiert werden.

SYS.4.4.A24 Sichere Konfiguration und Nutzung eines eingebetteten Webservers (H)

In IoT-Geräten integrierte Webserver SOLLTEN möglichst restriktiv konfiguriert sein. Der Webserver SOLLTE, soweit möglich, NICHT unter einem privilegierten Konto betrieben werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Im Dokument "Sicherheit von Geräten im Internet der Dinge" gibt das BSI einen Überblick über die elementaren Best Practices zum sicheren Betrieb von IoT-Kameras zu geben.

Das Department of Homeland Security (DHS) hat im Dokument "Strategic Principles for securing the Internet of Things (IoT)" strategische Grundsätze für die Sicherheit von IoT-Geräten veröffentlicht.

Das Open Web Application Security Project (OWASP) stellt auf seiner Webseite Hinweise zur Absicherung von IoT-Geräten zur Verfügung.

Der europäische Standard ETSI EN 303 645 "Cyber Security for Consumer Internet of Things: Baseline Requirements" dient als Empfehlung für die sichere Entwicklung von IoT-Geräten (Security by Design). Hierzu gehören unter anderem sichere Authentisierungsmechanismen, ein angemessenes Updatemanagement und die Absicherung der Kommunikation. Er findet unter anderem auch beim IT-Sicherheitskennzeichen des BSI Anwendung in verschiedenen Produktkategorien des IoT.