NIST Interner Bericht
NIST IR 8425 ger

Profil der IoT-Referenzgrundlage für Verbraucher-IoT-Produkte

Michael Fagan
Katerina Megas
Paul Watrobski
Jeffery Marron
Barbara Cuthill

Diese Veröffentlichung ist kostenlos erhältlich unter:
https://doi.org/10.6028/NIST.IR.8425.ger

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Interner Bericht
NIST IR 8425 ger

Profil der IoT-Referenzgrundlage für Verbraucher-IoT-Produkte

Michael Fagan
Katerina N. Megas
Paul Watrobski
Jeffrey Marron
Barbara B. Cuthill
Abteilung für angewandte Cybersicherheit
Labor für Informationstechnologie

Diese Veröffentlichung ist kostenlos erhältlich unter:
https://doi.org/10.6028/NIST.IR.8425.ger

September 2022

U.S. Handelsministerium
Gina M. Raimondo, Ministerin
National Institute of Standards and TechnologyLaurie E. Locascio, NIST-Direktorin und stellvertretende Handelsministerin für Standards und Technologie

Bestimmte kommerzielle Einrichtungen, Geräte oder Materialien können in diesem Dokument genannt werden, um ein experimentelles Verfahren oder Konzept angemessen zu beschreiben. Eine solche Kennzeichnung soll weder eine Empfehlung oder Befürwortung durch das Nationale Institut für Standards und Technologie (NIST) („National Institute of Standards and Technology“) bedeuten, noch soll sie implizieren, dass die Einrichtungen, Materialien oder Geräte notwendigerweise die besten für den jeweiligen Zweck sind.

In dieser Veröffentlichung kann auf andere Publikationen verwiesen werden, die derzeit vom NIST in Übereinstimmung mit den ihm zugewiesenen gesetzlichen Aufgaben entwickelt werden. Die in dieser Veröffentlichung enthaltenen Informationen, einschließlich der Konzepte und Methoden, können von den Bundesbehörden bereits vor der Fertigstellung solcher Begleitpublikationen verwendet werden. Bis zur Fertigstellung der einzelnen Veröffentlichungen bleiben also die derzeitigen Anforderungen, Leitlinien und Verfahren, soweit vorhanden, in Kraft. Für Planungs- und Übergangszwecke sollten die Bundesbehörden die Entwicklung dieser neuen Veröffentlichungen des NIST aufmerksam verfolgen.

Organisationen sind aufgefordert, alle Publikationsentwürfe während der öffentlichen Kommentierungszeiträume zu prüfen und dem NIST Feedback zu geben. Viele weitere NIST-Publikationen zum Thema Cybersicherheit, außer den oben genannten, sind unter https://csrc.nist.gov/publications erhältlich.

NIST-Richtlinien für technische Bereiche
Erklärungen zu Copyright, Fair Use und Lizenzierung
Syntax des NIST-Veröffentlichungsindexes für technische Bereiche („NIST Technical Series Publication Identifier Syntax“)

Veröffentlichungshistorie
Genehmigt durch das NIST Editorial Review Board am 2022-09-08

Wie diese NIST Technical Series Veröffentlichung zu zitieren ist:
Fagan M, Megas KN, Watrobski P, Marron J, Cuthill B (2022) Profile of the IoT Core Baseline for Consumer IoT Products. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8425. https://doi.org/10.6028/NIST.IR.8425

Autor ORCID iDs
Michael Fagan: 0000-0002-1861-2609
Katerina N. Megas: 0000-0002-2815-5448
Paul Watrobski: 0000-0002-6449-3030
Jeffrey Marron: 0000-0002-7871-683X
Barbara B. Cuthill: 0000-0002-2588-6165

Kontaktinformationen
iotsecurity@nist.gov

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

Alle Kommentare unterliegen der Freigabe gemäß dem Freedom of Information Act (FOIA).

Berichte über Computersystemtechnik

Das Information Technology Laboratory (ITL) am National Institute of Standards and Technology (NIST) fördert die US-Wirtschaft und das öffentliche Wohl, indem es die technische Führung für die Mess- und Normungsinfrastruktur der Nation übernimmt. Das ITL entwickelt Tests, Testmethoden, Referenzdaten, Konzeptnachweise und technische Analysen, um die Entwicklung und den produktiven Einsatz von Informationstechnologie zu fördern. Zu den Aufgaben des ITL gehört die Entwicklung von Management-, Verwaltungs-, technischen und physischen Standards und Richtlinien für die kosteneffiziente Sicherheit und den Schutz der Privatsphäre von Informationen, die nicht die nationale Sicherheit betreffen, in Informationssystemen des Bundes.

Zusammenfassung

Diese Veröffentlichung dokumentiert das Verbraucherprofil der IoT-Referenzgrundlage für Verbraucher-IoT-Produkte (Internet of Things (IoT), Internet der Dinge) und identifiziert Cybersicherheitsfähigkeiten, die für den IoT-Verbrauchersektor (d. h. IoT-Produkte für den Heim- oder Privatgebrauch) allgemein erforderlich sind. Sie kann auch ein Ausgangspunkt für Unternehmen sein, die den Kauf von IoT-Produkten in Betracht ziehen. Das Verbraucherprofil wurde als Teil der NIST-Antwort auf die Executive Order 14028 entwickelt und wurde ursprünglich in *Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products* veröffentlicht. Die Fähigkeiten des Verbraucherprofils sind als Cybersicherheitsergebnisse formuliert, die für das gesamte IoT-Produktspektrum gelten sollen. In diesem Dokument werden auch die Grundlagen für die Entwicklung des empfohlenen Verbraucherprofils und die damit verbundenen Überlegungen erörtert. Das NIST bezog eine Reihe relevanter Quellen ein, um das Verbraucherprofil zu erstellen, und arbeitete ein Jahr lang mit Interessengruppen zusammen, um die Empfehlungen zu entwickeln.

Schlüsselwörter

Internet der Dinge („Internet of Things“, IoT); Verbraucher-IoT; Cybersicherheit; IoT-Produkte; Datenschutz; Sicherheit; sicherungsfähige Produkte.

Zielgruppe

Dieser Bericht richtet sich an Hersteller von Konsumgütern, insbesondere an Produktsicherheitsbeauftragte, Einzelhändler und damit verbundene Integratoren und technische Supportfirmen, die den Verbraucher- und Unternehmenssektor bedienen, sowie an Prüf- und Zertifizierungsstellen, die an der Erstellung von Referenzgrundlagen für IoT-Cybersicherheitsleistungen interessiert sind.

Mitteilung über die Offenlegung von Patenten

HINWEIS: Das ITL hat die Inhaber von Patentansprüchen, deren Verwendung für die Einhaltung der Leitlinien oder Anforderungen dieser Veröffentlichung erforderlich sein könnte, aufgefordert, diese Patentansprüche dem ITL mitzuteilen. Die Inhaber von Patenten sind jedoch nicht verpflichtet, auf Patentanfragen von ITL zu antworten, und ITL hat keine Patentrecherche durchgeführt, um festzustellen, welche Patente, wenn überhaupt, auf diese Veröffentlichung zutreffen könnten.

Zum Zeitpunkt der Veröffentlichung und nach Aufforderung(en) zur Identifizierung von Patentansprüchen, deren Verwendung für die Einhaltung der Leitlinien oder Anforderungen dieser Veröffentlichung erforderlich sein könnte(n), wurden dem ITL keine solchen Patentansprüche gemeldet.

Das ITL übernimmt keine Gewähr dafür, dass bei der Verwendung dieser Publikation keine Lizenzen erforderlich sind, um Patentverletzungen zu vermeiden.

Inhaltsübersicht

Liste der Tabellen

Liste der Abbildungen

Danksagungen

Die Autoren danken allen, die zu dieser Publikation beigetragen haben, einschließlich der Teilnehmer an den Workshops und anderen interaktiven Sitzungen; den Einzelpersonen und Organisationen aus dem privaten und öffentlichen Sektor, einschließlich der Hersteller aus verschiedenen Sektoren sowie mehreren Herstellerhandelsorganisationen, die während der Antwortfrist der Executive Order 14028 des NIST Feedback gegeben haben. Besonderer Dank gilt den Mitgliedern des Cybersecurity for IoT-Teams Rebecca Herold, Brad Hoehn und David Lemire.

1. Einführung

Am 12. Mai 2021 erließ der Präsident die Executive Order (EO) 14028, die neben anderen Richtlinien das NIST aufforderte, Anforderungen für ein Programm zur Kennzeichnung der Cybersicherheit von IoT-Produkten für Verbraucher zu empfehlen. Als Teil der Antwort des NIST auf diese Richtlinie[1]wurde ein Profil der IoT-Referenzgrundlage[2] für Verbraucher-IoT-Produkte erstellt. Dieses Profil diente als Teil der Empfehlungen, die das NIST als Reaktion auf die EO im Februar 2022 unter dem Titel *Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products* [EO_Kriterien].veröffentlichte.

Das Profil baut auf der NISTIR 8259-Serie auf, indem es die IoT-Referenzgrundlage für Verbraucher-IoT-Produkte erweitert. NISTIR 8259, *Foundational Cybersecurity Activities for IoT Device Manufacturers* [IR8259] (*Grundlegende Cybersicherheitsaktivitäten für Hersteller von IoT-Geräten*), bietet Herstellern von IoT-Geräten einen grundlegenden Leitfaden für die Entwicklung von IoT-Geräten, die von Kunden sicher genutzt werden können. NISTIR 8259 zielt nicht auf einen bestimmten IoT-Sektor ab, sondern erörtert, wie Hersteller die Cybersicherheit für IoT-Geräte im Allgemeinen angehen können. NISTIR 8259A, *IoT-Geräte-Cybersicherheitsfähigkeit-Referenzgrundlage („IoT Device Cybersecurity Capability Core Baseline“)* [IR8259A] und NISTIR 8295B, *Referenzgrundlage für nicht-technische IoT-unterstützende Fähigkeiten („IoT Non-Technical Supporting Capability Core Baseline“)* [IR259B] definieren die IoT-Geräte-Cybersicherheitsfähigkeit-Referenzgrundlage, auch als Referenzgrundlage bezeichnet („IoT Device Cybersecurity Capability Core Baseline“, auch als „Referenzgrundlage“ bezeichnet). Die Referenzgrundlage ist ein Ausgangspunkt für die Hersteller, um die Cybersicherheitsfunktionen zu ermitteln, die ihre Kunden von den von ihnen hergestellten IoT-Geräten erwarten können. NISTIR 8259A erörtert die Cybersicherheitsfähigkeiten von Geräten, d. h. Funktionen oder Merkmale, die vom Gerät durch seine eigene Hardware und Software implementiert werden. So werden in NISTIR 8259A unter anderem Konzepte wie Datenschutz, Zugriffskontrolle und Softwareaktualisierung erörtert. NISTIR 8259B erörtert nicht-technische unterstützende Fähigkeiten, d. h. Maßnahmen, die von Organisationen zur Unterstützung der Cybersicherheit des Geräts ergriffen werden. In NISTIR 8259B werden beispielsweise Konzepte wie Aufklärung und Bewusstsein sowie die Entgegennahme von Informationen und Anfragen (z. B. durch Hersteller/Entwickler) erörtert.

Wie NISTIR 8259 sind diese Basisdokumente nicht branchen- oder anwendungsspezifisch, sondern stellen einen Ausgangspunkt für *jedes* IoT-Gerät dar. Die Anpassung der Basisfähigkeiten an einen bestimmten Sektor und/oder Anwendungsfall erfordert eine Art Profiling. Der Profiling-Prozess unter Verwendung der NISTIR 8259-Serie leitet einen Profiler an, sektor- bzw. anwendungsfallspezifische Informationen zu sammeln und die relevanten Auswirkungen zu interpretieren, um die Basisfähigkeiten auszuwählen, die am besten auf die Bedürfnisse und Ziele der Kunden im jeweiligen Sektor bzw. Anwendungsfall zutreffen.

[1] Weitere Informationen über die Antwort des NIST auf die Aufforderung der EO 14028, Empfehlungen für ein Cybersicherheitslabel für IoT-Produkte für Verbraucher abzugeben, finden Sie unter https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/cybersecurity-labeling-consumers-0

[2] Die Begriffe *Referenzgrundlage („Core Baseline“), IoT-Referenzgrundlage („IoT Core Baseline“) und Referenzgrundlage zu Basisfähigkeiten von IoT-Geräten („IoT Device Core Capability Baseline“)* beziehen sich alle auf die in den NISTIRs 8259A und 8259B vorgestellten Fähigkeiten.

Der Rest dieses Dokuments beschreibt die Ergebnisse dieses Profiling-Prozesses für den Verbrauchersektor und ist wie folgt gegliedert:

- In Abschnitt 2 wird die beabsichtigte Anwendbarkeit des Verbraucherprofils auf IoT-Produkte für Verbraucher erläutert und das Verbraucherprofil definiert.
- In Abschnitt 3 wird das Verfahren zur Erstellung des Verbraucherprofils näher beschrieben.
- Abschnitt 4 befasst sich mit zusätzlichen Überlegungen, die der Leser bei der Verwendung des Verbraucherprofils anstellen sollte.

2. Verbraucherprofil der IoT-Referenzgrundlage („IoT Core Baseline“)

Dieser Abschnitt baut auf dem Whitepaper *Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products* [EO_Kriterien] auf. Zunächst wird der Umfang eines „IoT-Produkts“ definiert, dann wird das Profil des IoT-Produkts für Verbraucher der IoT-Referenzgrundlage vorgestellt.

2.1. Erklärung zum IoT-Produktumfang

Verbraucher -IoT-Produkte bestehen häufig aus einer Reihe von Systemkomponenten, die zusammenarbeiten, um Funktionen zu liefern, die am Endpunkt oder an der „Gerätekomponente“ des Produkts realisiert werden. Das NIST beschreibt ein IoT-Gerät als Computerausrüstung mit mindestens einem Wandler (d.h. Sensor oder Aktuator) und mindestens einer Netzwerkschnittstelle [IR8259]. Alle IoT-Produkte enthalten mindestens ein IoT-Gerät und es ist möglich, dass diese lediglich aus nur dieser Produktkomponente bestehen. In vielen Fällen kann das IoT-Produkt als ein Gerät gekauft werden (d. h. das IoT-Gerät), benötigt aber noch andere Komponenten für den Betrieb, wie z. B. ein Backend (z. B. einen Cloud-Server) oder eine begleitende Benutzeranwendung auf einem PC oder Smartphone.

Komplexe IoT-Produkte können mehrere physische IoT-Geräte enthalten, andere Arten von Geräten umfassen oder mit mehreren Backends oder Begleitanwendungen als Komponenten verbunden sein. Obwohl es möglicherweise eine große Anzahl von Komponentenkombinationen gibt, aus denen ein IoT-Produkt entstehen kann, ist es hilfreich, an drei spezifische Arten von IoT-Produktkomponenten zu denken (abgesehen vom IoT-Gerät selbst, das immer in einem IoT-Produkt vorhanden ist):

- Spezielle Netzwerk-/Gateway-Hardware (z. B. ein Hub innerhalb des Systems, in dem das IoT-Gerät verwendet wird).
- Begleitende Anwendungssoftware (z. B. eine mobile App für die Kommunikation mit dem IoT-Gerät).
- Backends (z. B. ein Cloud-Dienst oder mehrere Dienste, die Daten aus dem IoT-Gerät speichern und/oder verarbeiten können).

Einige IoT-Produktkomponenten, wie z. B. das/die IoT-Gerät(e) (und vielleicht eine spezielle Netzwerk-/Gateway-Hardware[3]), werden „in der Box" enthalten sein, die der Kunde kauft.[4] Andere Komponenten, wie z. B. begleitende Anwendungssoftware oder Backends, werden „außerhalb der Box" existieren[5], sind aber dennoch Teil des IoT-Produkts durch die Unterstützung, die sie für den Betrieb des IoT-Produkts bieten. Unabhängig von diesen Beziehungen haben diese zusätzlichen Produktkomponenten Zugriff auf das IoT-Gerät und die Daten, die es erstellt und verwendet. Damit sind sie potenzielle Angriffsvektoren, die sich auf das IoT-Gerät, den Kunden und andere auswirken können (z. B. durch Angriffe auf Systeme, lokale Netzwerke oder das Internet insgesamt). Da diese zusätzlichen Komponenten neue oder einzigartige Risiken für das IoT-Produkt mit sich bringen können, muss das gesamte IoT-Produkt, einschließlich der Zusatzkomponenten, gesichert werden können.

Anmerkung zu den Überlegungen zur Konformitätsbewertung von IoT-Komponenten

In diesem Dokument werden die Eigenschaften auf der Ebene des IoT-Produkts erörtert, aber IoT-Produkte werden als eine Reihe von IoT-Produktkomponenten definiert. Bei der Betrachtung des Konformitätsbewertungsprozesses in diesem Zusammenhang ist es wichtig, die Komplexität der Bewertung der vielfältigen Kombinationen von IoT-Komponenten, aus denen ein Produkt bestehen könnte, zu beachten. Darüber hinaus können einige dieser IoT-Produktkomponenten vollständig oder teilweise *modularisiert* sein, so dass die Kunden die Möglichkeit haben, eine Komponente und/oder eine Komponentenplattform auszuwählen. So wird beispielsweise manche begleitende Anwendungssoftware auf mobilen Betriebssystemen oder über einen Webbrowser ausgeführt, wobei die Cybersicherheit weit über die Rolle hinausgeht, die diese Komponente im IoT-Produkt spielen mag. In diesen Fällen sollte bei der Bewertung dieser IoT-Produktkomponenten im Hinblick auf die Konformität mit den Cybersicherheitsfähigkeiten im Verbraucherprofil diese Tatsache berücksichtigt werden, und es sollten so weit wie möglich bestehende Normen und/oder Konformitätsmechanismen als Teil des IoT-Produktkonformitätsmechanismus verwendet werden. So kann es beispielsweise Zertifizierungsprogramme für Betriebssysteme oder Clouds geben, die eine teilweise Unterstützung für die im

[3] Einige spezielle Netzwerk-/Gateway-Hardware kann vom Kunden separat erworben werden, wird aber dennoch benötigt, damit das IoT-Produkt über die Grundfunktionen hinaus funktioniert. In den meisten Fällen, in denen ein IoT-Produkt separat gekaufte spezielle Netzwerk-/Gateway-Hardware erfordert, übernimmt diese Hardware spezifische, einheitliche Aufgaben bei der Implementierung eines IoT-Produkts (z. B. Protokollübersetzung). Einige IoT-Produkte benötigen beispielsweise andere Netzwerkverbindungen als die herkömmlichen WLAN-/Ethernet-Verbindungen, wie Bluetooth, Zigbee oder Z-Wave, für die ein *Hub* oder *Gateway* erforderlich ist, um eine breitere Konnektivität (d. h. über WLAN und/oder Ethernet) zu ermöglichen. Dieser *Hub* oder *Gateway* ist nicht immer Teil eines IoT-Produkts, sondern wird als Teil der Netzwerkinfrastruktur des Kunden betrachtet, ähnlich wie ein WLAN-Router bei IoT-Produkten, die WLAN verwenden.

[4] „In-the-Box"-Komponenten, insbesondere die IoT-Geräte, die als Endpunkt des Produkts dienen, können als das *Gesicht* des IoT-Produkts betrachtet werden, da sie von den Kunden physisch gehandhabt, verwaltet und genutzt werden. Auch wenn andere Komponenten für den Betrieb des IoT-Produkts von entscheidender Bedeutung sein können (einschließlich der Cybersicherheit), spielt(n) das (die) IoT-Gerät(e) eine zentrale Rolle für das IoT-Produkt und steht (stehen) im Allgemeinen im Zentrum des Betriebs des IoT-Produkts.

[5] Einige „Outside-the-Box"-Komponenten können in Bezug auf den Kunden völlig abgelegen sein, während andere physisch in der Umgebung des Kunden (z. B. in seinem Haus) vorhanden sein können, aber dennoch von dem/den IoT-Gerät(en) getrennt sind.

Verbraucherprofil genannten Cybersicherheitsfunktionen nachweisen können. In vielen Fällen wird die Unterstützung, die die IoT-Komponente für das Produkt bietet, jedoch durch zusätzliche Anwendungssoftware und/oder Hardware erreicht, die von den bestehenden Programmen möglicherweise nicht berücksichtigt oder bewertet wird. Die Bewertung der Cybersicherheit für das IoT-Produkt kann daher die bestehende Zertifizierung akzeptieren und die Cybersicherheit der zusätzlichen Anwendungssoftware/Hardware bewerten.

In diesem Zusammenhang wird ein IoT-Produkt als ein IoT-Gerät oder IoT-Geräte und alle zusätzlichen Produktkomponenten, die für die Nutzung des IoT-Geräts über die grundlegenden Betriebsfunktionen hinaus erforderlich sind definiert. So kann, zum Beispiel, eine nicht angeschlossene intelligente Glühbirne zwar immer noch in einer Farbe leuchten, aber ihre intelligenten Funktionen, wie z. B. der Farbwechsel, können ohne andere Produktkomponenten nicht genutzt werden.

2.2. Verbraucherprofil

In diesem Abschnitt werden die Cybersicherheitsfähigkeiten[6] definiert, die von IoT-Produkten und IoT-Produktentwicklern als Teil eines Verbraucherprofils erwartet werden.

Es wird empfohlen, die Produktkriterien sowohl auf das IoT-Produkt insgesamt ( ) als auch auf jede einzelne IoT-Produktkomponente anzuwenden. Die meisten Kriterien beziehen sich direkt auf das IoT-Produkt und sollen durch im IoT-Produkt implementierte Software- und/oder Hardware-Mittel erfüllt werden. Einige Kriterien gelten eher für den IoT-Produktentwickler als für das IoT-Produkt selbst. Es wird erwartet, dass diese Kriterien durch Handlungen erfüllt werden und durch Behauptungen und Nachweise des Entwicklers und nicht durch das IoT-Produkt selbst gestützt werden.

In der folgenden Abbildung werden die IoT-Produktfähigkeiten auf hoher Ebene und die Aktivitäten der IoT-Produktentwickler[7] dargestellt, die auf der Grundlage der NISTIRs 8259A und 8259B entwickelt wurden und in den folgenden Abschnitten erörtert werden.

[6] Der Begriff Fähigkeit wird in diesem Dokument in Anlehnung an die NISTIR 8259-Reihe verwendet, aber dieselben Fähigkeiten wurden in Abschnitt 2.2 der *Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products*als „Ergebnisse“ dargestellt. Diese Begriffe sind synonym und können im Zusammenhang mit diesem Dokument und dem Whitepaper austauschbar verwendet werden.
[7] In der Reihe NISTIR 8259 wird auf Hersteller von IoT-Geräten Bezug genommen, die mit den hier behandelten IoT-Produktentwicklern identisch sein können. Da IoT-Produkte jedoch aus mehreren Komponenten bestehen, erhöht sich die Wahrscheinlichkeit, dass das Unternehmen, das ein IoT-Produkt auf den Markt bringt, das/die physische(n) IoT-Gerät(e) nicht selbst hergestellt hat, sondern von einem anderen Unternehmen hergestellte Geräte verwendet, um ein IoT-Produkt herzustellen. Daher wird in diesem Dokument der Begriff IoT-Produktentwickler verwendet.

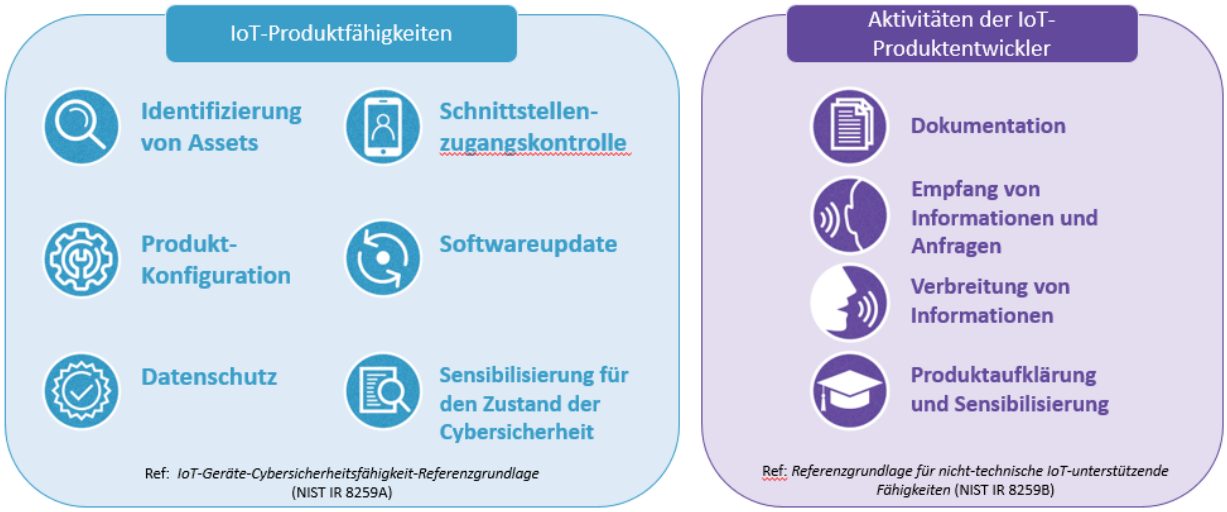

Abb. 1. Identifizierte Fähigkeiten für das Verbraucherprofil.

Für jede Fähigkeit werden der Name und eine ausführliche Definition der Fähigkeit angegeben, gefolgt von einer alphanumerischen Liste der Unterkriterien für jede Fähigkeit. Bei einigen Unterkriterien sind[8] nach dem **fettgedruckten** Text zusätzliche Details zum Ergebnis (d. h. normativer Text) aufgeführt, während zusätzliche Erläuterungen und Beispiele (d. h. informativer Text) nach dem *kursiv gedruckten* Text aufgeführt sind. Schließlich wird zu jeder Fähigkeit eine kurze Beschreibung des beabsichtigten Nutzens der Fähigkeit für die Cybersicherheit gegeben.

[8] Die Unterkriterien sollen zusätzliche Details darüber liefern, wie das in der High-Level-Fähigkeiten-Definition beschriebene Ergebnis durch ein IoT-Produkt erreicht werden kann. Die Unterkriterien umfassen möglicherweise nicht alle möglichen Unterstützungen, die für ein Ergebnis in allen Anwendungsfällen erforderlich sind, und die Unterkriterien gelten möglicherweise auch nicht für alle Anwendungsfälle.

2.2.1. IoT-Produktfähigkeiten

Identifizierung von Assets

Das IoT-Produkt ist eindeutig identifizierbar und beinhaltet alle IoT-Produktkomponenten.

1. Das IoT-Produkt kann vom Kunden und anderen autorisierten Stellen (z. B. dem IoT-Produktentwickler) eindeutig identifiziert werden.[9]
2. Das IoT-Produkt identifiziert jede IoT-Produktkomponente eindeutig und unterhält ein aktuelles Inventar[10] der angeschlossenen Produktkomponenten.

Cybersecurity-Dienstprogramm: Die Fähigkeit, IoT-Produkte und ihre Komponenten zu identifizieren, ist notwendig, um Aktivitäten wie Asset Management für Updates, Datenschutz und digitale Forensik für die Reaktion auf Vorfälle zu unterstützen.

[9] In einigen Fällen kann es eine eindeutige Kennung für das IoT-Produkt selbst geben (sogar unabhängig von der Kennung des IoT-Geräts), aber in vielen Fällen kann die Kennung des IoT-Produkts im Allgemeinen als Kennung einer der IoT-Komponenten interpretiert werden. Um die Einzigartigkeit des Produktidentifikators über alle Produktinstanzen hinweg zu gewährleisten, handelt es sich dabei in der Regel um das IoT-Gerät oder eine andere „In-Box"-Komponente und nicht um eine von vielen Instanzen gemeinsam genutzte Komponente wie das Backend.
[10] Je nach IoT-Produktarchitektur können sich Bestände auf einer Komponente (z. B. IoT-Gerät, Backend-Anwendung) oder auf mehreren Komponenten befinden (z. B. werden einige Komponenten auf spezieller Netzwerk-/Gateway-Hardware inventarisiert).

Produkt-Konfiguration

Die Konfiguration des IoT-Produkts ist veränderbar, es besteht die Möglichkeit, eine sichere Standardeinstellung wiederherzustellen, und alle Änderungen können nur von autorisierten Personen, Diensten und anderen IoT-Produktkomponenten vorgenommen werden.

1. Autorisierte Personen (d. h. Kunden), Dienste und andere IoT-Produktkomponenten können die Konfigurationseinstellungen des IoT-Produkts über eine oder mehrere IoT-Produktkomponenten ändern.[11]
2. Autorisierte Personen (d. h. Kunden), Dienste und andere IoT-Produktkomponenten haben die Möglichkeit, das IoT-Produkt auf eine sichere Standardkonfiguration (d. h. nicht initialisiert) zurückzusetzen.
3. Das IoT-Produkt wendet die Konfigurationseinstellungen auf die entsprechenden IoT-Komponenten an.

Cybersecurity-Dienstprogramm: Die Möglichkeit, Aspekte der Funktionsweise des IoT-Produkts zu ändern, kann den Kunden helfen, die Funktionalität des IoT-Produkts an ihre Bedürfnisse und Ziele anzupassen. Kunden können ihre IoT-Produkte so konfigurieren, dass sie bestimmte Bedrohungen und Risiken, die ihnen bekannt sind, entsprechend ihrer Risikobereitschaft vermeiden.

[11] Bei einigen Komponenten kann es eine für die Cybersicherheit relevante Konfiguration von Aspekten der Komponente (z. B. Plattform oder Infrastruktur von Backends) geben, die nicht in den angemessenen Rahmen für die Verwaltung durch das IoT-Produkt und/oder den Kunden fallen. So sollte beispielsweise in den meisten Fällen die Anwendungssoftware des IoT-Produkts nicht die Cybersicherheit des Betriebssystems verwalten, auf dem die Software läuft.

Datenschutz

Das IoT-Produkt schützt Daten, die in allen IoT-Produktkomponenten gespeichert sind und sowohl zwischen IoT-Produktkomponenten als auch außerhalb des IoT-Produkts übertragen werden, vor unbefugtem Zugriff, Offenlegung und Änderung.

1. Jede IoT-Produktkomponente schützt die von ihr gespeicherten Daten mit sicheren Mitteln.
2. Das IoT-Produkt ist in der Lage, gespeicherte Daten zu löschen oder unzugänglich zu machen, die entweder vom oder über den Kunden, das Haus, die Familie usw. gesammelt wurden.
3. Wenn Daten zwischen IoT-Produktkomponenten oder außerhalb des Produkts gesendet werden, werden Schutzmaßnahmen für die Datenübertragung verwendet.[12]

Cybersecurity-Dienstprogramm: Die Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Daten ist für die Cybersicherheit von IoT-Produkten von grundlegender Bedeutung. Die Kunden werden erwarten, dass die Daten geschützt werden und dass der Schutz der Daten dazu beiträgt, die sichere und beabsichtigte Funktionalität des IoT-Produkts zu gewährleisten.

[12] Dazu kann auch die Fähigkeit gehören, mit Produktkomponenten zu kommunizieren, die die Datenschutzfunktion nicht auf die gleiche Weise wie andere Komponenten implementieren können (z. B. keine angemessene Kryptographie unterstützen). Solche Kommunikation (z. B. Datenübertragungen mit minderwertigem oder begrenztem Schutz) sollte dennoch auf eine Weise erfolgen, die das nachfolgende Risiko reduziert, wie z. B. ein Nahbereichsübertragungsprotokoll und/oder ein lokales Netzwerkprotokoll (z. B. Zigbee, Bluetooth) zur Kommunikation mit einigen Produktkomponenten unter begrenzten, aber notwendigen Umständen.

Schnittstellenzugangskontrolle

Das IoT-Produkt beschränkt den logischen Zugriff auf lokale und Netzwerkschnittstellen – und auf Protokolle und Dienste, die von diesen Schnittstellen verwendet werden –auf autorisierte Personen, Dienste und IoT-Produktkomponenten.

1. Jede IoT-Produktkomponente kontrolliert den Zugang zu und von allen Schnittstellen (z. B. lokale Schnittstellen, unabhängig davon, ob sie von außen zugänglich sind oder nicht, Netzwerkschnittstellen, Protokolle und Dienste), um den Zugriff auf ausschließlich autorisierte Stellen zu beschränken. **Mindestanforderungen an die IoT-Produktkomponente:**
    a. Es werden ausschließlich Schnittstellen verwendet, die für den Betrieb des IoT-Produkts erforderlich sind, und es wird nur auf diese Schnittstellen Zugriff gewährt. Alle anderen Kanäle und Zugänge zu den Kanälen werden entfernt oder gesichert.
    b. Für alle Schnittstellen, die für die Nutzung des IoT-Produkts erforderlich sind, gibt es Zugangskontrollmaßnahmen (z. B. eindeutige, passwortbasierte Multifaktor-Authentifizierung, physische Schnittstellen, die von der Außenseite einer Komponente nicht zugänglich sind).
    c. Für alle Schnittstellen sind die Zugriffs- und Änderungsberechtigungen begrenzt.
2. Einige, aber nicht notwendigerweise alle IoT-Produktkomponenten verfügen über die Mittel zum Schutz und zur Aufrechterhaltung der Schnittstellenzugriffskontrolle. **Das IoT-Produkt muss mindestens:**
    a. überprüfen, ob die zwischen IoT-Produktkomponenten ausgetauschten Daten den festgelegten Definitionen von Format und Inhalt entsprechen.
    b. die unbefugte Übertragung oder den Zugriff auf andere Produktkomponenten verhindern.
    c. eine angemessene Zugangskontrolle bei der ersten Verbindung (d. h. beim Onboarding) und bei der Wiederherstellung der Verbindung nach einer Unterbrechung oder einem Ausfall aufrechterhalten.

Cybersecurity-Dienstprogramm: Die Aufzählung und Kontrolle des Zugriffs auf alle internen und externen Schnittstellen des IoT-Produkts trägt dazu bei, die Vertraulichkeit, Integrität und Verfügbarkeit des IoT-Produkts, seiner Komponenten und Daten zu bewahren, indem unbefugter Zugriff und Änderungen verhindert werden.

Softwareupdate

Die Software[13] aller IoT-Produktkomponenten kann von autorisierten Personen, Diensten und anderen IoT-Produktkomponenten nur unter Verwendung eines sicheren und konfigurierbaren Mechanismus aktualisiert werden, der für jede IoT-Produktkomponente geeignet ist.

1. Jede IoT-Produktkomponente kann verifizierte Software-Updates empfangen, verifizieren und anwenden.
2. Das IoT-Produkt ergreift Maßnahmen, um die Software auf den Komponenten des IoT-Produkts auf dem neuesten Stand zu halten (d. h. automatische Anwendung von Updates oder konsequente Benachrichtigung des Kunden über verfügbare Updates über das IoT-Produkt).

Cybersecurity-Dienstprogramm: Software kann Schwachstellen aufweisen, die erst nach der Bereitstellung des IoT-Produkts entdeckt werden; Software-Aktualisierungsfunktionen können die sichere Bereitstellung von Sicherheits-Patches gewährleisten.

[13] Dazu gehören sowohl ausführbarer Code als auch Softwarebibliotheken, Support Packs und andere nicht ausführbare Softwaredaten.

Sensibilisierung für den Zustand der Cybersicherheit

Das IoT-Produkt unterstützt die Erkennung von Cybersicherheitsvorfällen, die IoT-Produktkomponenten und die von ihnen gespeicherten und übertragenen Daten betreffen oder beeinträchtigen.

1. Das IoT-Produkt erfasst und speichert sicher Informationen über den Zustand der IoT-Komponenten[14], die zur Erkennung von Cybersicherheitsvorfällen verwendet werden können, die IoT-Produktkomponenten und die von ihnen gespeicherten und übertragenen Daten betreffen oder beeinträchtigen.

Cybersecurity-Dienstprogramm: Der Schutz von Daten und die Sicherstellung der ordnungsgemäßen Funktionalität können durch die Fähigkeit unterstützt werden, den Kunden zu warnen, wenn das Gerät auf unerwartete Weise zu arbeiten beginnt, was bedeuten könnte, dass ein unbefugter Zugriff versucht wird, Malware geladen wurde, Botnets erstellt wurden, Geräte-Softwarefehler aufgetreten oder andere Arten von Aktionen aufgetreten sind, die nicht vom Benutzer des IoT-Produkts initiiert wurden oder vom Entwickler beabsichtigt waren.

[14] Informationen über den Zustand von IoT-Komponenten, die für die Erkennung von Cybersicherheitsvorfällen nützlich sind, stehen in engem Zusammenhang mit dem IoT-Produkt, seinen Komponenten und seinem Betrieb. In den meisten Fällen sollten zeitliche Informationen wie Zeitstempel oder Standortdaten (digital oder physisch) erfasst werden. Software- und Hardwareversionen und Betriebszustände (z. B. bekannte Fehler oder Ausnahmen) können dazu beitragen, Schwachstellen in der Cybersicherheit zu erkennen (z. B. können bestimmte Software oder Hardware bekannte Schwachstellen aufweisen). Cybersecurity-Statusinformationen können auch Aufzeichnungen von Befehlen und Aktionen enthalten, die das IoT-Produkt empfangen und ausgeführt hat, oder andere Daten, die für das IoT-Produkt und seine Funktionsweise von Bedeutung sind und daher für die Erkennung von Vorfällen nützlich sind.

2.2.2. Nicht-technische Unterstützungsfähigkeiten für IoT-Produkte

Dokumentation

Der IoT-Produktentwickler erstellt, sammelt und speichert[15] vor dem Kauf durch den Kunden sowie während der gesamten Entwicklung eines Produkts und seines späteren Lebenszyklus Informationen, die für die Cybersicherheit des IoT-Produkts und seiner Komponenten relevant sind.

1. Während des gesamten Entwicklungszyklus erstellt oder sammelt und speichert der IoT-Produktentwickler Informationen, die für die Cybersicherheit des IoT-Produkts und seiner Produktkomponenten relevant sind, **einschließlich**:
    a. Annahmen, die während des Entwicklungsprozesses gemacht wurden, und andere Erwartungen im Zusammenhang mit dem IoT-Produkt, **einschließlich**:
        i. erwartete Kunden und Anwendungsfälle.
        ii. physische Nutzung und Eigenschaften, einschließlich der Sicherheit des Standorts des IoT-Produkts und seiner Produktkomponenten (z. B. eine Kamera für die Verwendung innerhalb des Hauses, die über einen Aus-Schalter am Gerät verfügt, im Gegensatz zu einer Sicherheitskamera für die Verwendung außerhalb des Hauses, die keinen Aus-Schalter am Gerät hat).
        iii. Netzzugang und Anforderungen (z. B. Bandbreitenanforderungen).
        iv. Daten, die von dem IoT-Produkt erzeugt und verarbeitet werden.
        v. alle erwarteten Dateneingaben und -ausgaben (einschließlich Fehlercodes, Häufigkeit, Art/Form, Bereich der akzeptablen Werte usw.).
        vi. die vom IoT-Produktentwickler angenommenen Cybersicherheitsanforderungen für das IoT-Produkt.
        vii. alle Gesetze und Vorschriften, denen das IoT-Produkt und die damit verbundenen Support-Aktivitäten entsprechen.
        viii. erwartete Lebensdauer und voraussichtliche Cybersicherheitskosten im Zusammenhang mit dem IoT-Produkt (z. B. Preis für die Wartung) sowie Dauer und Bedingungen des Supports.
    b. aller IoT-Komponenten, einschließlich, aber nicht beschränkt auf das IoT-Gerät, die Teil des IoT-Produkts sind.
    c. wie die Kriterien des Basisprodukts durch das IoT-Produkt und seine

[15] Die in diesem Kriterium behandelte Dokumentation wird vom IoT-Produktentwickler gepflegt und kontrolliert. Die Weitergabe dieser Informationen kann angemessen sein und sich auf autorisierte Techniker und Cybersicherheitsexperten beschränken, die weitere Informationen über das IoT-Produkt suchen (z. B. bei der Bewertung des IoT-Produkts im Hinblick auf die Kennzeichnung oder bei der Untersuchung einer Sicherheitsverletzung), aber die dokumentierten Informationen sollen nicht in allen Fällen direkt an die Verbraucher weitergegeben werden.

Produktkomponenten erfüllt werden, einschließlich der Kriterien des Basisprodukts, die von den IoT-Produktkomponenten nicht erfüllt werden, und warum (z. B. weil die Fähigkeit aufgrund der Risikobewertung nicht benötigt wird).

d. Überlegungen zum Produktdesign und zum Support für das IoT-Produkt, *zum Beispiel*:
    i. alle Hardware- und Softwarekomponenten aus allen Quellen (z. B. Open Source, proprietäre Drittanbieter, intern entwickelt), die zur Herstellung des IoT-Produkts verwendet werden (d. h. zur Herstellung jeder Produktkomponente).
    ii. die IoT-Plattform, die bei der Entwicklung und dem Betrieb des IoT-Produkts verwendet wird, ihre Produktkomponenten, einschließlich der zugehörigen Dokumentation.
    iii. Vertrauenswürdigkeit und Schutz von Software- und Hardwareelementen, die zur Erstellung des IoT-Produkts und seiner Produktkomponenten implementiert wurden (z. B. sicheres Booten, Hardware-Root of Trust und sichere Enklave).
    iv. Berücksichtigung der bekannten Risiken im Zusammenhang mit dem IoT-Produkt und des bekannten potenziellen Missbrauchs.
    v. sichere Softwareentwicklung und angewandte Praktiken in der Lieferkette.
    vi. Akkreditierungs-, Zertifizierungs- und/oder Bewertungsergebnisse für Verfahren im Bereich der Cybersicherheit.
    vii. die einfache Installation und Wartung des IoT-Produkts durch einen Kunden (d. h. die Benutzerfreundlichkeit des Produkts [ISO9241]).
e. Wartungsanforderungen für das IoT-Produkt, *zum Beispiel*:
    i. Erwartungen an die Cybersecurity-Wartung und zugehörige Anweisungen oder Verfahren (z. B. Schwachstellen-/Patch-Management-Plan).
    ii. wie der IoT-Produktentwickler autorisierte unterstützende Parteien identifiziert, die Wartungsaktivitäten durchführen können (z. B. autorisierte Reparaturzentren).
    iii. Überlegungen zur Cybersicherheit des Instandhaltungsprozesses (z. B. wie Kundendaten, die nicht mit dem Instandhaltungsprozess in Verbindung stehen, auch gegenüber den Instandhaltern vertraulich bleiben).
f. die mit dem IoT-Produkt verbundenen Richtlinien und Prozesse für einen sicheren Systemlebenszyklus, **einschließlich:**
    i. Schritte, die während der Entwicklung unternommen werden, um sicherzustellen, dass das IoT-Produkt und seine Produktkomponenten frei von bekannten, ausnutzbaren Schwachstellen sind.

ii. der Prozess der Zusammenarbeit mit Komponentenlieferanten und Drittanbietern, um sicherzustellen, dass die Sicherheit des IoT-Produkts und seiner Produktkomponenten für die Dauer des unterstützten Lebenszyklus aufrechterhalten wird.
iii. Überlegungen für die Zeit nach Beendigung des Supports, z. B. die Entdeckung einer Schwachstelle, die erhebliche Auswirkungen auf die Sicherheit, den Datenschutz oder die Sicherheit der Kunden hätte, die das IoT-Produkt und seine Produktkomponenten weiterhin nutzen.

g. die mit dem IoT-Produkt verbundenen Richtlinien und Prozesse für das Schwachstellenmanagement, **einschließlich**:
   i. Methoden zur Entgegennahme von Meldungen über Schwachstellen (siehe Informations- und Abfrageempfang unten).
   ii. Verfahren zur Erfassung gemeldeter Schwachstellen.
   iii. einer Richtlinie zur Reaktion auf gemeldete Schwachstellen, einschließlich des Verfahrens zur Koordinierung der Maßnahmen zur Behebung von Schwachstellen zwischen Komponentenlieferanten und Drittanbietern.
   iv. einer Richtlinie zur Offenlegung gemeldeter Schwachstellen.
   v. Verfahren zum Erhalt von Benachrichtigungen von Komponentenlieferanten und Drittanbietern über Änderungen des Status der von ihnen gelieferten Komponenten, z. B. Produktionsende, Ende des Supports, veralteter Status (z. B. das Produkt wird nicht mehr zur Verwendung empfohlen) oder bekannte Sicherheitslücken.

Cybersecurity-Dienstprogramm: Das Generieren, Erfassen und Speichern wichtiger Informationen über das IoT-Produkt und seine Entwicklung (z. B. Bewertung des IoT-Produkts und der bei seiner Erstellung und Wartung angewandten Entwicklungspraktiken) kann den IoT-Produktentwickler über die tatsächliche Cybersicherheitslage des Produkts informieren.

Empfang von Informationen und Rückfragen

Der IoT-Produktentwickler ist in der Lage, für die Cybersicherheit relevante Informationen zu erhalten und auf Anfragen des Kunden und anderer Personen zu Informationen, die relevant für die Cybersicherheit sind, zu antworten.

1. Der IoT-Produktentwickler kann Informationen über die Cybersicherheit des IoT-Produkts und seiner Produktkomponenten erhalten und auf Anfragen von Kunden und anderen Personen zur Cybersicherheit des IoT-Produkts und seiner Produktkomponenten antworten, **einschließlich:**
    a. der Fähigkeit des IoT-Produktentwicklers, eine Kontaktstelle zu bestimmen, die Informationen über Wartung und Schwachstellen (z. B. Fehlerberichtsfunktionen und Bug Bounty-Programme) von Kunden und anderen Mitgliedern des IoT-Produkt-Ecosystems (z. B. Reparaturtechniker im Auftrag des Kunden) erhält.
    b. der Fähigkeit des IoT-Produktentwicklers, Anfragen von Kunden und anderen Mitgliedern des IoT-Produkt-Ecosystems zur Cybersicherheit des IoT-Produkts und/oder seiner Komponenten zu erhalten und zu beantworten.

Cybersecurity-Dienstprogramm: Wenn IoT-Produkte von Kunden genutzt werden, haben diese Kunden möglicherweise Fragen oder berichten über Probleme, die dazu beitragen können, die Cybersicherheit des IoT-Produkts im Laufe der Zeit zu verbessern.

Verbreitung von Informationen

Der Entwickler des IoT-Produkts verbreitet (z. B. an die Öffentlichkeit) und verteilt (z. B. an den Kunden oder andere Mitglieder des IoT-Produkt-Ecosystems) Informationen, die für die Cybersicherheit relevant sind.

1. Der Entwickler des IoT-Produkts kann über einen Kanal (z. B. einen Beitrag in einem öffentlichen Kanal, E-Mails an die registrierten Adressen aller betroffenen Kunden) viele/alle Stellen informieren, um die Öffentlichkeit und die Kunden des IoT-Produkts über sicherheitsrelevante Informationen und Ereignisse während des Support-Lebenszyklus zu informieren. **Diese Informationen müssen mindestens Folgendes umfassen**:
    a. aktualisierte Support-Bedingungen (z. B. Häufigkeit der Aktualisierungen und Mechanismen der Anwendung) und Ankündigung der Verfügbarkeit und/oder Anwendung von Software-Updates.
    b. Ende der Laufzeit des Supports oder der Funktionalität für das IoT-Produkt.
    c. notwendige Wartungsarbeiten.
    d. neue Schwachstellen in IoT-Geräten, zugehörige Details und erforderliche Abhilfemaßnahmen seitens des Kunden.
    e. Entdeckung von Sicherheitsverletzungen im Zusammenhang mit einem IoT-Produkt und seinen Produktkomponenten, die von den Kunden verwendet werden, sowie die damit verbundenen Details und die vom Kunden erforderlichen Abhilfemaßnahmen (falls vorhanden).
2. Der Entwickler des IoT-Produkts kann für die Cybersicherheit des IoT-Produkts und seiner Produktkomponenten relevante Informationen verbreiten, um geeignete Stellen des Ecosystems (z. B. Hersteller von IoT-Produktkomponenten und/oder unterstützende Stellen, gemeinsame Stellen für die Verfolgung von Schwachstellen, Akkreditierungs- und Zertifizierungsstellen, dritte Support- und Wartungsorganisationen) über cybersicherheitsrelevante Informationen zu informieren, *zum Beispiel*.:
    a. anwendbare Dokumentation, die während des Entwurfs und der Entwicklung des IoT-Produkts und seiner Produktkomponenten erfasst wurde.[16]
    b. Warnungen zur Cybersicherheit und zu Sicherheitslücken sowie Informationen zur Behebung von Sicherheitslücken.
    c. ein Überblick über die vom IoT-Produktentwickler angewandten Verfahren und Schutzmaßnahmen für die Informationssicherheit.

[16] Dieses Unterkriterium soll darauf hinweisen, dass die im Rahmen der Dokumentationsfähigkeit erfassten Informationen möglicherweise an bestimmte Stellen weitergegeben werden müssen (z. B. an Hersteller von IoT-Produktkomponenten und/oder unterstützende Stellen, gemeinsame Behörden für die Verfolgung von Schwachstellen, Akkreditierungs- und Zertifizierungsstellen, externe Support- und Wartungsorganisationen). In den meisten Fällen wird diese Art von Dokumentation nur an interessierte Parteien weitergegeben, die einen bestimmten Zweck mit den Informationen verfolgen (z. B. Konformitätsbewertung), und nicht an die Öffentlichkeit oder gar an Kunden im Verbrauchersektor.

d. Akkreditierungs-, Zertifizierungs- und/oder Bewertungsergebnisse für die Cybersicherheitspraktiken des IoT-Produktentwicklers.
e. ein Risikobewertungsbericht oder eine Zusammenfassung für die Risikolage im Geschäftsumfeld des IoT-Produktentwicklers.

Cybersecurity-Dienstprogramm: Da sich das IoT-Produkt, seine Komponenten, Bedrohungen und Abhilfemaßnahmen ändern, müssen die Kunden darüber informiert werden, wie sie das IoT-Produkt sicher nutzen können.

Produktaufklärung und Sensibilisierung

Der IoT-Produktentwickler sensibilisiert und informiert Kunden und andere Personen im IoT-Produkt-Ecosystem über cybersicherheitsrelevante Informationen (z. B. Überlegungen, Funktionen) in Bezug auf das IoT-Produkt und seine Produktkomponenten.[17]

1. Der Entwickler des IoT-Produkts schafft ein Bewusstsein für die Cybersicherheit des IoT-Produkts und seiner Produktkomponenten und klärt die Kunden darüber auf, welche Informationen für die Cybersicherheit relevant sind, **einschließlich**:
    a. Das Vorhandensein und die Nutzung von Cybersicherheitsfunktionen für IoT-Produkte, die **mindestens Folgendes umfassen**:
        i. wie man Konfigurationseinstellungen ändern kann und welche Auswirkungen die Änderung der Einstellungen auf die Cybersicherheit hat.
        ii. wie man Zugangskontrollfunktionen konfigurieren und verwenden kann (z. B. Festlegen und Ändern von Passwörtern).
        iii. wie Softwareupdates vorgenommen werden und welche Anweisungen für den Kunden erforderlich sind, um die Softwareupdate-Funktion zu nutzen.
        iv. wie man Gerätedaten verwaltet, einschließlich der Erstellung, Aktualisierung und Löschung von Daten auf dem IoT-Produkt.
    b. wie das IoT-Produkt und seine Produktkomponenten während seiner Lebensdauer gewartet wird, auch nach Ablauf der Sicherheitsunterstützung (z. B. Lieferung von Software-Updates und Patches) durch den IoT-Produktentwickler.
    c. wie ein IoT-Produkt und seine Produktkomponenten sicher neu bereitgestellt oder entsorgt werden können.
    d. Optionen für das Schwachstellenmanagement (z. B. Konfigurations- und Patch-Management und Anti-Malware), die für das IoT-Produkt oder seine Produktkomponenten verfügbar sind und von den Kunden genutzt werden könnten.
    e. zusätzliche Informationen, die Kunden nutzen können, um fundierte Kaufentscheidungen über die Sicherheit des IoT-Produkts zu treffen (z. B. Dauer und Umfang der Produktunterstützung durch Software-Upgrades und Patches).

[17] Die Informationen und das Fachwissen für die Entwicklung einer wirksamen Aufklärung und Sensibilisierung in Bezug auf ein IoT-Produkt können bei den Entwicklern oder Herstellern von IoT-Produktkomponenten vorhanden sein. Es wird empfohlen, bereits vor der Einführung eines IoT-Produkts ein Bildungs- und Sensibilisierungssystem einzurichten, das Informationen über die IoT-Cybersicherheit teilt, da dies bei der Umsetzung dieser und anderer Cybersicherheitsfunktionen hilfreich sein wird.

Cybersecurity-Dienstprogramm: Die Kunden müssen darüber informiert werden, wie sie das Gerät sicher nutzen können, um die besten Ergebnisse in Bezug auf die Cybersicherheit für die Kunden und den Markt für IoT-Verbraucherprodukte zu erzielen.

3. Überlegungen zum Verbrauchersektor bei der Erstellung des Profils

Das NIST nutzte die Konzepte der Profilierung der IoT-Geräte-Cybersicherheitsfähigkeit-Referenzgrundlage, um das Verbraucherprofil zu entwickeln. Der erste Schritt bestand darin, Quellen und andere Informationen über die Cybersicherheit von IoT-Produkten zu sammeln. Anschließend erstellte das NIST anhand dieser Informationen ein Verbraucherprofil, das auf den Quellen, Informationen und den daraus resultierenden Erkenntnissen beruht.

3.1. Sammeln von Quelleninformationen über die Cybersicherheit von IoT-Produkten für Verbraucher

Das Verbraucherprofil entstand als Reaktion des NIST auf die EO 14028, die das NIST anwies, Empfehlungen für ein Programm zur Kennzeichnung der Cybersicherheit von IoT-Produkten zu entwickeln. Die Empfehlungen waren umfassender als die Entwicklung eines Verbraucherprofils für die IoT-Referenzgrundlage, aber das Profil war ein Schlüsselelement dieser Aufgabe. Daher konnte das NIST Quellen sammeln und mit externen Stakeholdern über die Bedürfnisse und Ziele der Kunden von IoT-Produkten diskutieren. Im Laufe eines Jahres mit Veranstaltungen, Treffen und anderen Aktivitäten wurden Hunderte von Kommentaren zur Kennzeichnung der Cybersicherheit von IoT-Produkten für Verbraucher gesammelt, von denen viele in die Erstellung der grundlegenden Basisdaten für diesen Sektor eingeflossen sind.

Das NIST untersuchte auch öffentlich zugängliche Quellen, um Schwachstellen zu identifizieren, die auf den Bereich der IoT-Produkte für Verbraucher zutreffen. Diese Informationen sind wichtig, um einen Querschnitt der Schwachstellen von IoT-Produkten für Verbraucher zu ermitteln, der als Grundlage für die Bestimmung von Bedrohungen und Schwachstellen dienen kann. Diese Bedrohungen und Schwachstellen fließen in die Profilerstellung ein, insbesondere in Aspekte der minimalen Sicherheit. Tabelle 1, entnommen aus dem *Consumer Cybersecurity Labeling for IoT Products: Discussion Draft on the Path Forward* Whitepaper [Path_Forward] listet eine Reihe von anwendbaren, gut dokumentierten Schwachstellen, die zugehörigen Angriffskategorien des MITRE ATT&CK Framework [ATT_CK] und die profilierten Fähigkeiten auf, die zur Behebung der Schwachstelle beitragen können.[18]

Tabelle 1. Beispiel für IoT-Schwachstellen bei Verbrauchern und die entsprechenden Fähigkeiten aus dem Verbraucherprofil.

Schwachstelle	Relevante Verbraucherprofil-Fähigkeiten
Mirai-Malware-Varianten-Angriffe – Nutzung einer schwachen Authentifizierung, um das Laden von Malware auf das Gerät zu ermöglichen und dieses Gerät für DDOS- und andere Angriffe zu nutzen.	

[18] Die genannten Fähigkeiten sind nicht erschöpfend, sondern sollen zeigen, dass die im Verbraucherprofil genannten Fähigkeiten zur Unterstützung der Cybersicherheit dazu beitragen können, die festgestellten Schwachstellen zu verringern oder zu verhindern. So hätte beispielsweise eine Schnittstellenzugriffskontrolle den unbefugten Zugriff auf ein IoT-Gerät verhindern können.

Schwachstelle	Relevante Verbraucherprofil-Fähigkeiten
Unbefugter Zugriff auf das IoT-Gerät	Identifizierung von Assets Schnittstellenzugangskontrolle Verbreitung von Informationen Aufklärung und Sensibilisierung
Bösartiger Code kann auf das IoT-Gerät geladen werden	Softwareupdate Sensibilisierung für den Zustand der Cybersicherheit Aufklärung und Sensibilisierung
Befehle können über das Gerät gestartet werden	Schnittstellenzugangskontrolle Dokumentation
Unerlaubte Veröffentlichung von Fitness-Tracker-Daten – Die Standortdaten des Fitness-Trackers für Militärangehörige wurden öffentlich bekannt gegeben, obwohl das Produkt auf Datenschutz eingestellt war.	
Schwachstellen von Webanwendungen	Produktkonfiguration Sensibilisierung für den Zustand der Cybersicherheit Dokumentation Verbreitung von Informationen
Schwachstellen in mobilen Anwendungen	Produkt-Konfiguration Sensibilisierung für den Zustand der Cybersicherheit Dokumentation Verbreitung von Informationen
Möglichkeit der Re-Identifizierung de-identifizierter Daten	Produkt-Konfiguration Datenschutz Dokumentation
Unbefugter Zugriff auf die Daten von Überwachungskameras – Unbefugter Zugriff auf Daten und Ansichten des Inneren und Äußeren von Gebäuden trat bei Sicherheitskameras verschiedener Marken auf.	
Schwache Authentifizierung	Schnittstellenzugangskontrolle

Schwachstelle	Relevante Verbraucherprofil-Fähigkeiten
Unbefugter Datenaustausch	Datenschutz Dokumentation Verbreitung von Informationen
Nichtbeantwortung von Fragen und Beschwerden an die Entwickler	Empfangen von Informationen und Anfragen
Mangel an Überwachungsmöglichkeiten und -verfahren	Identifizierung von Assets Produkt-Konfiguration Dokumentation
Fehlende Kontrollen bei der Datenaufzeichnung/-erfassung	Identifizierung von Assets Produkt-Konfiguration Dokumentation Verbreitung von Informationen Aufklärung und Sensibilisierung

Das NIST untersuchte auch das bestehende Normen-, Konformitäts- und Kennzeichnungs-Ecosystem für IoT-Geräte und -Produkte, um zu verstehen, wo andere IoT-Produkterwägungen für Verbraucher berücksichtigt wurden. Es wurden etwa 30 Quellendokumente geprüft, darunter IoT-Cybersicherheitsgesetze, Kataloge von Cybersicherheitsfähigkeiten, Grundfähigkeiten und Einstufungssysteme.[19] Alle befassten sich speziell mit dem IoT-Gerät selbst, aber einige bezogen auch die Cloud, die mobile App, den Hub oder andere externe Komponenten in ihre Überlegungen als Teil eines IoT-Produkts ein. In den öffentlichen Kommentaren und Diskussionen mit den Interessenvertretern wurde die breitere Sichtweise (d. h. IoT-Produkt vs. IoT-Gerät) unterstützt, da das NIST einen großen Konsens über die Notwendigkeit feststellte, alle Komponenten eines IoT-Produkts in den Geltungsbereich eines etablierten Satzes von Cybersicherheitsfähigkeiten aufzunehmen.

3.2. Bewertung der Quellen für die Cybersicherheit von IoT-Produkten für Verbraucher

Die Quelldokumente lassen sich am ehesten mit den technischen und nichttechnischen Unterstützungsfähigkeiten vergleichen, die in den NISTIRs 8259A und 8259B festgelegt sind. Von den 30 gesammelten Quellendokumenten hatten 8 einen direkten Bezug zu IoT-Produkten für Verbraucher. Diese Unterstichprobe wurde mit den in NISTIR 8259A/B beschriebenen Fähigkeiten verglichen. Dabei zeigte sich eine weitgehende Übereinstimmung mit den

[19] Die EO 14028 wies das NIST an, Stufen für die IoT-Kennzeichnungsempfehlungen für Verbraucher in Betracht zu ziehen, aber die NIST-Forschung und das anschließende Feedback ergaben keinen klaren und effektiven Satz oder Rahmen für die Entwicklung von Stufen. In den vorhandenen Quellen, die sich mit den Ebenen befassen, wurde kein einheitlicher Standpunkt vertreten. Darüber hinaus erhielt das NIST die Rückmeldung, dass die Stufen das zunehmende Risiko von IoT-Produkten für Verbraucher widerspiegeln sollten, aber die Vielfalt der IoT-Anwendungsfälle für Verbraucher macht es erforderlich, diese Anwendungsfälle auf der Grundlage des Risikos zu gruppieren, was innerhalb des einjährigen Zeitrahmens für die Reaktion auf EO 14028 nicht möglich war.

technischen Fähigkeiten, wenngleich einige gemeinsame technische Fähigkeiten, die nicht in NISTIR 8259A zu finden sind, zur Anpassung der Kerngrundlagen für das Verbraucherprofil verwendet wurden. Es gibt jedoch nur wenige Quellendokumente, die sich mit den nichttechnischen Fähigkeiten befassen, die auf der Grundlage von NISTIR 8259B entwickelt wurden. Da die erwarteten Nutzer von Verbraucher-IoT-Geräten in der Regel keine Experten für Cybersicherheit sind, sind diese nichttechnischen Unterstützungsfunktionen für einen sicheren Betrieb unerlässlich.

Dies wurde durch öffentliche Kommentare und mündliche Rückmeldungen während der Arbeit an der EO-Antwort bestätigt, die dem NIST als weitere Informationsquelle für das Verbraucherprofil dienten. Aus diesen Quellen erfuhr das NIST auch, dass sich der Verbrauchersektor von der allgemeinen Situation oder anderen Sektoren unterscheiden kann. So ist zum Beispiel das Cybersecurity-Risikomanagement von Unternehmenskunden in der Regel strukturierter und formalisierter als das von Kunden im Verbrauchersektor verwendete Cybersecurity-Risikomanagement. Außerdem haben Unternehmen in der Regel einen besseren Zugang zu Fachwissen im Bereich der Cybersicherheit als normale Verbraucher. Diese Unterschiede und andere Erkenntnisse haben Auswirkungen auf die Art und Weise, wie Cybersicherheitskapazitäten angegangen und bereitgestellt werden müssen. Tabelle 2 zeigt die wichtigsten Erkenntnisse, die bei der Entwicklung des IoT-Profils für Verbraucher verwendet wurden.

Tabelle 2. Hervorgehobene Einblicke und wichtige Erkenntnisse aus dem Consumer IoT Profiling Prozess.

Hervorgehobene Einblicke	Wichtige Erkenntnisse
Die Erkenntnisse über die Cybersicherheit im Verbrauchersektor auf der Grundlage von Risiken und Schwachstellen sind ähnlich wie die des allgemeinen Referenzgrundlagenfalles (z. B. die in Tabelle 1 aufgeführten).	Die meisten Fähigkeiten haben ähnliche Cybersicherheitskonzepte wie die Referenzgrundlage
Cybersicherheitsrichtlinien auf Geräteebene wären angesichts der Bedürfnisse und Ziele der Kunden in diesem Bereich unzureichend, unter anderem, weil sie nicht zwischen IoT-Geräten und unterstützenden Komponenten unterscheiden.	Produkt ist die bevorzugte Stufe für IoT-Cybersicherheitsrichtlinien für Verbraucher.
Datenschutz und Sicherheit sind neben der Cybersicherheit die wichtigsten Anliegen für IoT-Produkte für Verbraucher.	Cybersicherheitsfähigkeiten müssen so konzipiert sein, dass sie keine Risiken in diesen Bereichen schaffen und allgemeine Ansätze zur Minderung von Datenschutz- und Sicherheitsrisiken unterstützen.

Hervorgehobene Einblicke	Wichtige Erkenntnisse
Es gibt keine eindeutigen, allgemeingültigen Bedürfnisse und Ziele der Verbraucher in Bezug auf die Cybersicherheit im Verbrauchersektor, und das NIST hat in den Quellendokumenten, die in die Überprüfung der Landschaft einbezogen wurden, mehrere Ansätze zur Berücksichtigung der Kundenbedürfnisse und -ziele identifiziert.	Die Fähigkeiten sollten auf allgemein anerkannten und allgemein anwendbaren Cybersicherheitsfunktionen beruhen.
Die Bedürfnisse und Ziele der Kunden in diesem Sektor werden unterschiedlich sein. Die Kunden verfügen möglicherweise nur über begrenzte Kenntnisse und Fähigkeiten in Bezug auf IoT/IT-Technologien und Cybersicherheitsfunktionen.	Menschliche Faktoren im Zusammenhang mit Cybersicherheitskapazitäten sind für die Minderung von Cybersicherheitsrisiken von größter Bedeutung.

Diese Erkenntnisse und die daraus resultierenden Schlussfolgerungen führen das NIST zu den folgenden Überlegungen bezüglich eines IoT-Profils für Verbraucher:

1. Es wurde deutlich, dass viele IoT-Geräte von Verbrauchern durch zusätzliche Komponenten unterstützt werden, wie z. B. ein Backend und/oder eine mobile App, die für die Nutzung des IoT-Geräts so wichtig sind, dass das Gerät ohne diese Komponenten nicht sinnvoll genutzt werden kann.
2. Außerdem haben die Verbraucher zu Hause oft wenig Kontrolle über diese zusätzlichen Komponenten. Wenn man also darüber nachdenkt, wie sich die Gerätezentrierung auf den Verbrauchersektor auswirkt, sollte das Konzept über das Gerät hinausgehen und das gesamte Produkt einbeziehen. Dieser Bereich kann zusätzliche Komponenten als Teil eines IoT-Produkts umfassen, einschließlich solcher, mit denen der Verbraucher nur indirekt interagiert (z. B. Backend).
3. Das Verbraucherprofil muss im Kontext der wichtigsten Wahrnehmungen und Überlegungen zum Schutz der Privatsphäre und zur Sicherheit in der Branche umgesetzt werden. Sicherheits- und Datenschutzüberlegungen sind bei IoT-Produkten für Verbraucher jedoch dynamisch, da selbst in diesem speziellen Sektor die Anwendungsfälle für IoT-Produkte sehr unterschiedlich sein können. Ein Produkt und seine Funktionsweise können eindeutige Auswirkungen auf die Sicherheit haben, aber das ist nicht immer der Fall. Das Gleiche gilt für die Privatsphäre. Erschwerend kommt hinzu, dass verschiedene Anwendungsfälle zwar allgemeine Überlegungen zur Sicherheit und/oder zum Schutz der Privatsphäre enthalten können, die konkreten Auswirkungen und/oder Abhilfemaßnahmen jedoch sehr unterschiedlich sein können. Dies alles bedeutet, dass die Cybersicherheitsfunktionen des Verbraucherprofils eine Vielzahl von Anwendungsfällen unterstützen müssen, wobei darauf zu achten ist, dass sie diese Bereiche nicht behindern.

4. Die Cybersicherheitspraktiken der Kunden (d. h. der privaten Verbraucher), die Verbraucher-IoT-Produkte verwalten, sind unterschiedlich definiert und ausgereift. Die Unvorhersehbarkeit und der Ad-hoc-Charakter der Risikominderung für Verbraucher-IoT-Produkte machen deutlich, dass sich in dem Profil allgemein nützliche und allgemein empfohlene Cybersicherheitspraktiken widerspiegeln müssen.
5. Darüber hinaus besteht in diesem Sektor ein wichtiger Bedarf an nutzbaren Cybersicherheitsfunktionen, die so implementiert sind, dass sie nur eine minimale/effiziente Einrichtung und Interaktion mit dem Kunden erfordern, da diese Kunden nicht über umfassende Kenntnisse oder Ressourcen verfügen, die sie nutzen können, wenn die Funktionen für sie nicht nutzbar sind.
6. Schließlich sollten je nach Funktionalität und Anwendungsfall eines IoT-Produkts spezifische Standards, Lösungen, Implementierungen oder Abhilfemaßnahmen verwendet werden. Das bedeutet, dass es keinen einzigen Satz spezifischer Anforderungen gibt, der auf alle IoT-Produkte für Verbraucher anwendbar ist. Daher beschreibt das Verbraucherprofil die Cybersicherheitsrichtlinien für IoT-Produkte im Hinblick auf die Ergebnisse, die mit dem Produkt als Ganzes erreicht und unterstützt werden sollen, es gilt aber möglicherweise nicht für alle IoT-Produktkomponenten in gleicher Weise. Einige Komponenten können oder müssen nicht alle Kriterien erfüllen.[20] Diese Ergebnisse bieten Anhaltspunkte für eine Vielzahl von Technologien und Anwendungsfällen, ermöglichen jedoch eine flexible Anwendung des Verbraucherprofils auf bestimmte IoT-Produkte.[21]

NIST wandte diese Überlegungen auf die NISTIRs 8259A/B Fähigkeiten der Referenzgrundlage an, um den allgemeinen IoT-Ansatz für den Verbrauchersektor anzupassen. Das daraus resultierende Verbraucherprofil ist zwar direkter auf den Sektor zugeschnitten, soll aber dennoch eine breite Palette von IoT-Technologien, Anwendungsfällen und Risikominderungsüberlegungen abdecken. Daher kann die Anwendung des Verbraucherprofils auf ein bestimmtes Produkt, einen Produkttyp oder eine IoT-Produktkomponente zusätzliche, aber ähnliche Anpassungen durch die Erfassung und Berücksichtigung von Informationen, wie in diesem Abschnitt beschrieben, erfordern.

[20] Wie in den in *Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products* erörtert, gelten nicht alle Fähigkeiten oder Unterkriterien für alle IoT-Produktkomponenten oder werden von diesen in gleicher Weise unterstützt. Dies könnte auf Produktrisikoerwägungen, die Produktentwicklung (z. B. über Verträge und die Lieferkette delegierte Cybersicherheitsaufgaben), die Art der Komponenten, aus denen das Produkt besteht (z. B. können Backends hochgradig verteilt sein), oder Beschränkungen der IoT-Komponenten (z. B. können Geräte eingeschränkt sein, begleitende Software-Apps können begrenzten Zugang und Funktionalität haben) zurückzuführen sein. Die Berücksichtigung dieses Aspekts bei der Anwendung der Fähigkeiten und Unterkriterien auf reale Produkte (z. B. über einen Konformitätsbewertungsmechanismus) ist von entscheidender Bedeutung für einen robusten Cybersicherheitsmarkt und ein Ecosystem, das unterschiedlichen Bedürfnissen und Kontexten gerecht werden kann.

[21] NIST bittet diejenigen, die über Anleitungen, Standards oder Programme verfügen, die ihrer Meinung nach einige oder alle in diesem Profil widergespiegelten Ergebnisse unterstützen oder sich anderweitig darauf beziehen, sich im NIST Online Informative Reference (OLIR) Catalog darüber zu informieren, wie sie öffentliche Zuordnungen zwischen ihrer Arbeit und dem Verbraucherprofil einreichen können.

Referenzen

[ATT_CK] The MITRE Corporation (2013) Adversarial Tactics, Techniques, and Common Knowledge. (The MITRE Corporation, Bedford, MA). https://attack.mitre.org/

[EO_Criteria] National Institute of Standards and Technology (2022) Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper. https://doi.org/10.6028/NIST.CSWP.24

[IR8259] Fagan M, Megas KN, Scarfone K, Smith M (2020) Foundational Cybersecurity Activities for IoT Device Manufacturers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8259. https://doi.org/10.6028/NIST.IR.8259

[IR8259A] Fagan M, Megas KN, Scarfone K, Smith M (2020) IoT Device Cybersecurity Capability Core Baseline. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8259A. https://doi.org/10.6028/NIST.IR.8259A

[IR8259B] Fagan M, Marron J, Brady KG, Jr, Cuthill BB, Megas KN, Herold R (2020) IoT Non-Technical Supporting Capability Core Baseline. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8259B. https://doi.org/10.6028/NIST.IR.8259B

[ISO9241] International Organization for Standardization/International Electrotechnical Commission (2018) ISO 9241-11:2018 Ergonomie der Mensch-System-Interaktion – Part 11: Benutzerfreundlichkeit: Definitionen und Konzepte (ISO Genf, Schweiz). Erhältlich unter https://www.iso.org/standard/63500.html

[Pfad_Forward] National Institute of Standards and Technology (2021) Consumer Cybersecurity Labeling for IoT Products: Discussion Draft on the Path Forward. (National Institute of Standards and Technology, Gaithersburg, MD). Erhältlich unter: https://www.nist.gov/document/draft-paper-consumer-cybersecurity-labeling-iot-products-discussion-draft-path-forward

Appendix A. Glossar

Verbraucher-IoT-Produkt
IoT-Produkte, die für den persönlichen Gebrauch, die Familie oder den Haushalt bestimmt sind.

Referenzgrundlage
Eine Reihe von Cybersicherheitsfähigkeiten für Geräte und nichttechnische unterstützende Fähigkeiten, die zur Unterstützung gemeinsamer Cybersicherheitskontrollen benötigt werden, die die Geräte und Gerätedaten, Systeme und Ecosysteme des Kunden schützen.

Produkt-Cybersicherheitsfähigkeit
Cybersicherheitsmerkmale oder -funktionen, die Computergeräte durch ihre eigenen technischen Mittel (d. h. Gerätehardware und -software) bereitstellen. [IR8259]

> *Anmerkung:* Dieser Begriff ist gleichbedeutend mit den in NISTIR 8259 definierten Cybersicherheitsfähigkeiten *von Geräten* , bezieht sich jedoch auf ein IoT-Produkt im Sinne dieses Dokuments und nicht nur auf ein IoT-Gerät.

IoT-Geräte
Geräte, die mindestens einen Messwertgeber (Sensor oder Aktuator) für die direkte Interaktion mit der physischen Welt und mindestens eine Netzwerkschnittstelle (z. B. Ethernet, WLAN, Bluetooth) für die Verbindung mit der digitalen Welt haben.

IoT-Produkt
Ein IoT-Gerät oder IoT-Geräte und alle zusätzlichen Produktkomponenten (z. B. Backend, mobile App), die zur Nutzung des IoT-Geräts über die grundlegenden Betriebsfunktionen hinaus erforderlich sind.

IoT-Produktkomponente
Ein IoT-Gerät oder eine andere digitale Ausrüstung oder Dienstleistung (z. B. Backend, mobile App), die zur Erstellung von IoT-Produkten verwendet wird.

Nicht-technische Unterstützungsfähigkeit
Nicht-technische unterstützende Fähigkeiten sind Maßnahmen, die eine Organisation zur Unterstützung der Cybersicherheit eines IoT-Geräts durchführt.