Leitfaden für die IoT-Sicherheit der Verbraucher

Titel

Leitfaden für die IoT-Sicherheit der Verbraucher

Datum

Oktober 2018

Zusammenfassung

Da wir zu Hause immer mehr Geräte mit dem Internet verbinden, werden Produkte und Geräte, die bisher offline waren, nun Teil des „Internets der Dinge“ (Internet of Things – IoT).

Das IoT eröffnet ein neues Kapitel in der Art und Weise, wie in unseren Häusern zunehmend Technologie eingesetzt wird, um das Leben einfacher und angenehmer zu machen. Da Online-Geräten und -Diensten immer mehr personenbezogene Daten anvertraut werden, ist die Cybersicherheit dieser Produkte heute ebenso wichtig wie die physische Sicherheit unserer Häuser und Wohnungen.

Ziel dieses Leitfadens ist es, alle an der Entwicklung, Herstellung und dem Vertrieb von IoT für Verbraucher beteiligten Parteien mit einer Reihe von Richtlinien zu unterstützen, um die Sicherheit von Produkten durch die Konzeption zu gewährleisten und es den Menschen einfacher zu machen, in einer digitalen Welt sicher zu bleiben.

Dieser Leitfaden fasst in dreizehn ergebnisorientierten Richtlinien das zusammen, was allgemeinhin als gute Praxis in der IoT-Sicherheit gilt. Er wurde vom Department for Digital, Culture, Media and Sports (DCMS) in Zusammenarbeit mit dem National Cyber Security Centre (NCSC) entwickelt und ist das Ergebnis der Zusammenarbeit mit Industrie, Verbraucherverbänden und Hochschulen. Der Leitfaden wurde erstmals im März 2018 im Entwurf als Teil des Berichts „Secure by Design“ (Sicherheit durch technische Konzeption) veröffentlicht.[1]

Einleitung

Das Internet der Dinge (IoT) bietet den Menschen große Chancen. Bei einer beträchtlichen Anzahl von Geräten auf dem heutigen Markt wurde jedoch festgestellt, dass es an grundlegenden Sicherheitsmaßnahmen mangelt. Die Nutzer sollten von den vernetzten Technologien auf sichere Weise profitieren und darauf vertrauen können, dass ihre Online-Aktivitäten durch angemessene Sicherheits- und Datenschutzmaßnahmen geschützt sind.

[1] DCMS, 2018, „Secure by Design: Improving the cyber security of consumer Internet of Things: Report“ (Sicherheit durch Technik: Verbesserte Cybersicherheit des Internets der Dinge für Verbraucher: Bericht)https://www.gov.uk/government/publications/secure-by-design.

Dieser Leitfaden legt praktische Schritte für IoT-Hersteller und andere Branchenbeteiligte fest, um die Sicherheit von IoT-Produkten für Verbraucher und die damit verbundenen Services zu verbessern. Die Umsetzung der dreizehn Richtlinien trägt zum Schutz der Privatsphäre und Sicherheit der Verbraucher bei und erleichtert ihnen gleichzeitig die sichere Verwendung ihrer Produkte. Außerdem wirkt sie der Gefahr von Distributed Denial of Service (DDoS)-Angriffen entgegen, die von unzureichend gesicherten IoT-Geräten und -Services ausgehen.

In den Richtlinien sind die allgemein anerkannten bewährten Verfahren der IoT-Sicherheit zusammengefasst. Sie sind eher ergebnisorientiert als vorschreibend und bieten Organisationen dadurch die Flexibilität, innovative und für ihre Produkte geeignete Sicherheitslösungen zu entwickeln und zu implementieren.

Dieser Leitfaden ist kein Patentrezept für die Lösung aller Sicherheitsherausforderungen. Nur durch den Wechsel zu einer sicherheitsorientierten Denkweise und die Investition in einen sicheren Entwicklungslebenszyklus kann ein Unternehmen erfolgreich ein sicheres IoT aufbauen. Produkte und Dienstleistungen sollten im Hinblick auf die Sicherheit entwickelt werden, von der Produktentwicklung an und über den gesamten Lebenszyklus hinweg. Unternehmen sollten darüber hinaus regelmäßig die Cyber-Sicherheitsrisiken bewerten, die für ihre Produkte und Dienstleistungen relevant sind, und geeignete Maßnahmen ergreifen, um diese zu minimieren.

Die Lieferketten von IoT-Produkten können komplex und international sein und häufig mehrere Komponentenhersteller und Dienstleister umfassen. Ziel des Leitfadens ist es, positive Veränderungen in Sachen Sicherheit in der gesamten Lieferkette einzuleiten und zu fördern.

Zahlreiche Branchenverbände und internationale Foren entwickeln Sicherheitsempfehlungen und -standards für das Internet der Dinge.[2] Dieser Leitfaden soll diese Bemühungen und die entsprechenden veröffentlichten Cybersicherheitsstandards ergänzen und unterstützen. Er wurde in direkter Zusammenarbeit mit der Industrie entwickelt, in der Hoffnung, dass zukünftige Prüf- und Gütezeichensysteme im Zusammenhang mit dem Verbraucher-IoT sich daran orientieren.

Die Umsetzung des Leitfadens kann Unternehmen dabei helfen, die Einhaltung der geltenden Datenschutzgesetze zu gewährleisten. So fordert beispielsweise die Datenschutz-Grundverordnung der EU (DSGVO), dass personenbezogene Daten sicher verarbeitet werden.[3]

Implementierung

[2] PETRAS, 2018, „Summary literature review of industry recommendations and international developments on IoT security“ (Zusammenfassender Literaturüberblick über Branchenempfehlungen und internationale Entwicklungen zur IoT-Sicherheit), https://www.gov.uk/government/publications/secure-by-design.

[3] Artikel 5(1)(f) der DSGVO betrifft die „Integrität und Vertraulichkeit“ personenbezogener Daten.

Der Leitfaden wird durch ein Zuordnungsdokument ergänzt, das jede seiner Richtlinien mit den wichtigsten Industriestandards, Empfehlungen und Leitlinien verknüpft.[4] Dieses Dokument bietet einen zusätzlichen Kontext für die dreizehn Richtlinien des Leitfadens und unterstützt die Industrie bei deren Umsetzung. In diesem Dokument wird auch der Zusammenhang zwischen dem Leitfaden und den Bemühungen um die IoT-Sicherheit aufgezeigt, die von einer Vielzahl von globalen Organisationen unternommen werden.

Priorisierung und Struktur

Die ersten drei Richtlinien haben Priorität, da Maßnahmen in Bezug auf Standardpasswörter, Offenlegung von Schwachstellen und Sicherheitsupdates kurzfristig die größten Sicherheitsvorteile bringen.

Der unterstützende Text erläutert die Begründung und fügt weitere Details zu jeder Richtlinie hinzu. Zusätzliche Erläuterungen am Ende des Dokuments dienen der Beantwortung häufig gestellter Fragen.

Zielgruppen

Für jede Richtlinie wird angegeben, welcher der Beteiligten in erster Linie für die Umsetzung verantwortlich ist. Beteiligte sind folgendermaßen definiert:

Gerätehersteller	Die Einheit, die ein fertig montiertes, mit dem Internet verbundenes Produkt herstellt. Ein Endprodukt kann die Produkte vieler verschiedener Hersteller enthalten.
IoT-Serviceprovider	Unternehmen, die Services wie Netzwerke, Cloud-Storage und Datentransfer anbieten, die als Bestandteil von IoT-Lösungen gebündelt werden. Im Rahmen des Services können auch internetfähige Geräte angeboten werden.
Entwickler von mobilen Anwendungen	Einheiten, die Anwendungen entwickeln und bereitstellen, die auf mobilen Geräten laufen. Diese werden oft als Interaktionsmöglichkeit mit Geräten im Rahmen einer IoT-Lösung angeboten.
Einzelhändler	Die Verkäufer von internetfähigen Produkten und den damit verbundenen Services für Verbraucher.

Terminologie

Durch die Verwendung des Begriffs „sicherheitssensible Daten“ soll zwischen anderen Arten von sensiblen Daten unterschieden werden – zum Beispiel besonderen Kategorien

[4] DCMS, 2018, „Mapping of IoT Security Recommendations, Guidance and Standards to the Code of Practice for Consumer IoT Security“ (Zuordnung von IoT-Sicherheitsempfehlungen, Leitlinien und Standards zum Leitfaden für die IoT-Sicherheit der Verbraucher), https://www.gov.uk/government/publications/secure-by-design.

personenbezogener Daten (formal bekannt als „sensible personenbezogene Daten“), wie sie in der DSGVO definiert sind. Zu den sicherheitssensiblen Daten können beispielsweise kryptographische Initialisierungsvektoren zählen.

Der Begriff „Verbraucher“ wird aus Gründen der Konsistenz durchgängig verwendet; als Verbraucher gelten im Allgemeinen Endverbraucher und -verbraucherinnen von IoT-Produkten und -Services.

Anwendungsbereich

Dieser Leitfaden gilt für IoT-Produkte für Verbraucher, die mit dem Internet und/oder dem Heimnetzwerk und den damit verbundenen Services verbunden sind. Die nicht vollständige Liste der Beispiele umfasst:

- vernetzte Kinderspielzeuge und Babyfonanlagen,
- vernetzte sicherheitsrelevante Produkte wie Rauchmelder und Türschlösser,
- Smart-Kameras, -Fernseher und -Lautsprecher,
- tragbare Gesundheitstracker,
- vernetzte Hausautomations- und Alarmsysteme,
- vernetzte Haushaltsgeräte (z. B. Waschmaschinen, Kühlschränke),
- Smart-Home-Assistenten.

Zugehörige Services werden hier als die digitalen Services betrachtet, die mit IoT-Geräten verbunden sind, z. B. mobile Anwendungen, Cloud-Computing/-Storage und Anwendungs-Programmierschnittstellen (APIs) von Drittanbietern für Services wie Messaging-Diensten.

Überprüfung

Das Department for Digital, Culture, Media and Sports (Ministerium für Digitales, Kultur, Medien und Sport) wird den Leitfaden regelmäßig, mindestens jedoch alle zwei Jahre, überprüfen und Aktualisierungen veröffentlichen. Wenden Sie sich an securebydesign@culture.gov.uk, um aktuelle Informationen zu erhalten.

Richtlinien

1) Keine Standardpasswörter verwenden

Alle IoT-Gerätepasswörter müssen eindeutig sein und dürfen nicht auf einen einheitlichen werkseitigen Standardwert zurückgesetzt werden können.

Viele IoT-Geräte werden mit einheitlichen Standardbenutzernamen und -passwörtern (z. B. „admin, admin“) verkauft, die vom Verbraucher geändert werden sollen. Diese Praxis hat zahlreiche Sicherheitsprobleme im IoT verursacht und muss beseitigt werden. Best Practices für Passwörter und andere Authentifizierungsmethoden sollten befolgt werden.[5]

Gilt hauptsächlich für: Gerätehersteller

2) Eine Richtlinie zur Offenlegung von Schwachstellen implementieren

Alle Unternehmen, die internetfähige Geräte und Services bereitstellen, müssen im Rahmen einer Richtlinie zur Offenlegung von Sicherheitsschwachstellen einen öffentlichen Ansprechpartner benennen, damit Sicherheitsforscher und andere Personen Probleme melden können. Die offengelegten Schwachstellen sollten zeitnah behoben werden.

Durch die Kenntnis einer Sicherheitslücke können Unternehmen entsprechend reagieren. Im Rahmen des Produkt-Sicherheitslebenszyklus sollten Unternehmen Schwachstellen innerhalb ihrer eigenen Produkte und Services ebenfalls kontinuierlich überwachen, identifizieren und beheben. Schwachstellen sollten zunächst direkt an die betroffenen Beteiligten gemeldet werden. Ist dies nicht möglich, können Schwachstellen den zuständigen staatlichen Behörden gemeldet werden.[6] Weitere Informationen zu den einzelnen Ansätzen, die unter verschiedenen Umständen zu verfolgen sind, finden Sie in den Erläuterungen. Unternehmen sind außerdem angehalten, Informationen an die zuständigen Branchenverbände weiterzugeben.[7]

Gilt hauptsächlich für: Gerätehersteller, IoT-Serviceprovider und Entwickler von mobilen Anwendungen

3) Software auf dem aktuellen Stand halten

---

[5] Eine Orientierungshilfe finden Sie beispielsweise hier: NCSC, 2016, „Password Guidance: Simplifying Your Approach“ (Passwort-Leitfaden: Vereinfachen Sie Ihren Ansatz), https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach. Siehe auch: NIST, 2017, „NIST Special Publication 800-63B: Digital Identity Guidelines – Authentication and Lifecycle Management“ (Richtlinien für digitale Identitäten – Authentifizierung und Lebenszyklusmanagement), https://pages.nist.gov/800-63-3/sp800-63b.html#sec5.

[6] Im Vereinigten Königreich können Meldungen über Schwachstellen an folgende Adresse gesendet werden: https://www.ncsc.gov.uk/contact.

[7] Zu den zuständigen Branchenverbänden gehören die GSMA und die IoT Security Foundation. Ein Leitfaden zur koordinierten Offenlegung von Schwachstellen ist bei der IoT Security Foundation erhältlich, die auf die Norm ISO/IEC 29147 zur Offenlegung von Schwachstellen verweist. Das koordinierte Programm zur Offenlegung von Schwachstellen auf Branchenebene der GSMA finden Sie unter https://www.gsma.com/cvd.

Softwarekomponenten in internetfähigen Geräten sollten sicher aktualisiert werden können. Die Aktualisierungen müssen zeitnah erfolgen und dürfen sich nicht auf die Funktion des Geräts auswirken. Für Endgeräte ist eine End-of-Life-Richtlinie zu veröffentlichen, die ausdrücklich die Mindestdauer, für die ein Gerät Software-Updates erhält, sowie die Gründe für die Länge des Supportzeitraums angibt. Die Notwendigkeit jeder Aktualisierung sollte den Verbrauchern deutlich gemacht werden, und eine Aktualisierung sollte leicht durchzuführen sein. Bei eingeschränkten Geräten, die nicht physisch aktualisiert werden können, sollte das Produkt isolierbar und austauschbar sein.

Die Herkunft von Sicherheitspatches sollte ebenfalls überprüft werden, und sie sollten über einen sicheren Kanal bereitgestellt werden. Die Grundfunktionen eines Geräts sollten während einer Aktualisierung nach Möglichkeit weiter ausgeführt werden, z. B. sollte eine Uhr weiterhin die Uhrzeit anzeigen, ein Raumthermostat weiterhin noch funktionieren und ein Schloss weiterhin entriegelt und verriegelt werden können. Dies mag hauptsächlich wie eine entwicklungsbezogene Überlegung wirken, es kann jedoch für einige Arten von Geräten und Systemen zu einem kritischen Sicherheitsproblem werden, wenn dieser Aspekt nicht angemessen berücksichtigt oder gehandhabt wird.

Software-Updates sollten nach dem Verkauf eines Geräts für einen dem Gerät angemessenen Zeitraum bereitgestellt und auf die Geräte übertragen werden. Dieser Support-Zeitraum für Software-Updates muss einem Verbraucher beim Kauf des Produkts deutlich gemacht werden. Der Einzelhandel und/oder die Hersteller sollten den Verbraucher darüber informieren, dass eine Aktualisierung erforderlich ist. Für eingeschränkte Geräte ohne die Möglichkeit eines Software-Updates sollten die Bedingungen und der Zeitraum für den Austauschservice klar sein.

Gilt hauptsächlich für: Gerätehersteller, IoT-Serviceprovider und Entwickler von mobilen Anwendungen

4) Zugangsdaten und sicherheitssensible Daten sicher speichern

Alle Zugangsdaten müssen innerhalb der Services und auf den Geräten sicher gespeichert werden. Fest kodierte Zugangsdaten in der Gerätesoftware sind nicht akzeptabel.

Durch das Reverse Engineering von Geräten und Anwendungen können Zugangsdaten wie fest kodierte Benutzernamen und Passwörter in Software leicht erkannt werden. Einfache Verschleierungsmethoden, die auch zum Verbergen oder Verschlüsseln dieser fest kodierten Informationen verwendet werden, können leicht aufgehoben werden. Zu den sicherheitssensiblen Daten, die sicher gespeichert werden sollen, gehören z. B. kryptographische Schlüssel, Gerätekennungen und Initialisierungsvektoren. Es sollten sichere, vertrauenswürdige Speichermechanismen verwendet werden, wie sie beispielsweise von einer Trusted Execution Environment (vertrauenswürdigen Laufzeitumgebung) und dem zugehörigen vertrauenswürdigen, sicheren Speicher bereitgestellt werden.

Gilt hauptsächlich für: Gerätehersteller, IoT-Serviceprovider, Entwickler von mobilen Anwendungen

5) Sicher kommunizieren

Sicherheitssensible Daten, einschließlich der Remote-Verwaltung und -Kontrolle, sollten während der Übertragung verschlüsselt werden, abgestimmt auf die Eigenschaften der Technologie und der Nutzung. Alle Schlüssel sollten sicher verwaltet werden.

Die Verwendung von offenen, von Experten geprüften Internetstandards wird dringend empfohlen.

Gilt hauptsächlich für: Gerätehersteller, IoT-Serviceprovider, Entwickler von mobilen Anwendungen

6) Angriffsflächen minimieren

Alle Geräte und Services sollten nach dem „Prinzip der minimalen Rechte“ (principle of least privilege) arbeiten. Nicht genutzte Ports sollten geschlossen werden, die Hardware sollte nicht unnötig zugänglich sein. Dienste sollten nicht verfügbar sein, wenn sie nicht verwendet werden, und der Code sollte auf den Funktionsumfang minimiert werden, der für den Betrieb des Services erforderlich ist. Die Software sollte mit angemessenen Rechten ausgeführt werden, die sowohl die Sicherheit als auch die Funktionalität berücksichtigen.

Das Prinzip der minimalen Rechte ist ein Grundstein einer soliden Sicherheitstechnik, der für das IoT ebenso anwendbar ist wie für jeden anderen Anwendungsbereich.

Gilt hauptsächlich für: Gerätehersteller, IoT-Serviceprovider

7) Software-Integrität gewährleisten

Software auf IoT-Geräten sollte mit sicheren Boot-Mechanismen verifiziert werden. Wenn eine nicht autorisierte Änderung erkannt wird, sollte das Gerät den Verbraucher/Administrator auf ein Problem hinweisen und sich nur mit den für die Alarmfunktion erforderlichen Netzwerken verbinden.

Die Möglichkeit der Remote-Wiederherstellung aus diesen Situationen sollte sich auf einen als funktionierend bekannten Status stützen, beispielsweise die lokale Speicherung einer als funktionierend bekannten Version, um eine sichere Wiederherstellung und Aktualisierung des Geräts zu ermöglichen. Dadurch werden Denial-of-Service und kostspielige Rückrufe oder Wartungsmaßnahmen vermieden. Gleichzeitig wird das Risiko minimiert, dass ein Angreifer das Gerät möglicherweise übernimmt, indem er Updates oder andere Mechanismen der Netzwerkkommunikation manipuliert.

Gilt hauptsächlich für: Gerätehersteller

8) Den Schutz von personenbezogenen Daten gewährleisten

Wenn Geräte und/oder Services personenbezogene Daten verarbeiten, muss dies in Übereinstimmung mit den geltenden Datenschutzgesetzen erfolgen, beispielsweise der

Datenschutz-Grundverordnung (DSGVO) und dem britischen Datenschutzgesetz Data Protection Act 2018. Gerätehersteller und IoT-Serviceprovider müssen den Verbrauchern für jedes Gerät und jeden Service klare und transparente Informationen darüber zur Verfügung stellen, wie, von wem und zu welchen Zwecken ihre Daten verwendet werden. Dies gilt auch für eventuell beteiligte Dritte (einschließlich Werbetreibender). Werden personenbezogene Daten auf der Grundlage der Einwilligung des Verbrauchers verarbeitet, so ist diese gültig und rechtmäßig einzuholen. Diese Verbraucher müssen die Möglichkeit haben, diese Einwilligung jederzeit zu widerrufen.

Diese Richtlinie stellt Folgendes sicher:
i) IoT-Hersteller, Serviceprovider und Entwickler von Anwendungen halten bei der Entwicklung und Bereitstellung von Produkten und Services die Datenschutzverpflichtungen ein.
ii) Personenbezogene Daten werden in Übereinstimmung mit geltenden Datenschutzgesetzen verarbeitet.
iii) Die Benutzer werden darin unterstützt, sicherzustellen, dass die Datenverarbeitungsvorgänge bei ihren Produkten einheitlich sind und wie angegeben ablaufen.
iv) Die Benutzer erhalten die Möglichkeit, ihre Privatsphäre zu schützen, indem die Geräte- und Servicefunktionen entsprechend konfiguriert werden.

Gilt hauptsächlich für: Gerätehersteller, IoT-Serviceprovider, Entwickler von mobilen Anwendungen, Einzelhändler

9) Systeme ausfallsicher gestalten

Die Ausfallsicherheit muss in IoT-Geräte und -Services integriert werden, wenn dies aufgrund ihrer Nutzung oder durch andere auf sie angewiesene Systeme erforderlich ist. Dabei ist die Möglichkeit eines Ausfalls von Datennetzen und Strom zu berücksichtigen. Soweit dies nach vernünftigem Ermessen möglich ist, sollten die IoT-Services im Falle eines Netzwerkausfalls betriebsbereit und lokal funktionsfähig bleiben und sich bei Wiederherstellung nach einem Stromausfall ordnungsgemäß wiederherstellen lassen. Geräte sollten sich in einem angemessenen Status und in geordneter Weise wieder mit einem Netzwerk verbinden lassen können anstatt eine umfangreiche Wiederverbindung vorzunehmen.

IoT-Systeme und -Geräte werden von Verbrauchern für immer wichtigere Anwendungsfälle eingesetzt, die sicherheitsrelevant oder lebensrettend sein können. Die Aufrechterhaltung des lokalen Servicebetriebs bei einem Netzwerkausfall ist eine der Maßnahmen, die zur Steigerung der Ausfallsicherheit ergriffen werden können. Weitere Maßnahmen sind unter anderem der Aufbau von Redundanzen bei den Services sowie die Abwehr von DDoS-Angriffen. Der erforderliche Grad der Ausfallsicherheit sollte verhältnismäßig sein und durch die Nutzung bestimmt werden. Es sollten jedoch andere Beteiligte berücksichtigt werden, die von dem System, Service oder Gerät abhängen, da es größere Auswirkungen haben kann als erwartet.

Gilt hauptsächlich für: Gerätehersteller, IoT-Serviceprovider

10) System-Telemetriedaten überwachen

Wenn Telemetriedaten von IoT-Geräten und -Services, beispielsweise Nutzungs- und Messdaten, gesammelt werden, sollten diese auf Sicherheitsanomalien überwacht werden.

Die Überwachung der Telemetrie, einschließlich Protokolldaten, ist für die Sicherheitseinschätzung nützlich und ermöglicht die frühzeitige Erkennung und Beseitigung ungewöhnlicher Umstände, die Minimierung von Sicherheitsrisiken und die schnelle Eindämmung von Problemen. Nach Richtlinie 8 sollte die Verarbeitung personenbezogener Daten jedoch auf ein Minimum beschränkt werden, und die Verbraucher sollten darüber informiert werden, welche Daten erhoben werden und aus welchen Gründen dies geschieht.

Gilt hauptsächlich für: IoT-Serviceprovider

11) Verbrauchern die einfache Löschung personenbezogener Daten ermöglichen

Geräte und Services sollten so konfiguriert sein, dass personenbezogene Daten leicht von ihnen entfernt werden können, wenn eine Eigentumsübertragung stattfindet, wenn der Verbraucher sie löschen möchte und/oder wenn der Verbraucher das Gerät entsorgen möchte. Die Verbraucher sollten klare Anweisungen erhalten, wie sie ihre personenbezogenen Daten löschen können.

IoT-Geräte können den Besitzer wechseln und werden irgendwann recycelt oder entsorgt. Es können Mechanismen bereitgestellt werden, mit denen der Verbraucher die Kontrolle behalten und personenbezogene Daten aus Services, Geräten und Anwendungen löschen kann.

Gilt hauptsächlich für: Gerätehersteller, IoT-Serviceprovider, Entwickler von mobilen Anwendungen

12) Installation und Wartung von Geräten vereinfachen

Die Installation und Wartung von IoT-Geräten sollte mit möglichst wenigen Schritten erfolgen und bewährte Sicherheitsverfahren in Bezug auf die Benutzerfreundlichkeit befolgen. Die Verbraucher sollten außerdem Anleitungen zur sicheren Einrichtung ihres Geräts erhalten.

Durch Irrtümer des Verbrauchers oder Fehlkonfigurationen verursachte Sicherheitsprobleme können reduziert und manchmal sogar beseitigt werden, wenn die Komplexität und das mangelhafte Design der Benutzeroberflächen angemessen behoben werden. Klare Anweisungen für Benutzer, wie man Geräte sicher konfiguriert, können die Gefährdung durch Bedrohungen ebenfalls reduzieren.

Gilt hauptsächlich für: Gerätehersteller, IoT-Serviceprovider, Entwickler von mobilen Anwendungen

13) Eingabedaten überprüfen

Dateneingaben über Benutzeroberflächen und Übertragungen über Anwendungsprogrammierschnittstellen (APIs) oder zwischen Netzwerken in Services und Geräten müssen überprüft werden.

Durch falsch formatierte Daten oder Codes, die über verschiedene Arten von Schnittstellen übertragen werden, können Systeme beschädigt werden. Häufig setzen Angreifer automatisierte Tools ein, um potenzielle Lücken und Schwachstellen auszunutzen, die durch die mangelnde Überprüfung von Daten entstehen. Beispiele sind u. a. Daten, die:
i) nicht vom erwarteten Typ sind, z. B. ausführbarer Code anstelle eines vom Benutzer eingegebenen Texts.
ii) außerhalb des zulässigen Bereichs liegen, z. B. ein Temperaturwert, der die Grenzen eines Sensors übersteigt.

Gilt hauptsächlich für: Gerätehersteller, IoT-Serviceprovider, Entwickler von mobilen Anwendungen

Zusätzliche Erläuterungen

Richtlinie 1 zur Vermeidung von Standardkennwörtern: Obwohl viel getan wurde, um die Abhängigkeit von Passwörtern zu beseitigen und alternative Methoden zur Authentifizierung von Benutzern und Systemen anzubieten, werden einige IoT-Produkte nach wie vor mit Standard-Benutzernamen und -Passwörtern von Benutzeroberflächen bis hin zu Netzwerkprotokollen auf den Markt gebracht. Dies ist keine akzeptable Praxis und sollte eingestellt werden. Die Gerätesicherheit kann durch eindeutige und unveränderliche Identitäten weiter verbessert werden.

Richtlinie 2 zur koordinierten Offenlegung von Schwachstellen (Coordinated Vulnerability Disclosure – CVD): CVD wird von der Internationalen Organisation für Normung (ISO) standardisiert, ist einfach zu implementieren und hat sich in einigen großen Softwareunternehmen in aller Welt erfolgreich bewährt.[8] Die CVD ist in der IoT-Branche jedoch immer noch nicht etabliert, und einige Unternehmen scheuen vielleicht vor der Zusammenarbeit mit Sicherheitsforschern zurück. Die CVD bietet den Sicherheitsforschern die Möglichkeit, sich an Unternehmen zu wenden, um sie über Sicherheitsprobleme zu informieren. Dadurch kann das Unternehmen der Bedrohung durch böswillige Ausnutzung von Schwachstellen zuvorkommen und hat die Möglichkeit, diese im Vorfeld einer öffentlichen Offenlegung zu beheben.

Unternehmen, die mit dem Internet verbundene Geräte und Services anbieten, haben gegenüber Dritten eine Sorgfaltspflicht, die durch das Fehlen eines CVD-Programms verletzt werden könnte. Darüber hinaus können Unternehmen, die diese Informationen über Branchenverbände weitergeben, anderen helfen, die möglicherweise von dem gleichen Problem betroffen sind.

Die Offenlegung kann je nach den Umständen unterschiedliche Ansätze erfordern:

[8] Internationale Organisation für Normung, 2014, ISO/IEC 29147 – Offenlegung von Schwachstellen, https://www.iso.org/standard/45170.html.

Schwachstellen in Bezug auf einzelne Produkte oder Services: Das Problem sollte direkt den betroffenen Beteiligten (z. B. Gerätehersteller, IoT-Serviceprovider oder Entwickler von mobilen Anwendungen) gemeldet werden. Quellen für diese Berichte können Sicherheitsforscher oder Branchenkollegen sein. Wenn der Gerätehersteller oder sonstige Beteiligte nach einer Kontaktaufnahme nicht zeitnah handeln, kann das Problem dem NCSC direkt gemeldet werden.

Systemische Schwachstellen: Möglicherweise entdeckt ein Beteiligter, beispielsweise ein Gerätehersteller, ein Problem, das potenziell systemisch ist. Auch wenn die Behebung dieses Problems im eigenen Produkt des Geräteherstellers von entscheidender Bedeutung ist, bietet es der Branche und den Verbrauchern einen erheblichen Nutzen, wenn diese Informationen weitergegeben werden. Auf ähnliche Weise können Sicherheitsforscher ebenfalls versuchen, solche systemischen Schwachstellen zu melden. In diesem Fall kann ein entsprechend zuständiger Branchenverband eine breit angelegte Reaktion koordinieren. Das NCSC kann den zuständigen Branchenverband bei der koordinierten Reaktion beraten und anleiten.

Der Zeitraum für eine „zeitnahe“ Reaktion auf Schwachstellen variiert erheblich und ist ereignisabhängig, es ist jedoch der De-facto-Standard, dass die Schwachstellenbehebung nach spätestens 90 Tagen abgeschlossen sein sollte. Die Problembehebung kann bei Hardware erheblich länger dauern als bei Software. Darüber hinaus kann eine Korrektur, die auf Geräten bereitgestellt werden muss, im Vergleich zu einer Softwarekorrektur auf einem Server einige Zeit in Anspruch nehmen.

Richtlinie 3 zur Aktualisierung von Software: Sicherheitsupdates für Software zählen zu den wichtigsten Maßnahmen, die ein Unternehmen ergreifen kann, um seine Kunden und das gesamte technische Ökosystem zu schützen. Schwachstellen entstehen oft durch Softwarekomponenten, die nicht als sicherheitsrelevant betrachtet werden. Daher sollte grundsätzlich jede Software regelmäßig aktualisiert und gepflegt werden. Fehlerbehebungen können präventiv auf die Geräte übertragen werden, oft im Rahmen automatischer Updates. Dadurch können Sicherheitsschwachstellen beseitigt werden, noch bevor sie ausgenutzt werden. Dies zu verwalten kann komplex sein, insbesondere wenn es um Cloud-Updates, Geräte-Updates und andere Service-Updates geht. Daher ist ein klarer Verwaltungs- und Bereitstellungsplan ebenso wichtig wie die Transparenz für die Verbraucher über den aktuellen Stand des Update-Supports.

In vielen Fällen ist die Veröffentlichung von Software-Updates mit mehrfachen Abhängigkeiten von anderen Organisationen, beispielsweise von Herstellern von Unterkomponenten, verbunden. Dies ist kein Grund, Updates zurückzuhalten – das Ziel des Leitfadens besteht darin, positive Veränderungen in Sachen Sicherheit in der gesamten Software-Lieferkette herbeizuführen. Es gibt auch einige Situationen, in denen Geräte nicht gepatcht werden können. In diese Kategorie fallen einige besonders eingeschränkte Geräte, für die ein Austauschplan erstellt werden muss. Dieser sollte dem Verbraucher klar mitgeteilt werden. Dieser Plan sollte einen Zeitplan für den Austausch der Technologien und gegebenenfalls für das Auslaufen des Supports für Hard- und Software enthalten.

Für die Verbraucher kann es entscheidend sein, dass ein Gerät weiterhin funktioniert. Deshalb sollte ein Update nach Möglichkeit „die Funktion eines Gerätes nicht

beeinträchtigen“. Insbesondere Geräte, die eine sicherheitsrelevante Funktion erfüllen, sollten bei einem Update nicht vollständig abgeschaltet werden. Es sollte eine minimale Systemfunktionsfähigkeit gegeben sein, z. B. die Aufrechterhaltung des Betriebs einer Heizungsanlage oder einer Alarmanlage. Die Hersteller dieser Art von Geräten sollten auch in Erwägung ziehen, zu einer Architektur mit höherer Ausfallsicherheit zu wechseln.

Man muss sich bewusst sein, dass die Mechanismen von Software-Updates ein Vektor für Angriffe sind, und es sollte gewährleistet sein, dass sie gesichert sind.

Richtlinie 5 zum sicheren Kommunizieren: Die Angemessenheit der Sicherheitskontrollen und die Verwendung einer Verschlüsselung hängen von vielen Faktoren ab, einschließlich dem Nutzungskontext.[9] Da sich der Bereich der Sicherheit ständig weiterentwickelt, ist es schwierig, verbindliche Ratschläge zu Verschlüsselungsmaßnahmen zu erteilen, ohne das Risiko einzugehen, dass diese Ratschläge schnell veraltet sind. Bei der Implementierung sollte sichergestellt werden, dass das Produkt den Anforderungen der Benutzer entspricht und gleichzeitig resistent gegen Angriffe auf die Verschlüsselung bleibt.

Richtlinie 7 zur Gewährleistung der Software-Integrität: Erkennt ein IoT-Gerät, dass etwas Ungewöhnliches mit seiner Software vorgefallen ist, muss es in der Lage sein, die richtige Person zu informieren. In einigen Fällen können die Geräte in den Administrationsmodus versetzt werden – beispielsweise kann es bei einem Thermostat in einem Raum einen Benutzermodus geben, der die Änderung anderer Einstellungen verhindert. In diesen Fällen ist eine Warnung an den Administrator angemessen, da diese Person die Möglichkeit hat, auf die Warnung zu reagieren.

Richtlinie 9 zur Ausfallsicherheit von Systemen Diese Richtlinie soll sicherstellen, dass IoT-Services stets auf dem neuesten Stand gehalten werden, während die Nutzung von IoT-Geräten in allen Lebensbereichen eines Verbrauchers zunimmt. Das gilt auch für Funktionen, die für die persönliche Sicherheit relevant sind. Die Auswirkungen auf das Leben von Menschen könnten weitreichend sein, wenn z. B. bei einer vernetzten Tür die Internetverbindung abbricht und jemand ausgesperrt ist. Ein weiteres Beispiel ist eine Hausheizungsanlage, die sich aufgrund eines DDoS-Angriffs gegen einen Cloud-Service abschaltet. Dabei ist zu beachten, dass andere sicherheitsrelevante Vorschriften gelten können, dass es jedoch darauf ankommt, Ausfälle nicht zur Ursache solcher [Probleme werden zu lassen].

[9] Eine Orientierungshilfe finden Sie z. B. beim NCSC unter https://www.ncsc.gov.uk/guidance/tls-external-facing-services.