Internationale Arbeitsgruppe
für Datenschutz
in der Telekommunikation

675.55.8

Arbeitspapier
Aktualisierung der Firmware eingebetteter Systeme im Internet der Dinge

62. Tagung, 27./28. November 2017, Paris (Frankreich)

– *Übersetzung* –

Einführung

Schätzungen hinsichtlich der Zahl der Geräte im Internet der Dinge (Internet of Things, IoT), die bis 2020 online sein werden, gehen weit auseinander – und reichen von 26 Milliarden[1] bis 50 Milliarden[2] Geräten. Ganz egal, welche Zahl nun richtig ist: Fakt bleibt, dass es in den kommenden Jahren zu einem enormen Anstieg der Zahl von Geräten kommen wird, die mit dem Internet verbunden sind.

Für den Begriff „Internet der Dinge" gibt es keine allgemein anerkannte Definition. Eine Quelle[3] definiert IoT folgendermaßen: *„Eine globale Infrastruktur für die Informationsgesellschaft, die hochmoderne Services unterstützt, indem sie (physische und virtuelle) Dinge auf Grundlage vorhandener und neuer kompatibler Informations- und Kommunikationstechnologien miteinander vernetzt"*. Die Internet Society interpretiert IoT im weiteren Sinne als *„Erweiterung von Netzwerkverbindungen und Rechenfunktionen auf Objekte, Geräte, Sensoren und Elemente, die normalerweise nicht als Computer gelten"*[4].

---

[1] „Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020", Pressemitteilung von Gartner vom 12. Dezember 2013, online abrufbar unter http://www.gartner.com/newsroom/id/2636073

[2] *„The Internet of Things: How the Next Evolution of the Internet Is Changing Everything", Whitepaper von Cisco aus dem April 2011, online abrufbar unter* http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

[3] „Overview of the Internet of Things", ITU Telecommunication Standardization Sector Recommendations http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060

[4] „The Internet of Things: An Overview", The Internet Society, 2015, https://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151221-en.pdf

Sekretariat
Berliner Beauftragte für
Datenschutz und Informationsfreiheit
Friedrichstr. 219
10969 Berlin
Tel.: +49 30 13 88 90
Fax: +49 30 21 55 050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

Charakteristisch für Geräte, die das Internet der Dinge ausmachen, ist ihre Anbindung an ein Netzwerk sowie ihre Fähigkeit zum Sammeln und Übertragen von Daten über das Internet (egal ob per Kabel oder drahtlos). Durch die Verbindung solcher Geräte mit dem Internet entstehen beispielsweise Möglichkeiten zur Fernsteuerung, Fernmessung und Automatisierung. Gleichzeitig steigt jedoch das Risiko, dass diese Geräte und von ihnen verarbeitete Daten kompromittiert werden.

Das IoT-Ökosystem ist weitreichend und überschreitet zahlreiche Branchengrenzen. Dazu gehören zum Beispiel IT und Netzwerke, Sicherheit und öffentliche Sicherheit, Einzelhandel, Transportwesen, Industrie, Gesundheitswesen, Konsumgüter und Haushaltsgeräte, Energie, Gebäude. IoT-Geräte bestehen in der Regel aus einem oder mehreren eingebetteten Systemen bzw. beinhalten solche Systeme (eigenständige Rechenmodule), die meist einen bestimmten Verarbeitungszweck haben, um zusammen genommen die gewünschte Verarbeitungsfunktion des IoT-Geräts zu ergeben. Diese integrierten Systeme weisen begrenzte CPU-, Arbeitsspeicher- und Energieressourcen mit „*spezifischen Designbeschränkungen hinsichtlich Preis, Größe, Gewicht und anderen Skalierungsfaktoren*“[5] auf (und werden daher auch ressourcenbeschränkte Geräte genannt). Die Beschränkungen haben zur Folge, dass Hersteller oftmals keinen Mechanismus für Software- bzw. Firmwareupdates in die Geräte integrieren. Beispiele für IoT-Geräte sind vernetzte Umgebungssensoren (für Temperatur, Luftfeuchtigkeit und Druck), Lampen, Drucker oder Kameras in einem Home-Security-System.

In vielen Fällen besorgen sich Hersteller von IoT-Geräten Komponenten (wie eingebettete Systeme) für ihre Produkte bei Drittanbietern. Lieferanten solcher Subkomponenten produzieren zum Teil Jahr für Jahr Millionen solcher integrierten Systeme, weswegen Änderungen in der Lieferkette zeitaufwendig und teuer sind. Aufgrund dieser zeitlichen Verzögerung in der Lieferkette können einzelne Softwarekomponenten bereits Monate oder Jahre alt sein, bevor sie in einem Endprodukt verbaut werden.

Die Allgegenwart von IoT-Geräten, die Vielfalt der möglichen Sensoren sowie ihre Nähe zu Personen (einschließlich der Fähigkeit zur Einbettung in den menschlichen Körper) erhöhen die Wahrscheinlichkeit deutlich, dass diese Geräte Informationen über verschiedenste Aspekte (z. B. Physiologie, Verhalten, Aufenthaltsort usw.) im Leben einer Person verarbeiten (d. h. sammeln, verändern, speichern und übertragen). Da viele dieser Systeme von Gerät zu Gerät kommunizieren und menschliche Interaktion komplett umgehen, entstehen immense potenzielle Risiken für die Grundrechte und Freiheiten von Personen.

In diesem Arbeitspapier werden Risiken beleuchtet, die dann entstehen, wenn Firmware, die der Verhaltenssteuerung eines IoT-Geräts dient, nicht aktualisiert wird. Außerdem werden einige der Vorteile erfolgreicher Updates vorgestellt (z. B. Implementierung neuer Funktionen, die dem Benutzer unbekannt waren). Zu den Risiken gehören unter anderem eine unbefugte Sammlung, Modifizierung oder Offenlegung personenbezogener Daten, die vom Gerät erfasst werden, sowie eine Ausnutzung von Geräteschwachstellen, um ein Gerät zur Kompromittierung der Integrität anderer Systeme zu verwenden, die personenbezogene Daten verarbeiten oder schützen. Auf Geräte wie Desktop-PCs, Tablets, Smartphones, Smart TVs, Entertainment-Systeme in vernetzten Fahrzeugen usw. wird in diesem Dokument nicht eingegangen.

[5] „Terminology for Constrained-Node Networks“ https://tools.ietf.org/html/rfc7228

Was ist Firmware?

Eingebettete Systeme umfassen meist einen oder mehrere Mikrocontroller mit begrenztem Arbeitsspeicher sowie beschränkter Verarbeitungsleistung. Die im Mikrocontroller installierte Software ist genau auf die Anforderungen des Mikrocontrollers und die Aufgabe des Geräts zugeschnitten. Diese Software wird normalerweise als Firmware bezeichnet und stellt die erforderlichen Befehle bereit, damit das Gerät mit anderer Computerhardware bzw. dem übergeordneten Netzwerk kommunizieren kann. Firmware wird auf dem Gerät in nichtflüchtigem Speicher (Flash oder ROM) gespeichert.

Warum muss Firmware aktualisiert werden?

Jede Art von Software kann Fehler aufweisen – auch dann, wenn Software ausführlich getestet wurde. Manche von ihnen sind dem Hersteller ggf. bekannt, wurden jedoch nicht beseitigt, um Fertigungstermine nicht zu gefährden. Andere Fehler jedoch werden erst nach der Auslieferung von Geräten erkannt. Diese Fehler (auch Bugs genannt) sind unterschiedlich schwerwiegend. Manche von ihnen sind geringfügig und haben kaum Auswirkungen auf den regulären Betrieb eines Geräts. Andere Fehler hingegen haben ernsthafte Folgen und können dazu führen, dass sich Geräte fehlerhaft verhalten.

Wie bei anderer Software auch kann es verschiedene Gründe für eine Aktualisierung der Firmware geben:

a) das Hinzufügen neuer **Funktionen**;
b) der **Neukonfiguration** aufgrund veränderter Internetprotokolle;
c) der Behebung von **Firmwarefehlern**; oder
d) der Ersatz **schwacher Verschlüsselungsalgorithmen oder -schlüssel** (alle Verschlüsselungsalgorithmen weisen ein Ablaufdatum auf).

Bugs, die es Angreifern ermöglichen, die Sicherheit[6] eines Geräts zu verletzen (d. h. eine Softwareschwachstelle), können eine Gefahr für das übergeordnete Netzwerk, für die vom Gerät verarbeiteten Daten sowie für jene Personen bedeuten, auf die sich die Daten beziehen.

Wie kann Firmware aktualisiert werden?

Zu garantieren, dass Firmware so schnell wie möglich und richtig aktualisiert wird, ist schon bei traditionellen Computergeräten nicht einfach. Die Merkmale eingebetteter Systeme in IoT-Geräten bringen jedoch zusätzliche Herausforderungen mit sich.

Vielen eingebetteten Systemen fehlt es an Möglichkeiten zur einfachen oder automatischen Aktualisierung von Firmware, die sich verwenden lassen, nachdem ein Gerät die Fabrik verlassen hat. Grund dafür können verschiedene Faktoren sein, zum Beispiel die Spezifikation oder das Design des Geräts. Vom Hersteller bereitgestellte Firmwareupdates werden in der Regel auf einer Supportseite veröffentlicht, damit sie der Benutzer herunterladen und manuell installieren kann. Oftmals beginnt die manuelle Installation mit der Übertragung eines Firmware-Images über ein standardmäßiges oder proprietäres Protokoll, das überprüft (oder auch nicht), ob die jeweilige Person das entsprechende Verfahren initiieren darf. Anschließend muss das Firmware-Image auf das IoT-Gerät

[6] Sicherheitsverletzungen werden definiert als negativer Effekt auf die Vertraulichkeit, Integrität oder Verfügbarkeit.

übertragen werden, zum Beispiel durch Verbindungsherstellung mit einem Webserver, der in das Gerät integriert ist, durch Anschließen eines USB-Sticks an das Gerät bzw. durch eine andere Methode. Dabei muss beachtet werden, dass manche IoT-Geräte keine traditionelle oder überhaupt keine Benutzeroberfläche aufweisen. Das Update lässt sich teilweise durch einfaches Entpacken eines Dateiarchivs anwenden. Manchmal ist es jedoch erforderlich, dass das Gerät aufgrund der hohen Sicherheitssensibilität des Firmwareupdates in einen speziellen Zustand versetzt wird. Dabei werden die Konfiguration oder Personalisierung des Geräts durch den Benutzer einschließlich vorhandener Datenschutzeinstellungen ggf. überschrieben und müssen wiederhergestellt werden. In jedem Fall ist eine Aktualisierung der Firmware von IoT-Geräten für durchschnittliche Benutzer nicht immer einfach.

Probleme mit Firmwareupdates

Zur Gewährleistung zuverlässiger und sicherer Firmwareupdates müssen verschiedene Herausforderungen berücksichtigt werden. Dazu gehören u. a.:

1. Geräte sind unter Umständen nicht leicht zugänglich (physisch oder logisch), was eine Bereitstellung von Firmwareupdates schwierig oder unmöglich macht.

2. Geräte sind unter Umständen nicht updatefähig (zum Beispiel wegen technischer Begrenzungen), weswegen sie physisch durch andere Geräte ersetzt werden müssen, die die aktualisierte Firmware enthalten.

3. Ein Netzwerk, das heterogene Geräte (von verschiedenen Herstellern) umfasst, erhält Updates zu unterschiedlichen Zeitpunkten, sodass Schwachstellen unterschiedlich schnell (oder gar nicht) behoben werden, was den Sicherheitszustand des ganzen Netzwerks ständig in Zweifel lässt.

4. Die Verantwortung für die Aktualisierung von Geräten, die mehreren Unternehmen und Personen gehören, ist unklar oder nicht definiert.

5. Privatpersonen müssen darüber informiert werden, dass Firmwareupdates zur Verfügung stehen und eine rasche sowie konsistente Installation erfordern.

6. Firmwareupdates verändern Gerätefunktionen unter Umständen auf unerwartete und unerwünschte Weise.

7. Firmwareupdates können fehlschlagen und ein defektes Gerät zur Folge haben, das sich nicht wiederherstellen lässt (d. h., das Gerät ist nicht mehr einsatzfähig).

8. Das Updateverfahren unterstützt keine partiellen oder differenziellen Updates, auch wenn nur ein Teil des Firmwarecodes aktualisiert werden muss.

9. Das Verfahren zur Firmwareaktualisierung kann manipulationsanfällig sein (z. B. wird möglicherweise unabsichtlich manipulierter Code aus nicht vertrauenswürdigen Quellen anstelle des veröffentlichten Firmwareimages installiert, was zu einer Sicherheitsverletzung oder Beschädigung des Geräts führen kann).

10. Unter Umständen wird das Gerät vom Originalhersteller nicht mehr unterstützt und das erwartete Firmwareupdate ist nicht mehr verfügbar.

11. Kann ein Gerät nicht aktualisiert werden oder wurde kompromittiert, muss es möglicherweise vom Netzwerk isoliert werden.

12. Ist das Verfahren zur Firmwareaktualisierung schwierig oder zeitaufwendig, entscheiden Benutzer möglicherweise, kein Update vorzunehmen und auf die Verbesserung von Datenschutz und Sicherheit zu verzichten – vor allem dann, wenn Benutzer nicht verstehen, wie ein Update ihr Gerät sicherer machen würde.[7]

Risiken für Privatsphäre und Datenschutz

R1. Schwachstellen in Gerätefirmware können Angreifern direkten Zugriff auf die Sensoren eines Geräts bieten, sodass sie die Sensoren aktivieren und Sensordaten (z. B. Kamerabilder oder Audioaufnahmen) erfassen oder derartige Daten abrufen können, wenn diese auf dem Gerät gespeichert sind. Häufige Ziele sind sprachgesteuerte Geräte, IP-Kameras[8] und sogar Spielsachen[9].

R2. Angreifer können versuchen, Schwachstellen in IoT-Geräten auszunutzen, um sich die Kontrolle über diese zu verschaffen und sie als Proxy für weitere illegale Aktivitäten zu verwenden, die ein Risiko für Privatsphäre und Datenschutz darstellen.[10]

R3. Außerdem können Angreifer versuchen, auf andere gespeicherte Daten zuzugreifen, die von Sensordaten abgeleitet wurden (zum Beispiel Hinweise darauf, wann sich eine bestimmte Person in der Nähe des Geräts befand).

R4. Darüber hinaus können Angreifer auf dem Gerät gespeicherte Anmeldedaten abrufen, um sich Zugang zu Hintergrundsystemen zu verschaffen, und möglicherweise auf dort gespeicherte Sensordaten zugreifen bzw. Verschlüsselungsschlüssel abrufen oder manipulieren, die zum Schutz der Kommunikation des Geräts dienen. So lassen sich Daten während ihrer Übertragung abfangen.

R5. Wird das IoT-Gerät in einem Privathaushalt platziert, können Sensordaten und davon abgeleitete Daten Informationen über den normalen Tagesablauf sowie Verhaltensweisen und Gewohnheiten von Personen in dem Haushalt enthalten. Diese Informationen können aus längeren Zeiträumen stammen, jedoch mittels eines einzigen Zugriffs abgerufen werden.

R6. In Privathaushalten platzierte IoT-Geräte speichern möglicherweise auch andere Anmeldedaten von Personen (z. B. Anmeldedaten für den Versand von E-Mails oder das Posten von Informationen in sozialen Netzwerken im Namen der Person), die sich bei einem Angriff entwenden lassen. Mithilfe dieser Anmeldedaten wären weitere Angriffe möglich.

---

[7] Siehe Arunesh Mathur & Marshini Chetty, *„Impact of User Characteristics on Attitudes Towards Automatic Mobile Application Updates“*, Thirteenth Symposium on Usable Privacy and Security, Seite 175, 12. bis 14. Juli 2017, https://www.usenix.org/system/files/conference/soups2017/soups2017-mathur.pdf (Aktualisierung mobiler Apps). Siehe auch Kami Vaniea & Yasmeen Rashidi, *„Tales of Software Updates: The Process of Updating Software“*, 2016, https://vaniea.com/papers/chi2016.pdf (Aktualisierung von PCs) sowie M. Fagan et al., *„A Study of Users' Experiences and Beliefs About Software Update Messages“*, Computers in Human Behavior, Vol. 51, Teil A, S. 504-519 (Okt. 2015), https://dl.acm.org/citation.cfm?id=2805432 (ebd.).

[8] http://securityaffairs.co/wordpress/50929/malware/linux-mirai-elf.html

[9] „Bundesnetzagentur removes children's doll ‚Cayla' from the market“, https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/EN/2017/17022017_cayla.html?nn=404422

[10] https://krebsonsecurity.com/2016/iot-devices-as-proxies-for-cybercrime/

Empfehlungen

Bei der Betrachtung von Firmwareupdates im Kontext eingebetteter Systeme ist es wichtig, dass die Sicherheits- und Datenschutzaspekte in ihrer Gesamtheit berücksichtigt werden. Die Herausforderung besteht darin, die allgemeinen Sicherheitspraktiken, die traditionell in der IT-Branche zur Bekämpfung von Sicherheitsbedrohungen eingesetzt werden (z. B. sicheres Booten, Zugangskontrolle, Geräteauthentifizierung, Firewalls und Intrusion-Protection-Systeme sowie Updates), auch im IoT-Bereich anzuwenden.

Folgende Empfehlungen tragen zur Lösung der in diesem Arbeitspapier beschriebenen Probleme bei:

Regulierungsbehörden, Gesetzgeber und Aufsichtsbehörden

M1. Förderung der Entwicklung und Einführung von Verfahren für Firmwareupdates in eingebetteten Systemen;

M2. Förderung von Maßnahmen zur Aufklärung von Unternehmen und Privatpersonen hinsichtlich der Probleme mit Firmwareupdates;

M3. Förderung von Projekten, die der Behebung von Sicherheitslücken in Geräten dienen;[11]

M4. Festlegung von Anforderungen an die Sicherheit von IoT-Geräten, die an Privatpersonen verkauft werden, inklusive der Verpflichtung zur Bereitstellung von Informationen über die installierte Firmware, über den Zeitraum, in dem Updates für die Firmware der Geräte für bekannte Lücken zur Verfügung gestellt werden, und über das Verfahren, das Privatpersonen befolgen müssen, um sicherzustellen, dass auf das Produkt die neuesten Sicherheitsupdates angewendet werden; und

M5. Festlegung von Anforderungen zur Zertifizierung von Updateverfahren für IoT-Firmware unter Beachtung relevanter Branchenstandards. Dabei sollten die verschiedenen Arten von IoT-Geräten berücksichtigt werden. Durch eine Zertifizierung sollen die verschiedenen Risiken behoben sowie Sicherheits- und Datenschutzkontrollen in Firmwareupdates integriert werden.

Gerätehersteller

M6. Entwicklung und Implementierung eines sicheren Updateverfahrens für Gerätefirmware inklusive der Möglichkeit zur nahtlosen und raschen Bereitstellung von Updates (vorzugsweise durch automatische Updates), um den Aufwand für private Benutzer zu minimieren;

M7. Ist eine automatische Firmwareaktualisierung möglich, müssen Datenschutzaspekte, sicherheitsfreundliche Standardeinstellungen sowie die vom Benutzer zuvor festgelegten Konfigurationsoptionen berücksichtigt werden, während Anwender die Gelegenheit erhalten müssen, einzelne Updates zuzulassen oder abzulehnen und zu entscheiden, wann Updates durchgeführt werden sollen;

[11] Die Federal Trade Commission hat einen Wettbewerb veranstaltet, um die Öffentlichkeit dazu zu bringen, technische Lösungen bzw. Tools zu entwickeln, mit denen sich Endverbraucher vor Sicherheitslücken in Software schützen können, die sich auf IoT-Geräten in Privathaushalten befindet. https://www.ftc.gov/iot-home-inspector-challenge.

M8. Ermittlung, ob das Updateverfahren ausschließlich eine (automatische oder anderweitige) Installation von Updates, die von autorisierten Parteien bereitgestellt wurden, auf autorisierten Geräten zulässt, und Gewährleistung der Codeintegrität;

M9. Bereitstellung von Informationen an Benutzer über die Sicherheitsrisiken einer Installation von Updates aus nicht autorisierten Quellen, über die Gefahren einer Nicht-Installation autorisierter Updates und über die Vorteile einer Installation von Updates bzw. einer Aktivierung von automatischen Updates;

M10. Entwicklung und/oder Nutzung offener Standards für grundlegende Funktionen wie Verschlüsselung und Netzwerkkonnektivität;

M11. Anwendung allgemein anerkannter Best Practices für die Sicherheit und die Einschätzung von Datenschutzrisiken im Lebenszyklus eines Geräts;

M12. Gewährleistung, dass alle Drittanbieter kontinuierlichen Support für Firmware bereitstellen, die Bestandteil von an den Hersteller ausgelieferten Komponenten ist;

M13. Benachrichtigung der Benutzer über die installierte Firmware, über den Zeitraum, in dem Updates für die Gerätefirmware für bekannte Lücken zur Verfügung gestellt werden, und über das Verfahren, das Privatpersonen befolgen müssen, um sicherzustellen, dass auf das Produkt die neuesten Sicherheitsupdates angewendet werden;

M14. Festlegung und Kommunikation einer eindeutigen Frist für den Sicherheitssupport für alle entwickelten Geräte. Benachrichtigung an Benutzer vor dem Kauf, welchen Sicherheitssupport sie erhalten werden, und Erinnerung an Benutzer, wenn der Sicherheitssupport bald abläuft;

M15. rasche Bereitstellung von Updates für alle Geräte in der unterstützten Lebensdauer;

M16. Evaluierung kostengünstiger Alternativen für fortgesetzten Support nach Ende der Unterstützung durch den Hersteller wie Freigabe von Quellcode im Rahmen einer Open-Source-Lizenz für jene Geräte, deren Lebensdauer abgelaufen ist;

M17. Anwendung eines transparenten Updateansatzes, indem umfassende Informationen zu Fehlerbehebungen und neuen Funktionen in Softwareupdates sowie zu allen Änderungen des Orts bereitgestellt werden, an dem Daten verarbeitet werden (in Folge des Firmwareupdates);

M18. Möglichkeit für Benutzer, sich über Firmwareschwachstellen zu informieren, und Bereitstellung von Informationen zur Risikominderung, solange Updates entwickelt werden; und

M19. ausführliches Testen von Firmware vor der Bereitstellung sowie gründliches Testen aller Updates anhand der gleich hohen Standards.

Gerätebesitzer (Unternehmen)

M20. Ausschließlicher Erwerb von Geräten, für die Hersteller zeitnah Sicherheitsinformationen und Firmwareupdates bereitstellen, oder Minderung aller potenziellen Risiken, die durch Firmwareschwachstellen entstehen können, auf eine andere geeignete Weise;

M21. Unternehmen sollten eine Ressourcenliste führen, mit deren Hilfe sich Geräte physisch und logisch lokalisieren lassen;

M22. Unternehmen sollten die Architektur ihrer Systeme, die implementierten Vorsichtsmaßnahmen sowie Art und Ausmaß der von Geräten verarbeiteten Daten dokumentieren (inkl. der Rechtsgrundlage für die Verarbeitung);

M23. Unternehmen sollten dafür sorgen, dass sie auf von Geräteherstellern veröffentlichte Informationen über Sicherheitslücken hingewiesen werden, und so schnell wie möglich auf solche Warnungen reagieren;

M24. Unternehmen sollten für alle Gerätetypen (auch für Geräte unterschiedlicher Hersteller) ein dokumentiertes und prüfbares Verfahren zur Installation von Firmwareupdates aufweisen, das für alle zu implementierenden Updates Integritätsprüfungen umfasst und bestätigt, dass mit Sicherheit und Datenschutz verbundene Konfigurationseinstellungen beibehalten bzw. nach dem Rollout neu festgelegt werden;

M25. Unternehmen sollten erwägen, ob vor einer Installation Tests durchgeführt werden müssen, die über die vom Gerätehersteller absolvierten Tests hinausgehen;

M26. entscheidet sich ein Unternehmen gegen die Installation eines Firmwareupdates, sollte diese Entscheidung zusammen mit allen angewendeten Minderungsmaßnahmen dokumentiert werden; und

M27. Unternehmen sollten über eine Richtlinie verfügen, in der die Methode zum Herunterfahren, Isolieren und/oder Verschieben von Geräten aus dem Netzwerk in die Quarantäne beschrieben wird, falls eine schwerwiegende Sicherheitslücke oder -verletzung auftritt bzw. falls der Gerätehersteller keine Sicherheitsinformationen und Updates mehr für das Produkt bereitstellt.

Gerätebesitzer (Privatpersonen)

M28. Privatpersonen sollten sich bei Fragen zu Firmwareupdates für ihre Geräte an den Gerätehersteller wenden;

M29. Privatpersonen sollten die offizielle Lebensdauer ihres Geräts kennen und sich darüber im Klaren sein, dass danach möglicherweise keine Updates mehr zur Verfügung gestellt werden;

M30. Privatpersonen sollten eine Aktivierung automatischer Firmwareupdates erwägen (so verfügbar) oder anderweitig dafür sorgen, dass Firmware auf ihren Geräten auf dem aktuellen Stand ist;

M31. Privatpersonen sollten Firmwareupdates ausschließlich aus vertrauenswürdigen Quellen (z. B. von der Website des Geräteherstellers) oder über das bereitgestellte sichere Updateverfahren beziehen und soweit möglich deren Integrität verifizieren; und

M32. Privatpersonen sollten wissen, dass das jeweilige Gerät sowie das übergeordnete Netzwerk bei Ablehnung eines Firmwareupdates (zum Beispiel aus Angst vor einer Beeinträchtigung der Funktionalität oder Stabilität) unnötige Sicherheitslücken aufweisen und dadurch zusätzliche Risiken für die Person sowie alle anderen Personen entstehen können, die mit dem Gerät in Kontakt kommen.