Zentrum für sichere Informationstechnologie – Austria
Secure Information Technology Center – Austria

A-SIT

Seidlgasse 22 / 9, 1030 Wien
Tel.: (+43 1) 503 19 63–0
Fax: (+43 1) 503 19 63–66

Inffeldgasse 16a, 8010 Graz
Tel.: (+43 316) 873-5514
Fax: (+43 316) 873-5520

http://www.a-sit.at
E-Mail: office@a-sit.at

DVR: 1035461
ZVR: 948166612
UID: ATU60778947

BEURTEILUNG VON SICHERHEITSSTANDARDS FÜR IOT-HAUSHALTSGERÄTE

Version 1.0 vom 01.03.2019
Peter Aufner – peter.aufner@iaik.tugraz.at

Abstract/Zusammenfassung: Diese Arbeit bietet einen Überblick über verschiedene Sicherheitsstandards, welche auf Haushalts-IoT anwendbar sind. Es wird zwischen verpflichtenden Standards, wie dem CE-Siegel, optionalen Prüfsiegeln, die durch unabhängige Institutionen vergeben werden, legislativen Entwürfen und Standards aus der Softwareentwicklung unterschieden. Der Fokus liegt hier auf Sicherheit im Sinne der IT-Sicherheit, also dem Schutz von personenbezogenen Daten und der Vermeidung von Angriffen gegen oder unter Verwendung von IoT-Geräten. Es wird gezeigt, dass grundsätzlich das Wissen zum Schutz vor Schwachstellen in IoT in best practices vorhanden ist und manche Maßnahmen laut Entwürfen verpflichtend werden können.

Inhaltsverzeichnis

1. Verpflichtende Sicherheitsstandards für Haushaltsgeräte

In der Europäischen Union existiert das CE-Siegel, welches eine Reihe von Richtlinien zusammenfasst, an die sich Produzenten von Geräten halten müssen, um ein Produkt in der E.U. vertreiben zu dürfen. Diese umfassen beispielsweise die Richtlinie 2005/32/EG für Haushaltskühl- und gefriergeräte, oder 2009/48/EG für Spielzeuge. Der Hersteller handelt hierbei eigenverantwortlich und bewertet die Konformität seiner Produkte. Eine externe Überprüfung ist nicht zwingend vorgesehen.

© A-SIT, Partner für Sicherheitsfragen

Einige relevante Richtlinien werden in der folgenden Tabelle aufgezählt:

Produkttyp	**Richtlinie**
Haushaltskühl- und gefriergeräte	2012/27/EU [1]
Elektrische Betriebsmittel	2014/35/EU [2]
Spielzeug	2009/48/EG [3]
Funkanlagen	2014/53/EU [4]

Die genannten Richtlinien sehen Maßnahmen zur Wahrung der Sicherheit der Konsumenten vor. Sicherheit bezieht hierbei auf die körperliche Gesundheit und Unversehrtheit. Es soll Schutz vor gefährlichen Substanzen, Elektrizität, Elektromagnetismus, u.ä. gewahrt werden. Teilweise werden auch Rahmenbedingungen, welche die Mitgliedsstaaten zum Einsatz der Produkte bieten sollen, angegeben. Dies geschieht beispielsweise in der Norm für Funkanlagen, welche fordert, dass die Stromnetze in den Mitgliedsstaaten so beschaffen sein müssen, dass ein elektrisch sicherer Betrieb der Geräte gewährleistet ist.

Im Folgenden ein kurzer Umriss zu den Inhalten der Richtlinien:

2012/27/EU
Diese Richtlinie befasst sich mit dem Ressourcenverbrauch von Geräten. In Österreich ist sie in der Ökodesign Richtlinie umgesetzt. Es geht hier ausschließlich um Aspekte des Umweltschutzes.

2014/35/EU
Diese Richtlinie betrifft Geräte mit einer Nennspannung von 50-1000V Wechselstrom, oder 75-1500V Gleichstrom. Die zentrale Forderung der Richtlinie ist an jeden einzelnen Mitgliedsstaat, dass Geräte nur dann in den Umlauf gebracht werden dürfen, wenn sie bei korrekter Verwendung die Sicherheit von Menschen und Nutztieren nicht gefährden. Im Gegenzug haben alle Mitgliedsstaaten die Verteilung der Produkte zu akzeptieren und ihre Stromnetze so zu führen, dass der sichere Betrieb gewährleistet ist.

2009/48/EG
Diese Richtlinie bezieht sich auf Produkte, die für Kinder unter 14 Jahren im privaten Umfeld, also nicht z.B. als Spielplatzgerät oder Spielautomat für eine Spielhalle, gedacht sind.

Die Sicherheit bezieht sich hier vor allem auf die Gesundheit der Kinder. Es werden Limits für chemische Zusammensetzungen und elektrische Höchstspannungen definiert, sowie der Umgang mit potentiell verschluckbaren Teilen.

2014/53/EU
Diese Richtlinie befasst sich mit dem Schutz der Gesundheit durch Regulierung des Niveaus an elektromagnetischer Strahlung. Ebenso sollen Funkfrequenzen wirksam und effizient genutzt werden. Der Fokus ist auch hier auf den freien Warenverkehr zwischen den EU Mitgliedsstaaten. Die Richtlinie umfasst auch alle Geräte mit W-LAN Modulen.

Eine umfassende Anleitung zur Prüfung und Umsetzung der passenden Richtlinien steht Herstellern in Form des „Blue Guide“ der EU zu Verfügung. [5]

Zwar nicht direkt in Verbindung mit Haushaltsgeräten, aber trotzdem relevant für den EU Markt, ist die General Data Protection Regulation (GDPR) [6] der Europäischen Union. In Österreich ist diese besser unter dem Namen Datenschutz-Grundverordnung (DSGVO) bekannt. Sie ist in Österreich im Datenschutzgesetz umgesetzt. [7] Die GDPR reguliert wichtige Elemente des Datenschutzes von Unternehmenskunden:

- Unternehmen sind angehalten die Verarbeitung von persönlichen Daten nach dem State of the Art durchzuführen.
- Informationen über Datendiebstahl müssen bekannt gegeben werden.
- Kunden haben ein Recht ihre Daten einzusehen, sowie vergessen zu werden.

- Daten müssen portabel sein, will man also von einem Service zu einem anderen wechseln, muss dies ohne Umstände funktionieren.
- Unternehmen dürfen nur die für den Zweck notwendigen Daten verarbeiten.

2. Optionale Prüfsiegel

2.1. TÜV-Austria

Der TÜV-Austria hat ein eigenes Prüfsiegel „Trusted IoT-Device“ erarbeitet, dieses Prüfsiegel kann für verschiedene Klassen von IoT-Geräten erworben werden. [8] Bei der Zertifizierung werden laut Datenblatt [9] u.a. folgende Elemente überprüft:

- Generelle Konzeptprüfung
  - Entwicklungsmethodologie
  - Entwicklungs- und Integrationsumgebung
  - Identitätsmanagement
  - Plattformspezifische Merkmale
  - Sicherung assoziierter Anwendungen/Dienste
  - Sicherung von Schnittstellen (APIs)
  - Sicherung von Updates
  - Crypto Key Management
  - Protokollierung
  - Reviews (continuous monitoring)
- Soft- und Hardwarearchitektur
- Technischer Datenschutz (Privacy)
- Datensicherheit

Das Zertifikat wird für bis zu drei Jahre ausgestellt, wobei das zertifizierte Produkt jedes Jahr erneut einem Test unterzogen wird.

2.2. TÜV Rheinland

Der TÜV Rheinland bietet ebenfalls Zertifikate an, wobei diese zwischen dem IoT-Produkt-Zertifikat und dem IoT-Service-Zertifikat unterscheiden. [10]
Ersteres bezieht sich auf Eigenschaften des Geräts selbst, wie Datenschutz, Verschlüsselung der Übertragung und Daten sowohl lokal als auch online, dazugehörige App und Datennutzung.
Zweiteres bezieht sich auf Eigenschaften der Herstellerfirma. Dazu zählt die Sicherheit der (Cloud-) Infrastruktur, Datenschutz, organisatorische Sicherheit, etablierte Prozesse und Dokumentation.

3. Entwürfe für IoT Sicherheitsstandards

3.1. ENISA

In der State of the Union Address von 2017 bekräftigte Jean-Claude Juncker, dass sich die Europäische Kommission seit 2015 um Standardisierung und Erhöhung der Cybersicherheit, unter anderem für die IoT-Entwicklung, bemüht. Auf Basis der „European Agency for Network and Information Security“ (ENISA) soll hierfür die „EU Cybersecurity Agency“ etabliert werden um Kompetenzen zu bündeln. [11]
Im November 2017 veröffentlichte die ENISA die „Baseline Security Recommendations for IoT“ [12]. Dieses Dokument entstand auf Basis von Expertenmeinungen und Nachforschungen über die aktuelle Bedrohungslage für IoT. Sensoren, Geräte- und Netzwerkmanagement, sowie Kommunikationsprotokolle und –Gateways wurden als die kritischsten Elemente des IoT Ökosystems identifiziert.

Basierend darauf beschreibt das Dokument die drei kritischsten Angriffsszenarien:

1. Kompromittierung der IoT Administration
2. Manipulation von Sensorwerten
3. Botnets und Command Injection Schachstellen

Daraus leitet die ENISA eine Reihe von Best Practices ab, welche in die Kategorien: Policies, organisatorische und technische Maßnahmen gegliedert werden.

In den Policies werden mehrere Maßnahmen zu Security- und Privacy by design, sowie Asset Management und Risiko- und Bedrohungsanalyse gestellt. Dazu zählen die Forderungen die Architektur so zu gliedern, dass Elemente im Angriffsfall abgeschottet sind, Privatsphäre Überlegungen vor dem Launch neuer Anwendungen angestellt werden oder der Verwendung von Defense-in-Depth Strategien zur Risikoerkennung.

Zu den organisatorischen Maßnahmen zählen die Entwicklung einer Strategie für das Ende des Produktlebenszyklus, die Verwendung von erprobten Lösungen, sowie ein restriktiver Umgang mit der Datenweitergabe an Dritte.

Die technischen Maßnahmen umfassen u.a. ein unveränderliches Root-of-Trust zu nutzen, Verwendung von kryptografisch signiertem Code oder die standardmäßige Aktivierung aller Sicherheitsfeatures bei gleichzeitiger Deaktivierung ungenutzter Features.

Wie bereits beschrieben handelt es sich hierbei ausschließlich um Empfehlungen, die derzeit in keiner Weise durch EU-Recht bindend sind. Eine vollständige und korrekte Umsetzung dieser Empfehlung würde jedoch die Sicherheit von IoT-Geräten erheblich verbessern.

3.2. U.S. „Internet of Things Cybersecurity Improvement Act of 2017“

Eine ähnliche Bestrebung fand auch in den U.S.A. in Form des „Internet of Things Cybersecurity Improvement Act of 2017“ statt. [13] Dieser stellt, kurzgefasst, die folgenden Forderungen:

- Ermöglichung von Patches für Geräte, Verwendung standardisierter Protokolle, keine fest gespeicherten Passwörter, Auslieferung nur ohne bekannten Schwachstellen.
- Erstellung eines schriftlichen Zertifikats durch den Hersteller, dass ein Gerät zum Zeitpunkt der Auslieferung über keine bekannten Schwachstellen verfügt und Schließung von später auftretenden Lücken in angemessener Zeit.
- Erstellung einer Richtlinie für die koordinierte Offenlegung von Schwachstellen durch Sicherheitsforscher.

Darüber hinaus stellt der „Internet of Things Cybersecurity Improvement Act of 2017“ auch einige Anforderungen für den Einsatz von IoT durch Regierungsbehörden.

3.3. ePrivacy Regulation

Nicht ausschließlich an IoT gerichtet, aber dennoch relevant, ist die geplante ePrivacy Regulation der Europäischen Union. Sie kann als Ergänzung zur GDPR verstanden werden und soll genau definierte Sicherheitsstandards für einige Bereiche, die IoT betreffen, bringen. Dazu zählt die Vertraulichkeit digitaler Kommunikation und die Sicherheit von Endbenutzergeräten für diese Kommunikation. Zu dem zweiten Aspekt zählt insbesondere die Wahrung der Integrität von Informationen, welche auf den Geräten gespeichert werden und der Schutz von Informationen, die von ihnen übertragen werden. Internet of Things ist im aktuellen Entwurf explizit genannt als Beispiel für ‚machine-to-machine‘ Kommunikation, welche auch durch die Regulierung abgedeckt werden soll. Ergänzend zur GDPR wird auch gefordert, dass Softwarehersteller Endnutzer unterstützen müssen informierte Entscheidungen darüber zu treffen, welche Daten sie teilen wollen. [14]

4. Sicherheitsstandards aus der Software- und Hardwareentwicklung

Von Seiten der IT Welt existieren bereits Richtlinien und Best Practices die gut für die Entwicklung von IoT-Geräten genutzt werden können. Es macht für Unternehmen Sinn sich mit diesen Standards zu befassen, da die auftretenden Sicherheitsrisiken in IoT-Geräten oftmals in Fehlern im Software Engineering begründet liegen.

Hier sei besonders der ISO/IEC 30141 [14] erwähnt, welcher eine vollständige Referenzarchitektur für IoT-Geräte bietet. In diesem wird in einem eigenen Kapitel auf sicherheitsrelevante Themen Bezug genommen.

Als genereller Standard für IT Sicherheit existiert der ISO/IEC 27002 [15]. Dieser bietet Richtlinien sowohl auf organisatorischer, als auch auf technischer Ebene für sichere Praktiken im Unternehmen. Diese nutzen vor allem der Unternehmensinfrastruktur in Verbindung mit ISO/IEC 27017 [16] um Cloud-Anbindungen für IoT-Geräte zu schützen.

Die folgende Tabelle gibt eine Aufzählung weiterer ISO Normen und ihrer Relevanz für die Entwicklung sicherer IoT-Geräte:

Norm	**Bedeutung**
27005	Generelle Richtlinien für den Umgang mit Risiken im Unternehmen.
29134	Richtlinien für das sogenannte „Privacy Impact Assessment“. Hierbei geht es darum die Auswirkungen auf die Privatsphäre durch ein Produkt oder einen Prozess festzustellen.
11770-3	In dieser Norm wird der Umgang mit kryptografischen Schlüsseln festgelegt. Dies ist besonders wichtig für IoT-Geräte, welche mit Herstellerclouds kommunizieren um das Abgreifen von persönlichen Daten zu verhindern.
30111	Festlegung von Prozessen für den Umgang mit Schwachstellen in bereits vermarkteten Produkten.
29100	Framework zur Wahrung der Privatsphäre durch Minimierung der gesammelten Daten und anderer Maßnahmen.
27033, 27034, 27040	Diese Normen beziehen sich auf die sichere Implementierung von beispielsweise einem Cloud-Backend zu einem IoT-Gerät hinsichtlich Netzwerk-, Anwendungs- und Speichersicherheit

Über ISO-Standards hinaus, gibt es auch weitere etablierte Richtlinien zur sicheren Entwicklung von Software. Microsoft stellt hierfür den Security Development Lifecycle (SDL) zu Verfügung. Dieser beinhaltet Best Practices für den gesamten Softwareentwicklungszyklus. [17] Als offene Initiative steht Firmen das Open Software Assurance Maturity Model (OpenSAMM) zu Verfügung. Es bietet Hilfestellungen im Bereich Führung, Entwicklung, Verifikation und Verteilung und soll dabei helfen in Zyklen sicherere Software auf den Markt zu bringen. [19]

Frei verfügbar stellt die ETSI hilfreiche Dokumente zu Verfügung. Im TR 103 305 [19] werden die Top 20 best practices für Unternehmen im Bereich der Cybersecurity beschrieben. Diese beziehen sich nicht nur auf IoT Entwicklung, können aber auch in diesem Bereich nützlich sein.

5. Beurteilung der Sicherheitsstandards

Um die unterschiedlichen Sicherheitsstandards zu bewerten, ist es notwendig zu verstehen, von welchen Schwachstellen IoT-Geräte am häufigsten betroffen sind. Gemeint sind hiermit potentielle Schwachstellen, die durch die Hinzugabe von IoT Fähigkeiten in einen bestehenden Gerätetyp entstehen. Dazu gibt es eine Top 10 Liste des „OWASP Internet of Things Project“. [21] Die Top 10 reihen sich wie folgt:

1. Schwache, erratbare oder fest vorgegebene Passwörter
2. Unsichere Netzwerkdienste (direkt am Gerät)

3. Unsichere Ökosystem Interfaces (in der Cloud)
4. Fehlen eines sicheren Update Mechanismus
5. Verwendung unsicherer oder veralteter Komponenten
6. Unzureichender Schutz der Privatsphäre
7. Unsichere Datenübertragung und/oder -speicherung
8. Fehlendes Device Management
9. Unsichere Standardeinstellungen
10. Mangel an physischer Härtung

Diese Top 10 beziehen sich auf IoT-Geräte im Allgemeinen. Punkt 8 ist für Haushaltsgeräte eher nicht relevant, dieser bezieht sich auf IoT-Geräte für den Unternehmenseinsatz. Alle anderen Punkte sind auch für Haushaltsgeräte relevant.

Die folgende Tabelle bietet einen kurzen Überblick über das Verhältnis einzelner Maßnahmen zu den 10 Punkten. Grün bedeutet dabei, dass ein Punkt abgedeckt ist. Gelb, dass es nicht sicher aus den zu Verfügung stehenden Unterlagen hervorgeht, jedoch vermutet wird und Rot, dass ein Punkt nicht abgedeckt ist.

Schwachstelle - Richtlinie	Passwörter	Netzwerkdienste	Ökosystem Interfaces	Update Mechanismus	Komponenten	Privatsphäre	Daten-handhabung	Device Management	Standard-einstellungen	Physische Härtung
CE										
GDPR										
TÜV – „Trusted IoT-Device“										
TÜV – IoT-Produkt Zertifikat										
TÜV – IoT-Service Zertifikat										
Baseline Security Recommendations										
IoT Cybersecurity Improvement Act										
ePrivacy Regulation										
Softwareentwicklungsstandards										

Die verpflichtenden Sicherheitsstandards der CE-Richtlinie haben keine Relevanz in der Prävention von Schwachstellen aus dem IoT Bereich. Sie beziehen sich ausschließlich auf Bedrohungen der Gesundheit der Anwender, im weitesten Sinn.

Die GDPR hat vor allem eine Auswirkung auf die Bedrohung durch unsichere Ökosystem Interfaces und unzureichenden Schutz der Privatsphäre. Sie fordert zwar auch das Einhalten des State of the Art von Herstellern, ist hierbei jedoch unspezifisch in der Umsetzung. Allenfalls reduziert sie die Verletzlichkeit der Privatsphäre von Anwendern indem sie die Datensammlung der Hersteller reduziert.

Die optionalen Prüfsiegel des TÜV-Austria, als auch jene des TÜV Rheinland adressieren, laut Beschreibung, alle Punkte bis auf Punkt 8. Sie befassen sich umfassend sowohl mit dem Design der Hard- und Software des Geräts, als auch der Infrastruktur, welche vom Unternehmen zu Verfügung gestellt wird. Auf Letztere legt der Rheinländische TÜV mit dem extra Siegel besonderen Wert. Die jährlich zu wiederholende Zertifizierung gibt dem Siegel extra Gewicht, da so erzwungen wird, dass auch eventuell neuauftretende Lücken in bestehenden Produkten geschlossen werden um die Zertifizierung aufrecht zu erhalten.

Die „Baseline Security Recommendations for IoT“ stellen einen sehr umfangreichen Leitfaden zur Absicherung von IoT-Geräten und dazugehöriger Infrastruktur dar. Sie stützen sich oftmals auf ISO Normen und Best Practices aus der Welt der Softwareprogrammierung. Somit decken sie alle Punkte ab.

Der „Internet of Things Cybersecurity Improvement Act of 2017“ deckt alle Punkte, die die Geräte selbst und die dazugehörige Cloud betreffen mit Ausnahme von Punkt 8, explizit ab. Er richtet sich jedoch nicht an den Schutz der Privatsphäre der Anwender oder die sichere Speicherung von Daten.

Die ePrivacy Regulation der EU liegt derzeit als Entwurf vor und kann daher nicht endgültig beurteilt werden. Sie fordert Sicherheit sowohl bei der Kommunikation, als auch von den Endnutzergeräten. Hinsichtlich IoT besteht ein besonderer Fokus auf die Datenübertragung von Geräten untereinander. Es ist aus dem Entwurf nicht klar, ob mit Geräten auch die Herstellerclouds gemeint sind, oder ob sich dies ausschließlich auf IoT-Geräte untereinander bezieht. In letzterem Fall erscheint die Wirkung aus heutiger Sicht eher gering, da die Datenübertragung nahezu gänzlich zwischen den Clouddiensten abgewickelt wird.

Die Sicherheitsstandards aus der Softwareentwicklung decken zusammen alle Bereiche der genannten Schwachstellenkategorien ab. Besonders der ISO/IEC 30141 bietet eine umfangreiche Richtlinie für die sichere Entwicklung von IoT-Geräten. Sieht man von Punkt 10 ab, sind alle der genannten Schwachstellen bereits durch Best Practices, Coding Standards und Richtlinien aus der IT Entwicklung und Administration abgedeckt. Es kommt im Einzelnen nicht mehr darauf an, ob für ein Projekt ein Framework wie der Security Development Lifecycle von Microsoft herangezogen wird, oder passenden ISO Standards gefolgt wird.

6. Zusammenfassung

In dieser Arbeit wurden verschiedene Sicherheitsstandards, sowohl rechtlich bindend, als auch optional aufgezählt.

Rechtlich bindend existiert derzeit ausschließlich das CE-Siegel, welches jedoch keinen Bezug zur Sicherheit im Rahmen von IoT Funktionalitäten hat.

Grundsätzlich existiert bereits eine Fülle an Richtlinien und Best Practices zur Entwicklung sicherer IT-Produkte, die direkt auf IoT anwendbar sind. Diese kommen vor allem aus der Welt der Softwareentwicklung und sind in Form von ISO Normen und Frameworks umsetzbar.

Es existieren bereits Prüfsiegel wie jene des TÜV-Austria und TÜV Rheinland. Solche unabhängigen Prüfsiegel stärken das Vertrauen in die Sicherheit von IoT-Geräten.

Die ePrivacy Regulation der Europäischen Union enthält zumindest in der aktuellen Fassung einige Punkte, die zu besserem Datenschutz bei IoT-Geräten beitragen sollen. Gleiches gilt für den „Internet of Things Cybersecurity Improvement Act of 2017“ aus den U.S.A..

Referenzen

[1] EU, „Richtlinie 2012/27/EU des Europäischen Parlaments und des Rates vom 25. Oktober 2012 zur Energieeffizienz,“ [Online]. Available: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32012L0027. [Zugriff am 05 02 2019].

[2] EU, „Richtlinie 2014/35/EU des Europäischen Parlaments und des Rates vom 26. Februar 2014 zur Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung elektrischer Betriebsmittel zur Verwendung innerhalb bestimmter Spannungsgrenzen auf,“ [Online]. Available: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32014L0035. [Zugriff am 28 01 2019].

[3] EU, „Richtlinie 2009/48/EG des Europäischen Parlaments und des Rates vom 18. Juni 2009 über die Sicherheit von Spielzeug (Text von Bedeutung für den EWR),“ [Online]. Available: https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:32009L0048. [Zugriff am 28 01 2019].

[4] EU, „Richtlinie 2014/53/EU des Europäischen Parlaments und des Rates vom 16. April 2014 über die Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung

von Funkanlagen auf dem Markt," [Online]. Available: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32014L0053. [Zugriff am 28 01 2019].

[5] EC, „DocsRoom," [Online]. Available: http://ec.europa.eu/DocsRoom/documents/18027. [Zugriff am 28 01 2019].

[6] EU, „Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordn," [Online]. Available: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32016R0679. [Zugriff am 04 02 2019].

[7] RIS, „Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten - BGBl. I Nr. 165/1999," [Online]. Available: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001597. [Zugriff am 04 02 2019].

[8] TÜV-Austria, „Prüfung und Zertifizierung von IoT-Devices," [Online]. Available: https://it-tuv.com/leistungen/zertifizierungen/pruefung-und-zertifizierung-von-iot-devices/. [Zugriff am 30 01 2019].

[9] TÜV-Austria, „TTI_Datenblatt_Prüfung-und-Zertifizierung-von-IoT-Devices.pdf," [Online]. Available: https://it-tuv.com/wp-content/uploads/2017/08/TTI_Datenblatt_Pru%CC%88fung-und-Zertifizierung-von-IoT-Devices.pdf. [Zugriff am 30 01 2019].

[10] TÜV-Rheinland, „IoT Privacy - Zertifikate," [Online]. Available: https://www.tuv.com/landingpage/de/iot-privacy/main-navigation/zertifikate/. [Zugriff am 30 01 2019].

[11] EC, „Press release - State of the Union 2017," [Online]. Available: http://europa.eu/rapid/press-release_IP-17-3193_en.htm. [Zugriff am 29 01 2019].

[12] ENISA, „Baseline Security Recommendations for IoT," [Online]. Available: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot. [Zugriff am 29 01 2019].

[13] Congress.gov, „Internet of Things (IoT) Cybersecurity Improvement Act of 2017," [Online]. Available: https://www.congress.gov/bill/115th-congress/senate-bill/1691. [Zugriff am 28 01 2019].

[14] EC, „Proposal for a Regulation on Privacy and Electronic Communications," [Online]. Available: https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications. [Zugriff am 06 02 2019].

[15] ISO, „ISO/IEC 30141:2018(en), Internet of Things (IoT)," [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:30141:ed-1:v1:en. [Zugriff am 31 01 2019].

[16] ISO, „ISO/IEC 27002:2013(en), Information technology - Security techniques - Code of practice for information security controls," [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en. [Zugriff am 31 01 2019].

[17] ISO, „ISO/IEC 27017:2015(en), Information technology - Security techniques - Code of practice for information controls based on ISO/IEC 27002 for cloud services," [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27017:ed-1:v1:en. [Zugriff am 31 01 2019].

[18] Microsoft, „Microsoft Security Development Lifecycle," [Online]. Available: https://www.microsoft.com/en-us/securityengineering/sdl/. [Zugriff am 31 01 2019].

[19] OWASP, „Software Assurance Maturity Model (SAMM): A guide to building security into software development," [Online]. Available: https://www.opensamm.org/. [Zugriff am 01 02 2019].

[20] ETSI, „TR 103 305 - V1.1.1 - CYBER; Critical Security Controls for Effective Cyber Defence," [Online]. Available: https://www.etsi.org/deliver/etsi_tr/103300_103399/103305/01.01.01_60/tr_103305v010101p.pdf. [Zugriff am 01 02 2019].

[21] OWASP, „OWASP Internet of Things Project,“ [Online]. Available: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project. [Zugriff am 12 02 2019].