Active Era

Kontaktierte Server

App

- https://api.share.mob.com:443
  - 111.47.226.190
- https://devs.data.mob.com:443
  - 116.211.155.244
- https://api.config.sentinel.mob.com:443
  - 61.174.10.205
- https://f.gm.mob.com:443
  - 116.211.155.249
- https://l.gm.mob.com:443
  - 116.211.155.227
- https://plbslog.umeng.com:443
  - 203.119.215.106
  - IP gehört zu Alibaba
- https://ulogs.umeng.com:443
  - 203.119.214.125
  - IP gehört zu Alibaba
- https://online.fitdays.cn:443
  - 47.106.233.152
  - IP gehört zu Alibaba

Kontaktierte Geräte im Heimnetzwerk

Es wird lediglich die Waage per Bluetooth kontaktiert.

Häufigkeit und Größe der Übertragungen

Während der Verwendung der App werden Daten von/zu den oben angeführten Servern empfangen/gesandt.

Personenbezogene Daten

Es wurde die Übermittlung der folgenden personenbezogenen Daten festgestellt:
Alle bei der Anmeldung angegebenen Daten wie Nickname, Geburtsdatum, Geschlecht, Größe, Zielgewicht, Foto (optional), E-Mail.

Weiters die Daten der Messungen wie Gewicht, BMI, Körperfett, Fettabbau, Subkutanes Fett, Viszerales Fett, Körperwasser, Skelettmuskulatur, Muskelmasse, Knochenmasse, Protein %, BMR (Grundumsatzrate), Körperalter.

Test, ob ein Blocken der Verbindung die Funktionalität der IoT-Geräte einschränkt

Nach der erstmaligen Registrierung und Anmeldung funktioniert die App auch ohne eine Netzwerkverbindung. Eine Bluetooth Verbindung zu der Körperfettwaage wird zur Nutzung der App benötigt.

Vergleich der von den Herstellern angegebenen Datenschutz Informationen mit den tatsächlich erhobenen Daten

In der App ist eine deutsche Übersetzung der folgende Datenschutzrichtlinie enthalten: https://activeera.com/app-privacy-policy/

Der Hersteller gibt an im Rahmen der Nutzung des Produkts, (unter anderem) folgende personenbezogene Daten zu verarbeiten:

- Geburtsdatum
- Körpergröße
- Geschlecht
- andere körperbezogene Daten

Darüber hinaus wird die E-Mail-Adresse erhoben.

Der Hersteller weist darauf hin, dass standortbezogene Mobilfunkdienste zur Nutzung von Bluetooth-Funktionen notwendig ist. Der Hersteller gewährt, dass "[...] ihre standortbezogenen Dienste für keine andere Zwecke verwendet oder an Dritte weitergegeben werden."

Der Hersteller gibt an, zusätzliche personenbezogene Daten aus Quellen wie sozialen Medien, öffentlich verfügbaren Datenbanken oder bei anderen Anlässen, wenn Sie ihre Dienste nutzen, erfassen zu können.

> "We may gather additional Personal Data from sources such as Social Media, publicly available databases or on other occasions when you use our services." (Abschnitt 01)

Amazon Echo Dot

Kontaktierte Server

App

- https://account.api.here.com:443
  - 54.75.3.151
- https://direct.data.api.platform.here.com:443
  - 54.72.141.227
- https://cognito-identity.us-east-1.amazonaws.com:443
  - 107.23.139.90
  - 34.206.7.236
- https://kinesis.us-east-1.amazonaws.com:443
  - 3.227.250.203
  - 3.227.250.191
  - 3.91.171.128
  - 3.227.250.175
  - 3.227.250.197
  - 3.227.250.162
  - 3.91.171.153
  - 3.227.250.224
  - 3.227.250.254
  - 3.227.250.150
  - 3.91.171.217
  - 3.227.250.177
  - 3.91.171.132
  - 3.91.171.253
  - 3.227.250.155
  - 3.91.171.228
  - 3.91.171.233
  - 3.91.171.226
  - 3.91.171.152
- https://alexa.amazon.de:443

    - 13.32.1.72
- https://bugsnag-session.monitor.core.app.alexa.a2z.com:443
    - 52.26.249.41
    - 54.187.217.108
- https://www.amazon.de:443
    - 13.32.2.182
- https://images-eu.ssl-images-amazon.com:443
    - 151.101.189.16
- https://fls-eu.amazon.com:443
    - 34.252.249.200
- https://static.siege-amazon.com:443
    - 99.86.241.82
    - 99.86.241.8
- https://m.media-amazon.com:443
    - 151.101.189.16
- https://images-na.ssl-images-amazon.com:443
    - 13.32.13.69
    - 151.101.189.16
    - 184.51.8.71
- https://unagi.amazon.de:443
    - 54.239.32.228
    - 54.239.35.28
- https://arcus-uswest.amazon.com:443
    - 52.119.168.148
- https://cognito-identity.eu-west-1.amazonaws.com:443
    - 52.19.39.231
    - 54.74.121.124
- https://kinesis.eu-west-1.amazonaws.com:443
    - 99.80.34.182
    - 99.80.34.228
    - 99.80.34.157
    - 99.80.34.198

- https://alexa-comms-mobile-service.amazon.com:443
  - 13.32.134.236
- https://fls-eu.amazon.de:443
  - 54.220.148.161
- https://update.googleapis.com:443
  - 142.250.185.195
  - 142.250.185.99
- https://amazoncustomerservice.d2.sc.omtrdc.net:443
  - 44.237.54.118
- https://aax-eu.amazon-adsystem.com:443
  - 52.95.123.41
- https://completion.amazon.co.uk:443
  - 52.95.122.8
- https://unagi-eu.amazon.com:443
  - 54.239.32.228
- https://device-metrics-us-2.amazon.com:443
  - 52.94.234.57
- https://api.amazonalexa.com:443
  - 13.226.88.211
- https://avs-alexa-13-na.amazon.com:443
  - 52.94.227.146
- https://device-artifacts-v2.s3.amazonaws.com:443
  - 52.216.79.36
- https://api.eu.amazonalexa.com:443
  - 13.32.13.188
- https://dynamic-ui-service-eu.amazon.com:443
  - 52.95.118.220
- https://cdn-profiles.tunein.com:443
  - 104.17.58.239
- https://cdn-radiotime-logos.tunein.com:443
  - 104.17.57.239

- https://d1tjc249f8pnut.cloudfront.net:443
  - 99.86.245.199
- https://dss-na.amazon.com:443
  - 54.239.19.122
  - 52.94.237.71
- http://192.168.11.1:8080
- http://10.201.126.241:8080
- https://unagi-eu.amazon.com:443
  - 52.95.124.221
- https://endpoint.prod.eu-west-1.forester.a2z.com:443
  - 18.203.121.160

Echo Dot

- 52.95.122.231:443
  - TLSv1.2
  - IP gehört Amazon
- d2lg00fehdyg04.cloudfront.net
  - 13.32.14.149:443
- ffs-provisioner-config.amazon-dss.com
  - 13.32.2.75:443
- d90nnyvqgmkzx.cloudfront.net
  - 13.32.13.188:443
- d1gsg05rq1vjdw.cloudfront.net
  - 13.226.88.211:443
- fireoscaptiveportal.com
  - HTTP
  - 18.233.77.176:80
  - 18.205.179.227:80
  - 34.202.117.170:80
  - 34.225.63.25:80
  - 35.168.254.2:80
  - 54.175.35.223:80
  - 54.225.95.62:80

    - 35.172.9.94:80
    - 52.20.118.176:80
    - /generate_204
        - reply HTTP 204
- discovery.meethue.com
    - 34.95.100.122:443
- ingestion.us-east-1.prod.arteries.alexa.a2z.com
    - 52.22.198.112:443
- api.amazon.com
    - 52.46.128.39:443
    - 52.46.158.193:443
    - 52.94.240.240:443
    - 52.94.241.146:443
    - 54.239.26.244:443
    - 54.239.29.142:443
- device-metrics-us-2.amazon.com
    - 52.119.196.173:443
    - 52.119.197.180:443
    - 52.46.128.104:443
    - 52.46.145.63:443
    - 52.46.147.153:443
    - 52.46.147.155:443
    - 52.46.147.157:443
    - 52.46.147.159:443
    - 52.46.148.84:443
    - 52.46.148.87:443
    - 52.46.155.115:443
    - 52.46.155.138:443
    - 52.46.155.145:443
    - 52.46.155.159:443
    - 52.94.228.117:443
    - 52.94.228.74:443
    - 52.94.231.53:443
    - 52.94.234.57:443

    - 52.94.235.78:443
    - 52.94.243.170:443
    - 52.94.243.192:443
- todo-ta-g7g.amazon.com
    - 52.46.133.19:443
- msh.amazon.com
    - 52.46.145.179:443
- updates.amazon.com
    - 52.46.155.120:443
- prod.amcs-tachyon.com
    - 52.73.73.87:443
- dss-na.amazon.com
    - 52.94.224.149:443
- det-ta-g7g.amazon.com
    - 52.94.231.222:443
- 52.95.113.144:443
    - TLSv1.2
    - IP gehört Amazon
- bob-dispatch-prod-eu.amazon.com
    - 52.95.115.208:443
    - 52.95.119.186:443
    - 52.95.121.5:443
- arcus-uswest.amazon.com
    - 52.119.168.148:443
- s3-1-w.amazonaws.com
    - HTTP
    - /wifistub.html
    - Reply
        - HTML Seite mit UUID
    - 52.216.17.224:80
    - 52.216.100.11:80
    - 52.216.106.11:80

- 52.216.109.163:80
- 52.216.113.83:80
- 52.216.114.203:80
- 52.216.130.235:80
- 52.216.136.148:443
- 52.216.137.164:80
- 52.216.137.44:80
- 52.216.138.67:80
- 52.216.140.220:80
- 52.216.142.108:80
- 52.216.145.123:80
- 52.216.146.11:80
- 52.216.146.123:80
- 52.216.152.188:80
- 52.216.152.84:80
- 52.216.164.211:80
- 52.216.165.219:80
- 52.216.168.195:80
- 52.216.17.192:80
- 52.216.171.147:443
- 52.216.186.11:80
- 52.216.186.187:80
- 52.216.226.128:443
- 52.216.239.179:80
- 52.216.248.28:80
- 52.216.28.116:80
- 52.216.29.92:80
- 52.216.8.139:80
- 52.216.8.235:80
- 52.216.80.128:80
- 52.216.80.8:80
- 52.216.92.11:80
- 52.216.99.67:80
- 52.217.10.180:80
- 52.217.105.36:80

    - 52.217.107.44:80
    - 52.217.108.164:80
    - 52.217.108.228:80
    - 52.217.11.12:80
    - 52.217.111.228:80
    - 52.217.111.52:80
    - 52.217.16.172:80
    - 52.217.16.4:80
    - 52.217.192.33:80
    - 52.217.193.193:80
    - 52.217.33.76:443
    - 52.217.34.52:80
    - 52.217.36.100:80
    - 52.217.40.76:80
    - 52.217.42.132:80
    - 52.217.42.220:443
    - 52.217.42.220:80
    - 52.217.42.244:80
    - 52.217.44.148:80
    - 52.217.46.220:80
    - 52.217.48.204:80
    - 52.217.48.244:80
    - 52.217.49.84:80
    - 52.217.64.84:80
    - 52.217.67.20:80
    - 52.217.70.220:80
    - 52.217.72.108:80
    - 52.217.74.92:80
    - 52.217.78.68:80
    - 52.217.79.196:80
    - 52.217.84.116:80
    - 52.217.85.68:80
    - 52.217.92.44:80
- s3-r-w.eu-west-1.amazonaws.com

    - 52.218.62.56:443
- dcape-na.amazon.com
    - 72.21.195.82:443
- ec2-72-44-33-234.compute-1.amazonaws.com
    - 72.44.33.234:443
- d1s31zyz7dcc2d.cloudfront.net
    - 99.86.245.134:443
- www.googleapis.com
    - 142.250.185.106:443
    - 142.250.185.202:443
- 239.255.255.250
    - SSDP
    - Sucht per SSDP Discover nach UPnP Geräten im Netzwerk
    - Ungefähr alle 2 Stunden

Kontaktierte Geräte im Heimnetzwerk

Die App kontaktiert keine Geräte im Heimnetzwerk außer das Gateway.

Der Amazon Echo Dot schickt ungefähr alle 2 Stunden SSDP Discover Pakete aus, um UPnP Geräte im Netzwerk zu finden. Es wurden keine Antworten aufgezeichnet. Es wurden ansonsten keine Geräte im Heimnetzwerk kontaktiert.

Häufigkeit und Größe der Übertragungen

Der Amazon Echo Dot überträgt/sendet während der Verwendung und im Standby regelmäßig Daten an die oben angeführten Server. Die verschlüsselt übertragenen Daten des Echo Dot konnten nicht genauer geprüft werden. Es werden ebenfalls unverschlüsselt Daten zu fireoscaptiveportal.com und s3-1-w.amazonaws.com per HTTP gesandt. Bei diesen Anfragen werden keine personenbezogenen Daten übertragen.

Die App sendet und empfängt während der Verwendung Daten von/zu den oben angeführten Servern. Es werden ebenfalls HTTP Anfragen an die internen IP-Adressen 192.168.11.1 Port 8080 und 10.201.126.241 Port 8080 gesandt. Da der Pfad `/OOBE` abgerufen wird, scheint es sich um Anfragen für ein Out of Box Experience (OOBE) Setup zu handeln.

Personenbezogene Daten

Bei der Registrierung wurde der Name, die E-Mail-Adresse und das Passwort verschlüsselt an www.amazon.de übermittelt.

Die Übermittlung anderer personenbezogener Daten konnte nicht festgestellt werden.

Test, ob ein Blocken der Verbindung die Funktionalität der IoT-Geräte einschränkt

Die App und der Amazon Echo Dot benötigen eine Internetverbindung um die Funktionalität bereitstellen zu können.

Ein Blocken der Verbindung zu anderen Netzwerkgeräten per AP Isolation stellt keine Beeinträchtigung dar.

Vergleich der von den Herstellern angegebenen Datenschutz Informationen mit den tatsächlich erhobenen Daten

In der App ist folgende Datenschutzübersicht verlinkt:
https://www.amazon.de/gp/help/customer/display.html?nodeId=GA7E98TJFEJLYSFR&ref=kinw_myk_alxa_prvcy_de

In der App ist folgende Datenschutzrichtlinie verlinkt:
https://www.amazon.de/gp/help/customer/display.html?nodeId=3312401

Die während des Tests übermittelten personenbezogenen Daten sind in der Datenschutzerklärung vermerkt.

Anmerkungen

Die Anmeldung in der App wird per Certificate Pinning geschützt.

Nach der Anmeldung in der App wird die Signatur der App überprüft und der Zugriff auf Sprachfunktionen blockiert, wenn diese verändert wurde. Es ist ebenfalls nicht möglich den Echo Dot mit der App zu verbinden. Ob die Prüfung innerhalb der App oder serverseitig durchgeführt wird, ist nicht bekannt. Der weitere Datenverkehr der App konnte daher nicht geprüft werden.

HomeWizard Kitchen

Kontaktierte Server

App

- https://firebaseinstallations.googleapis.com:443
  - 142.250.186.170
- https://settings.crashlytics.com:443
  - 142.250.185.163
- https://api.homewizardeasyonline.com:443
  - 149.210.157.15
  - Reverse DNS: 149-210-157-15.colo.transip.net
- https://mailing.homewizard.com:443
  - 130.211.19.42
  - Reverse DNS: 42.19.211.130.bc.googleusercontent.com
- https://kitchen.homewizard.com:443
  - 35.186.255.246
  - Reverse DNS: 246.255.186.35.bc.googleusercontent.com
- https://push.homewizard.com:443
  - 34.98.115.45
  - Reverse DNS: 45.115.98.34.bc.googleusercontent.com

Aerofryer

- m.cloud.homewizard.com:443
  - 35.195.146.4

Kontaktierte Geräte im Heimnetzwerk

Es werden keine Geräte im Heimnetzwerk kontaktiert, außer dem Gateway.

Häufigkeit und Größe der Übertragungen

Der Aerofryer baut eine Verbindung zu m.cloud.homewizard.com Port 443 via TCP auf und hält diese Verbindung aufrecht. Es könnte sich daher um eine Websockets Verbindung handeln. Es werden ungefähr alle 5 Sekunden kleine Pakete (< 100 Byte) gesandt und empfangen. Dies deutet auf Websocket Ping/Pong Nachrichten hin. Meist wird zusätzlich eine Nachricht von ungefähr 600 - 900 Byte von dem Aerofryer an m.cloud.homewizard.com geschickt, jedoch nicht immer.

Die App überträgt während der Registrierung und der Anmeldung Daten zu api.homewizardeasyonline.com. Zur Interaktion mit dem Aerofryer wird eine Websockets Verbindung zu kitchen.homewizard.com aufgebaut und die zur Steuerung notwendigen Befehle geschickt, beziehungsweise Daten wie etwa verfügbare Geräte abgefragt.

Personenbezogene Daten

Bei der Registrierung werden E-Mail-Adresse und Name übertragen.

Test, ob ein Blocken der Verbindung die Funktionalität der IoT-Geräte einschränkt

Der Aerofryer benötigt eine Internetverbindung, um mit der Smartphone App bedient werden zu können. Ein Blocken der Internetverbindung verhindert die Bedienung per App, jedoch ist die Bedienung am Gerät selbst weiterhin möglich.

Ein Blocken der Verbindung zu anderen Netzwerkgeräten per AP Isolation stellt keine Beeinträchtigung dar.

Vergleich der von den Herstellern angegebenen Datenschutz Informationen mit den tatsächlich erhobenen Daten

Während der Registrierung eines Accounts in der App kann man über einen Link die "Geschäftsbedingungen" lesen und wird zu der Datenschutzrichtlinie weitergeleitet: https://www.homewizard.de/datenschutz

Die Angaben in der Datenschutzrichtlinie beziehen sich auf die Benutzung der Website und auf Bestellungen und gehen weder auf die App noch auf den Aerofryer ein.

Anmerkungen

Das Passwort kann nicht selbst vergeben werden. Es wird von HomeWizard generiert und anschließend per E-Mail zugesandt.

Kamtron Wireless IP Camera

Kontaktierte Server

App

- http://52.8.41.82:7080
  - Reverse DNS: ec2-52-8-41-82.us-west-1.compute.amazonaws.com.
- https://us11.mipcm.com:4443
  - 209.133.197.234
- http://209.133.197.234:4080
- 54.39.133.183:6030
  - UDP
  - Video Stream
  - Reverse DNS: ovca17.vimtag.com
- 54.157.82.107:7654
  - UDP
  - schickt 10 0x00 Bytes
  - Reverse DNS: ec2-54-157-82-107.compute-1.amazonaws.com.

Kamera

- 54.39.133.183:6030
  - UDP
  - Video Stream
  - Reverse DNS: ovca17.vimtag.com
- 54.39.133.19
  - TCP 4001
  - TCP 4024
  - ICMP (Ping)
  - Reverse DNS: ovca14.vimtag.com.
- 54.157.82.107:7654
  - UDP
  - schickt 10 0x00 Bytes
  - Reverse DNS: ec2-54-157-82-107.compute-1.amazonaws.com.

- 209.133.213.170
  - TCP 7001

Kontaktierte Geräte im Heimnetzwerk

App und Kamera stellen keine Verbindung zu Geräten im Heimnetzwerk außer dem Gateway her.

Die App versucht über die öffentliche IP-Adresse eine Verbindung zur Kamera herzustellen.

Häufigkeit und Größe der Übertragungen

Die App überträgt und empfängt während der Verwendung Daten zu den oben genannten Servern. Die Befehle zur Steuerung der Kamera und Gerätestatistiken werden an us11.mipcm.com:4443 per HTTPS übertragen.

Die Kamera schickt kurz nach dem Start einige KB Daten an 54.39.133.19 Port 4100 per TCP, danach ungefähr jede Minute kleinere Pakete (ca. 200 Byte).

Personenbezogene Daten

Bei der Registrierung werden Benutzername und Passwort übermittelt.

Test, ob ein Blocken der Verbindung die Funktionalität der IoT-Geräte einschränkt

Die Internetverbindungen werden für die Funktionalität der App und der Kamera benötigt.

Ein Blocken der Verbindung zu anderen Netzwerkgeräten per AP Isolation stellt keine Beeinträchtigung dar.

Vergleich der von den Herstellern angegebenen Datenschutz Informationen mit den tatsächlich erhobenen Daten

In der App wird die folgende Datenschutzrichtlinie geladen:
http://www.mipcm.com/disclaim/mipc/appyszcen.html

Personenbezogene Daten werden in der Datenschutzrichtlinie relativ breit definiert und inkludieren beispielsweise den Webbrowsertyp, Seitennavigation und diverse Gerätedaten.

Der Hersteller gibt an, bei der Registrierung Name, Telefonnummer und E-Mail-Adresse zu erheben. Bei der Aktivierung eines Produktes werden diverse Produktinformationen wie Seriennummer, Produktname, etc. gesammelt. Bei Benutzung der Aufnahme- oder Streamfunktionen können Video- und/oder Audiodaten des jeweiligen Produkts gespeichert und verarbeitet werden.

Kyvol Saugroboter

Kontaktierte Server

App

- https://android.bugly.qq.com:443
  - 129.226.103.217
  - 129.226.103.12
  - TLSv1.2
- a1.tuyaeu.com:443
  - 35.157.23.213
  - 18.194.156.95
  - 35.156.121.251
  - TLSv1.2
- h1.iot-dns.com:443
  - 52.27.85.79
  - TLSv1.2
- m1.tuyaeu.com:8883
  - 18.196.142.136
  - 18.194.10.142
  - secure-mqtt
  - TLSv1.2
- www.iotmsc.cn:10080
  - 112.74.107.164
  - TLSv1.2
- c.sayhi.360.cn:80
  - 112.65.70.244
- h.appjiagu.com:80
  - 180.163.249.200

Saugroboter

- 255.255.255.255:6667
  - UDP

    - verschlüsselt
- m2.tuyaeu.com:8886
    - 18.185.31.196
    - 3.120.92.134
    - 52.58.249.45
    - TLSv1.2
- a3.tuyaeu.com:443
    - 3.121.131.36
    - TLSv1.2

Kontaktierte Geräte im Heimnetzwerk

Der Saugroboter schickt ungefähr alle 5 Sekunden eine Broadcast Nachricht per UDP an den Port 6667. Die Nachricht ist verschlüsselt und scheint von Tuya für die Geräteerkennung verwendet zu werden.

Häufigkeit und Größe der Übertragungen

Nach dem Starten des Saugroboters wurden zuerst mehrere Pakete an m2.tuyaeu.com Port 8886 verschlüsselt via TLSv1.2 gesandt. Insgesamt wurden hierbei ca. 5,4 KiB übertragen.

Danach wurden mehrere Pakete an a3.tuyaeu.com Port 443 verschlüsselt mit TLSv1.2 übertragen. Insgesamt wurden hierbei ca. 5,7 KiB übertragen.

Der Saugroboter schickt ungefähr alle 5 Sekunden eine Broadcast Nachricht per UDP an den Port 6667. Die Nachricht ist verschlüsselt und scheint von Tuya für die Geräteerkennung verwendet zu werden.

Ungefähr jede Minute nach dem Startup sendet der Saugroboter 123 Byte Daten an m2.tuyaeu.com Port 8886 und empfängt eine Antwort mit ebenfalls 123 Byte. Beide Pakete sind per TLSv1.2 verschlüsselt.

Ungefähr alle 25 Minuten baut der Saugroboter eine mit TLSv1.2 verschlüsselte Verbindung zu a3.tuyaeu.com wobei ca. 1,5 KiB Daten übertragen werden.

Während der Bedienung sendet und empfängt der Saugroboter Daten an/von m2.tuyaeu.com Port 8886. Es scheint das MQTT Protokoll verwendet zu werden.

Während der Verwendung der App werden Daten verschlüsselt zu/von a1.tuyaeu.com Port 443 und m1.tuyaeu.com Port 8883 gesandt/empfangen.

Bei der Registrierung wurde eine verschlüsselte Verbindung zu www.iotmsc.cn Port 10080 aufgebaut. Nach dem Starten der App wurden verschlüsselte Verbindungen zu h1.iot-dns.com Port 443 und android.bugly.qq.com Port 443 aufgebaut. Während die App geöffnet ist, wird ungefähr alle 5 Minuten ein HTTP POST Request an c.sayhi.360.cn/pkl16.html gesandt. Dabei werden Daten in einem Binärformat übertragen und ebenfalls Daten in Binärformat empfangen.

Einmal wurde nach dem Starten der App eine HTTP Verbindung zu h.appjiagu.com festgestellt. Dabei wurde ein HTTP POST Request an /logctrl mit möglicherweise Base64 encodierten Daten übertragen. Die empfangenen Daten besitzen mit hoher Wahrscheinlichkeit die selbe Codierung. Die Domain enthält den Namen des Packers Jiagu, welcher bei der Android App verwendet wurde.

Personenbezogene Daten

Bei der Registrierung werden die E-Mail-Adresse und das Land abgefragt.

Die meisten Pakete werden verschlüsselt übertragen und konnten nicht inspiziert werden, da die Inspektion des Datenverkehrs aufgrund des verwendeten Jiagu Packers nicht möglich war.

Test, ob ein Blocken der Verbindung die Funktionalität der IoT-Geräte einschränkt

Der Kyvol E20 Saugroboter benötigt eine Internetverbindung um mit der Smartphone App bedient werden zu können. Ein Blocken der Internetverbindung verhindert die Bedienung per App, jedoch ist die Bedienung via mitgelieferter Fernbedienung weiterhin möglich.

Ein Blocken der Verbindung zu anderen Netzwerkgeräten per AP Isolation stellt keine Beeinträchtigung dar.

Vergleich der von den Herstellern angegebenen Datenschutz Informationen mit den tatsächlich erhobenen Daten

In der App ist die folgende Datenschutzrichtlinie verlinkt:
https://kyvol.com/pages/app_privacy-policy/de

Die während des Tests übermittelten personenbezogenen Daten sind in der Datenschutzerklärung vermerkt.

Informationen zur Datenschutzerklärung

Der Hersteller gibt an bei der Registrierung die Kontaktdaten wie beispielsweise E-Mail-Adresse, Telefonnummer und Benutzernamen zu erfassen. Weiters könnten Nickname, Profilbild, Ländercode, Sprachpräferenz oder Zeitzone erfasst werden.

Folgende Daten werden automatisch erfasst:

- Geräteinformationen wie MAC-Adresse, IP-Adresse
- Nutzungsdaten von Sites und Diensten
- System- und Ausnahmeprotokolle bei App Nutzung
- Standortinformationen bei speziellen Produkten wie beispielsweise Reinigungsrobotern.

Intelligente Geräte übertragen folgende Daten:

- Grundlegende Informationen wie Gerätename, ID, Onlinestatus, Aktivierungszeit, Firmware-Version und Aktualisierungsinformationen
- Gemeldete Informationen

- Je nach Gerät könnten unterschiedliche Informationen erfasst werden. Zum Beispiel kann ein Reinigungsroboter den **Reinigungsbereich** melden.

Medion MD 18861

Kontaktierte Server

App

- https://ums.pl.prod.iot.robart.cc:443
  - 46.51.140.185
  - Amazon
- https://eu.ums.pl.prod.iot.robart.cc:443
  - 46.51.140.185
  - Amazon
- https://eu.pl.prod.iot.robart.cc:443
  - 46.51.140.185
  - Amazon
- stage.iot.robart.cc
  - ICMP Echo

Roboter

- pl.prod.iot.robart.cc:443
- update.fw.robart.cc:443

Kontaktierte Geräte im Heimnetzwerk

Der Roboter meldet seine eigenen Dienste per MDNS Multicast an die IP-Adresse 224.0.0.251, welche von anderen Geräten im Heimnetzwerk empfangen werden, wenn diese sich für Nachrichten dieser IP-Adresse angemeldet haben.

Die gemeldeten Services sind:

- SSH und SFTP auf Port 22
- HTTP auf Port 10009

Weiters scheint der selbe Webserver von Port 10009 auf via HTTPS auf Port 443 erreichbar zu sein.

Es wurden keine Zugriffe auf diese Services festgestellt.

Häufigkeit und Größe der Übertragungen

Der Roboter hält während er in Betrieb ist eine mit TLSv1.2 verschlüsselte Verbindung zu pl.prod.iot.robart.cc und update.fw.robart.cc aufrecht.

Die App schickt während der Einrichtung regelmäßig ICMP Ping Nachrichten an stage.iot.robart.cc

Während der Verwendung schickt die App kontinuierlich verschlüsselte HTTP Anfragen an eu.ums.pl.prod.iot.robart.cc und an eu.pl.prod.iot.robart.cc. Die große Anzahl an Paketen liegt an der verwendeten Polling Methode, wobei die Daten oft vom Gerät abgefragt werden. Zu den abgefragten Daten zählt beispielsweise der Status des Roboters.

Personenbezogene Daten

Bei der Registrierung werden E-Mail-Adresse, Passwort und die gewählte Sprache übertragen.

Weiters werden Daten übertragen, welche benötigt werden um einen Raumplan zu zeichnen und die SSID des WLANs.

Test, ob ein Blocken der Verbindung die Funktionalität der IoT-Geräte einschränkt

Der Medion MD 18861 Saugroboter benötigt eine Internetverbindung um mit der Smartphone App bedient werden zu können.
Ein Blocken der Verbindung zu anderen Netzwerkgeräten per AP Isolation stellt keine Beeinträchtigung dar.

Vergleich der von den Herstellern angegebenen Datenschutz Informationen mit den tatsächlich erhobenen Daten

In der App ist die folgende Datenschutzrichtlinie verlinkt:
https://www.medion.com/legal/mcde/md18861/md18861-privacy-de.html

Die Datenschutzrichtlinie enthält Angaben zur Datennutzung bezüglich der Webseite (Punkt 12), dem MEDION Staubsaugerroboter MD18661 (Punkt 19) und generelle Information zu Apps (Punkt 17).

Angaben zu dem im Test verwendeten Staubsaugerroboter MD 18861 sind in der Datenschutzrichtlinie nicht enthalten, jedoch stimmen die Angaben zu dem Gerät MD 18661 großteils mit unseren Feststellungen überein. Einige technische Daten wie beispielsweise die lokale IP-Adresse des Roboters und die SSID des Heimnetzwerks sind nicht aufgelistet.

Mi Smart Band 5

Kontaktierte Server

App

- https://graph.facebook.com:443
  - 69.171.250.15
- https://api-mifit.huami.com:443
  - 18.159.200.30
  - 18.158.124.83
- https://upload-cdn.huami.com:443
  - 99.86.241.23
- https://api-user.huami.com:443
  - 35.158.82.221
- https://account.huami.com:443
  - 18.159.200.30
- https://api-mifit-de2.huami.com:443
  - 52.58.99.240
  - 18.159.200.30
  - 18.159.116.168
  - 18.185.194.119
  - 18.195.66.93
  - 18.158.23.72
- https://account-de2.huami.com:443
  - 18.194.200.10
  - 18.185.194.119
  - 18.158.75.71
  - 18.196.119.143
- https://cdn.awsbj0.fds.api.mi-img.com:443
  - 222.84.158.1
- https://fr.register.xmpush.global.xiaomi.com:443
  - 18.159.147.217

- http://resolver.msg.global.xiaomi.net:80
  - 52.29.233.229
- https://huami-firmware-cdn.huami.com:443
  - 99.86.241.8
- https://apilocate.amap.com:443
  - 47.246.152.0
- https://logs.amap.com:443
  - 106.11.14.3
- https://fe-cdn.huami.com:443
  - 99.86.241.39
- https://api-aos-de2.huami.com:443
  - 18.158.23.72
- https://web-analytics-de.huami.com:443
  - 18.185.4.57
- https://www.google-analytics.com:443
  - 142.250.185.110
- https://restapi.amap.com:443
  - 47.246.109.112
- https://adiu.amap.com:443
  - 203.119.211.253
- https://mpsapi.amap.com:443
  - 198.11.188.36
- https://wprd03.is.autonavi.com:443
  - 47.246.43.224
- https://wprd04.is.autonavi.com:443
  - 47.246.43.224
- https://wprd02.is.autonavi.com:443
  - 47.246.43.228
  - 47.246.43.230
- https://wprd01.is.autonavi.com:443
  - 47.246.43.229

- https://auth-de2.huami.com:443
  - 35.158.82.221
- fr.app.chat.global.xiaomi.net
  - 3.124.49.137
  - 3.64.210.150
  - 18.197.217.221
  - Ports
    - 5222
    - 443
    - 80

Kontaktierte Geräte im Heimnetzwerk

Es wird lediglich das Mi Smart Band 5 per Bluetooth kontaktiert.

Häufigkeit und Größe der Übertragungen

Während der Verwendung der App werden Daten zur Bereitstellung der Funktionalität an die oben genannten Server gesandt und auch von diesen empfangen.

Beim Start der App werden Informationen über das Gerät verschlüsselt an graph.facebook.com übermittelt, selbst wenn man nicht die Anmeldung per Facebook-Account nutzt.

Die App baut eine Verbindung zu fr.app.chat.global.xiaomi.net, beziehungsweise einer von verschiedenen amazonaws.com Subdomains zu denen man "weitergeleitet" wird, auf. Es werden hierfür die Ports 5222, 443 oder 80 in dieser Reihenfolge ausprobiert und verwendet.
Die URLs und Ports, zu denen sich die App verbindet, werden von resolver.msg.global.xiaomi.net unverschlüsselt per HTTP abgefragt.
Nachdem eine Verbindung zu einer der erhaltenen Adressen erstellt wurde, werden fortwährend Daten ausgetauscht. Die ersten zwei Pakete enthalten Klartextinformationen, wie im Folgenden ersichtlich, während der restlichen Datenaustausch offenbar verschlüsselt erfolgt.

```
.....................
xiaomi.com*.CONNH..j..HTC U11 life.
htc_1118777.2"*g-
590277A89886D34FBCC7ABF9CEC2483FA3E946E6('2.wifi:.fr.app.chat.global.xiaom
i.netB.de_ATJ...P...*........6...........
xiaomi.com*.CONNH.

1721534511..5dc1....".}~..
```

Personenbezogene Daten

Im Zuge der Registrierung wurden folgende Daten erfasst:

- Spitzname
- E-Mail-Adresse
- Geburtsdatum
- Größe
- Gewicht
- Aktivitätsziel (Schritte)
- Geschlecht
- Land

Um Daten über das Wetter abzurufen, wird der genaue Standort via Längen- und Breitengrad an api-mifit-de2.huami.com verschlüsselt per HTTPS gesandt.

Nach sportlichen Aktivitäten werden auch verschiedene "Fitnessdaten" übertragen, wie beispielsweise maximale, minimale und durchschnittliche Herzfrequenz, Start- und Endzeit, Dauer, Geschwindigkeit, etc. Die übertragenen Daten hängen von der sportlichen Aktivität ab.

Test, ob ein Blocken der Verbindung die Funktionalität der IoT-Geräte einschränkt

Nach der Anmeldung kann die App auch ohne Internetverbindung genutzt werden. Einzelne Funktionen wie etwa die Freundesliste funktionieren nicht.

Bei unseren Tests hat ein Blocken der Verbindungen zu resolver.msg.global.xiaomi.net ausgereicht, um auch die Verbindungen zu fr.app.chat.global.xiaomi.net zu verhindern. Es wurde keine Einschränkung der Funktionalität festgestellt.

Vergleich der von den Herstellern angegebenen Datenschutz Informationen mit den tatsächlich erhobenen Daten

In der App wird man zu folgender Datenschutzrichtlinie und Software-, Hardware- und Service-Vereinbarung weitergeleitet.

Datenschutzrichtlinie
https://upload-cdn.huami.com/tposts/11000?v=7qbl0tuyvy5f4bv

Software-, Hardware- und Service-Vereinbarung
https://upload-cdn.huami.com/tposts/8322?v=fes3igsgv771pne

Die während des Tests übermittelten personenbezogenen Daten sind in der Datenschutzerklärung vermerkt.

Anmerkungen

Obwohl die App die Funktion hat, die aktuelle Position auf einer Karte anzuzeigen und dabei das Logo von Google verwendet wurde, wurden keine Verbindungen zu Google Maps Services festgestellt. Es

werden dabei Verbindungen zu adiu.amap.com aufgebaut, jedoch wird keine Karte dargestellt.

Oral B Smart 5000

Kontaktierte Server

App

- https://firebaseinstallations.googleapis.com:443
  - 172.217.18.10
- https://sdkapicdn.applanga.com:443
  - 13.32.2.107
  - 13.32.2.15
- https://sd.alchemy.codes:443
  - 52.0.8.250
  - 52.21.163.129
- https://config.emb-api.com
  - 44.228.53.28
  - 52.35.12.196
- https://data.emb-api.com
  - 52.12.110.11
  - 52.39.3.208
  - 52.42.37.147
  - 54.185.195.254
  - Reverse DNS: *.us-west-2.compute.amazonaws.com
- https://sdk.iad-03.braze.com
  - 151.101.189.208
- https://cognito-idp.eu-west-1.amazonaws.com
  - 18.203.74.198
  - Reverse DNS: ec2-18-203-74-198.eu-west-1.compute.amazonaws.com.
- https://cdn.contentful.com
  - 151.101.190.49
- https://2ncybr2rpzcuddvfp3azb54v6q.appsync-api.eu-west-1.amazonaws.com
  - 99.86.242.82
  - 99.86.242.90

- 65.9.67.57
- Reverse DNS: server-99-86-242-82.vie50.r.cloudfront.net

Kontaktierte Geräte im Heimnetzwerk

Es wird lediglich die Zahnbürste per Bluetooth kontaktiert.

Häufigkeit und Größe der Übertragungen

Die App überträgt beim Starten und Stoppen Informationen über die App, das Smartphone und andere Daten, welche zur Fehlerbehebung und Weiterentwicklung der App und zur Erstellung von Statistiken verwenden werden können, wie etwa Nutzungsverhalten innerhalb der App, Fehler, etc.

Der Gebrauch der App veranlasst ebenfalls Übertragungen zur Speicherung der Daten, wie beispielsweise Daten des Zähneputzens.

Personenbezogene Daten

Bei der Registrierung werden der Name und die E-Mail-Adresse übertragen.

Test, ob ein Blocken der Verbindung die Funktionalität der IoT-Geräte einschränkt

Die App kann nach der Anmeldung auch ohne Netzwerkverbindung genutzt werden. Bluetooth wird von der App benötigt, um mit der Zahnbürste interagieren zu können.

Vergleich der von den Herstellern angegebenen Datenschutz Informationen mit den tatsächlich erhobenen Daten

In der App ist die folgende Datenschutzrichtlinie verlinkt:
https://www.pg.com/privacy/german/privacy_statement.shtml

> Diese Informationen können Ihr Mobiltelefon oder eine andere Geräte-Werbe-ID, Informationen über das Betriebssystem Ihres Telefons, die Verwendung der Anwendung oder des Geräts und Ihren physischen Standort umfassen. Sie erhalten eine Popup-Meldung auf Ihrem Telefon oder dem sonstigen von Ihnen benutzten Gerät, die Ihnen die Möglichkeit gibt, Ihre genaue Geolokalisierung zu akzeptieren oder abzulehnen (genau dort, wo Sie sich gerade befinden oder wo Sie auf das Internet zugreifen).

Trotz Standortberechtigung wurde keine Übertragung des Standortes festgestellt.

Planet Buddies Wireless Speaker

Das Herstellen einer Verbindung (Pairing) von einem Smartphone und dem Planet Buddies Wireless Speaker funktioniert ohne jegliche Authentifizierung, wie beispielsweise der Eingabe eines PINs.

Zusätzlich befindet sich der Lautsprecher laufend im Verbindungsmodus, wenn aktuell keine aktive Verbindung besteht. In diesem Fall kann auch eine fremde Person eine Bluetooth Verbindung zu dem Lautsprecher herstellen. Da der Lautsprecher zusätzlich über ein Mikrofon verfügt, kann der Fremde Audioaufnahmen erstellen oder beispielsweise mit einem Kind im Inneren des Hauses sprechen.

Replay Angriff

Wenn sich ein Alexa Echo Dot in der Nähe des Planet Buddies Wireless Speakers befindet, kann sich eine fremde Person mit dem Lautsprecher verbinden, um den Echo Dot innerhalb des Hauses per Sprachbefehle zu steuern.

Zu Demonstrationszwecken kann beispielsweise die Smart Sirene oder der Smart Garage Opener mit Alexa verbunden werden. Danach nimmt man einige Sprachbefehle mithilfe des Smartphones oder über den Planet Buddies Wireless Speaker auf, wie etwa "Alexa schalte Sirene ein" und verbindet sein Smartphone mit dem Lautsprecher. Nach Abspielen des Kommandos wird Alexa beispielsweise in einem anderen Raum ferngesteuert und aktiviert die Sirene.

Playbrush

Kontaktierte Server

App

- https://cdp.cloud.unity3d.com:443
  - 35.241.52.229
- https://api.playbrush.com:443
  - 34.249.188.84
  - Amazon AWS
- https://dashboard.playbrush.com:443
  - 52.212.188.139
  - 52.19.122.184
  - Amazon AWS Elastic Beanstalk
- https://perf-events.cloud.unity3d.com:443
  - 35.190.78.8
- https://config.uca.cloud.unity3d.com:443
  - 35.241.26.53

Kontaktierte Geräte im Heimnetzwerk

Es wird lediglich die Playbrush per Bluetooth kontaktiert.

Häufigkeit und Größe der Übertragungen

Während der Verwendung der App werden Verbindungen zu den oben angeführten Servern aufgebaut. Die eigentliche Funktionalität der App wird durch die Verbindungen zu api.playbrush.com und dashboard.playbrush.com bereitgestellt.

An die anderen Server werden Daten zur Fehlerbehebung, Gerätestatistiken und Ähnliches übertragen.

Personenbezogene Daten

Während der Registrierung werden die E-Mail-Adresse und der Name abgefragt.
Danach muss bei der Erstellung eines Profils das Alter der zugehörigen Person konfiguriert werden.

Nach jedem Putzvorgang werden Daten zu dem Putzvorgang übertragen, wie beispielsweise wie lange oder mit welchem Druck eine Seite geputzt wurde.

Test, ob ein Blocken der Verbindung die Funktionalität der IoT-Geräte einschränkt

Die App kann nach der Anmeldung auch ohne Netzwerkverbindung genutzt werden. Bluetooth wird von der App benötigt, um mit der Zahnbürste interagieren zu können.

Vergleich der von den Herstellern angegebenen Datenschutz Informationen mit den tatsächlich erhobenen Daten

In der App ist die folgende Datenschutzrichtlinie verlinkt:
https://eu.playbrush.com/pages/datenschutz/

Der Hersteller gibt an personenbezogene Daten bei einem Kauf auf der Playbrush-Website zu speichern.

Folgende Daten werden im Rahmen der Registrierung zur Nutzung der App gespeichert:

- Ausgewählte Benutzernamen
- Alter
- Gewähltes Passwort
- Rechnungsadresse
- Telefonnummer(optional)
- E-Mail-Adresse

Weiters werden bei der Registrierung folgende andere Daten gesammelt:

- Land aus den die Anfrage kommt
- Hardware-Identifikationsnummer
- Verwendung des Playbrush-Geräts

Folgende nicht personenbezogene Daten:

- Dauer eines jeden Zahnputzvorgangs
- Zeitpunkt und Häufigkeit der Zahnputzvorgänge
- Zahnputzmethode (Richtung und Geschwindigkeit)
- Druck

Smart Doorlock

Kontaktierte Server

App

- https://a1.tuyaeu.com:443
  - 3.64.122.223
  - 18.194.156.95
  - 35.156.121.251
- https://images.tuyaeu.com:443
  - 99.86.241.33
- https://sailormoon.tuyaeu.com:443
  - 18.156.146.119
- m1.tuyaeu.com:8883
  - 18.197.183.192
  - TLSv1.2
  - secure-mqtt

Kontaktierte Geräte im Heimnetzwerk

Es wird lediglich das Smart Doorlock per Bluetooth kontaktiert.

Häufigkeit und Größe der Übertragungen

Während der Verwendung überträgt die Android App in der Version `3.13.6` Daten verschlüsselt per HTTPS an a1.tuyaeu.com und lädt Bilder von images.tuyaeu.com. Es werden beispielsweise Inhalte der App, verbundene Geräte und der Status der Geräte abgefragt. Es wurden einige Versuche festgestellt, Log-Daten über Warnings an sailormoon.tuyaeu.com zu übermitteln. Diese wurden jedoch vom Server mit dem Antwortcode HTTP 403 FORBIDDEN abgelehnt.

Da die Übermittlung der Befehle, wie das Öffnen des Schlosses, nicht über diese Verbindungen erfolgt, wird vermutet, dass diese verschlüsselt via TLSv1.2 an m1.tuyaeu.com Port 8883 übertragen werden. Es scheint das MQTT Protokoll verwendet zu werden.

Obwohl die Interaktion der App mit dem Schloss per Bluetooth erfolgt, werden während der Verwendung der App Daten verschlüsselt via TLSv1.2 an m1.tuyaeu.com Port 8883 übertragen. Es wurde festgestellt, dass die App eine Liste mit Zeitpunkten, wann das Schloss geöffnet wurde, von a1.tuyaeu.com herunterlädt. Da die Öffnungsbefehle nicht an a1.tuyaeu.com gesandt werden, wird vermutet, dass diese, zusätzlich zur Übermittlung an das Gerät per Bluetooth, verschlüsselt an m1.tuyaeu.com übertragen werden.

Personenbezogene Daten

Bei der Registrierung werden die E-Mail-Adresse und das Land abgefragt.

Test, ob ein Blocken der Verbindung die Funktionalität der IoT-Geräte einschränkt

Die Funktionalität der App bezüglich des Smart Doorlocks kann nach der Anmeldung auch ohne Netzwerkverbindung genutzt werden. Bluetooth wird von der App benötigt, um mit dem Smart Doorlock interagieren zu können.

Vergleich der von den Herstellern angegebenen Datenschutz Informationen mit den tatsächlich erhobenen Daten

Folgende Datenschutzrichtlinie wird in der App angezeigt: https://images.tuyaeu.com/policy/policy_168_88002_de.html?_ty_navTitle=Datenschutzrichtlinie

Die während des Tests übermittelten personenbezogenen Daten sind in der Datenschutzerklärung vermerkt.

Informationen zur Datenschutzerklärung

Der Hersteller gibt an Kontodaten wie beispielsweise E-Mail-Adresse, Telefonnummer und Benutzernamen zu erfassen. Weiters könnten Nickname, Profilbild, Ländercode, Sprachpräferenz oder Zeitzone erfasst werden.

Folgende Daten werden automatisch erfasst:

- Geräteinformationen wie MAC-Adresse, IP-Adresse
- Nutzungsdaten von Sites und Diensten
- System- und Ausnahmeprotokolle bei App Nutzung
- Standortinformationen bei speziellen Produkten wie beispielsweise Reinigungsrobotern.

Intelligente Geräte übertragen folgende Daten:

- Grundlegende Informationen wie Gerätename, ID, Onlinestatus, Aktivierungszeit, Firmware-Version und Aktualisierungsinformationen
- Gemeldete Informationen
    - Je nach Gerät könnten unterschiedliche Informationen erfasst werden. Zum Beispiel kann ein Reinigungsroboter den Reinigungsbereich melden.

Anmerkungen

Die Abdeckung des Türknaufs, welcher zur Bedienung des Tastenfeldes und des Fingerabdruckscanners an der Außenseite der Tür montiert werden muss, wird nur leicht von einem Magneten gehalten und kann mühelos entfernt werden. Darunter befinden sich neben dem Batteriefach, ein Mikro-USB Anschluss und ein Schloss für einen mechanischen Schlüssel. Da es sich

um einen einfachen Schlüssel bestehend aus einem runden Halm mit einer einzigen Zacke handelt, dürfte kein ausreichender Schutz gegen Lockpicking gegeben sein.

Smart Garage Opener

Kontaktierte Server

App

- https://a1.tuyaeu.com:443
  - 3.64.122.223
  - 18.194.156.95
  - 35.156.121.251
- https://images.tuyaeu.com:443
  - 99.86.241.33
  - 99.86.241.109
- https://sailormoon.tuyaeu.com:443
  - 18.156.146.119
- m1.tuyaeu.com:8883
  - 18.196.142.136
  - TLSv1.2
  - secure-mqtt

Garage Opener

- a2.tuyaeu.com:443
  - 3.125.199.146
  - TLSv1.2
- a3.tuyaeu.com:443
  - 18.195.139.137
  - TLSv1.2
- m2.tuyaeu.com:8886
  - 52.57.38.165
  - TLSv1.2

Kontaktierte Geräte im Heimnetzwerk

Während der Suche nach neuen Geräten sendet die Android App in der Version `3.13.6` viele UDP Pakete an die Broadcast Adresse 255.255.255.255 und an diverse Multicast Adressen. Diese sind an Port 30011 oder 30012 gerichtet und unterscheiden sich in der Menge der enthaltenen Daten. Die

Daten enthalten lediglich 0-Bytes, jedoch eben eine unterschiedliche Anzahl dieser. Es wurden keine Antworten auf diese Pakete aufgezeichnet.

Der Smart Garage Opener schickt ungefähr alle 5 Sekunden eine Broadcast Nachricht per UDP an den Port 6667. Die Nachricht ist wahrscheinlich verschlüsselt und scheint von Tuya für die Geräteerkennung verwendet zu werden.

Übersicht

- App
  - UDP Discovery
    - 255.255.255.255
    - div. Multicast (224.0.0.0/8)
    - Port 30011 und 30012
    - nur 0x00 Bytes, aber unterschiedliche Anzahl
- Garage Opener
  - 255.255.255.255:6667
    - UDP

Häufigkeit und Größe der Übertragungen

Während der Verwendung überträgt die Android App in der Version `3.13.6` Daten verschlüsselt per HTTPS an a1.tuyaeu.com und lädt Bilder von images.tuyaeu.com. Es werden beispielsweise Inhalte der App, verbundene Geräte und der Status der Geräte abgefragt. Es wurden einige Versuche festgestellt, Log-Daten über Warnings an sailormoon.tuyaeu.com zu übermitteln. Diese wurden jedoch vom Server mit dem Antwortcode HTTP 403 FORBIDDEN abgelehnt.

Da die Übermittlung der Befehle, wie das Öffnen oder Schließen des Garagentores, nicht über diese Verbindungen erfolgt, wird vermutet, dass diese verschlüsselt via TLSv1.2 an m1.tuyaeu.com Port 8883 übertragen werden. Es scheint das MQTT Protokoll verwendet zu werden.

Der Smart Garage Opener hält eine verschlüsselte Verbindung zu m2.tuyaeu.com Port 8886 aufrecht. Während der Verwendung werden Daten an m2.tuyaeu.com Port 8886, a2.tuyaeu.com Port 443 und a3.tuyaeu.com Port 443 übertragen.

Der Smart Garage Opener schickt ungefähr alle 5 Sekunden eine Broadcast Nachricht per UDP an den Port 6667. Die Nachricht ist wahrscheinlich verschlüsselt und scheint von Tuya für die Geräteerkennung verwendet zu werden.

Ungefähr jede Minute nach dem Startup sendet der Smart Garage Opener 123 Byte Daten an m2.tuyaeu.com Port 8886 und empfängt eine Antwort mit ebenfalls 123 Byte. Beide Pakete sind per TLSv1.2 verschlüsselt.

Personenbezogene Daten

Bei der Registrierung werden die E-Mail-Adresse und das Land abgefragt.

Die Pakete des Smart Garage Openers werden verschlüsselt übertragen und konnten nicht inspiziert werden.

Test, ob ein Blocken der Verbindung die Funktionalität der IoT-Geräte einschränkt

Der Smart Garage Opener benötigt eine Internetverbindung, um mit der Smartphone App bedient werden zu können. Ein Blocken der Internetverbindung verhindert die Bedienung per App.

Ein Blocken der Verbindung zu anderen Netzwerkgeräten per AP Isolation stellt keine Beeinträchtigung dar.

Vergleich der von den Herstellern angegebenen Datenschutz Informationen mit den tatsächlich erhobenen Daten

Folgende Datenschutzrichtlinie wird in der App angezeigt: https://images.tuyaeu.com/policy/policy_168_88002_de.html?_ty_navTitle=Datenschutzrichtlinie

Die während des Tests übermittelten personenbezogenen Daten sind in der Datenschutzerklärung vermerkt.

Informationen zur Datenschutzerklärung

Der Hersteller gibt an Kontodaten wie beispielsweise E-Mail-Adresse, Telefonnummer und Benutzernamen zu erfassen. Weiters könnten Nickname, Profilbild, Ländercode, Sprachpräferenz oder Zeitzone erfasst werden.

Folgende Daten werden automatisch erfasst:

- Geräteinformationen wie MAC-Adresse, IP-Adresse
- Nutzungsdaten von Sites und Diensten
- System- und Ausnahmeprotokolle bei App Nutzung
- Standortinformationen bei speziellen Produkten wie beispielsweise Reinigungsrobotern.

Intelligente Geräte übertragen folgende Daten:

- Grundlegende Informationen wie Gerätename, ID, Onlinestatus, Aktivierungszeit, Firmware-Version und Aktualisierungsinformationen
- Gemeldete Informationen
    - Je nach Gerät könnten unterschiedliche Informationen erfasst werden. Zum Beispiel kann ein Reinigungsroboter den Reinigungsbereich melden.

Smart Sirene

Kontaktierte Server

App

- https://a1.tuyaeu.com:443
  - 3.64.122.223
  - 35.156.121.251
  - 18.194.156.95
- https://images.tuyaeu.com:443
  - 99.86.241.109
- m1.tuyaqu.com:8883
  - 18.194.10.142
  - TLSv1.2
  - secure-mqtt

Sirene

- a3.tuyaeu.com:443
  - 18.195.249.137
- m2.tuyaeu.com:8886
  - 3.121.210.75

Kontaktierte Geräte im Heimnetzwerk

Während der Suche nach neuen Geräten sendet die Android App in der Version `3.13.6` viele UDP Pakete an die Broadcast Adresse 255.255.255.255 und an diverse Multicast Adressen. Diese sind an Port 30011 oder 30012 gerichtet und unterscheiden sich in der Menge der enthaltenen Daten. Die Daten enthalten lediglich 0-Bytes, jedoch eben eine unterschiedliche Anzahl dieser. Es wurden keine Antworten auf diese Pakete aufgezeichnet.

Die Sirene schickt ungefähr alle 5 Sekunden eine Broadcast Nachricht per UDP an den Port 6667. Die Nachricht ist wahrscheinlich verschlüsselt und scheint von Tuya für die Geräteerkennung verwendet zu werden.

Zusätzlich wird ungefähr alle 10 Sekunden ein ARP Paket mit der eigenen IP- und MAC-Adresse an alle Geräte im Netzwerk geschickt.

Übersicht

- APP

    - UDP Discovery
        - 255.255.255.255
        - div. Multicast (224.0.0.0/8)
        - Port 30011 und 30012
        - nur 0x00 Bytes, aber unterschiedliche Anzahl
- Smart Sirene
    - 255.255.255.255:6667
        - UDP
    - FF:FF:FF:FF:FF:FF
        - Gratuitous ARP reply
        - schickt eigene IP an ganzes Netzwerk (ohne Anfrage)

Häufigkeit und Größe der Übertragungen

Während der Verwendung überträgt die Android App in der Version `3.13.6` Daten verschlüsselt per HTTPS an a1.tuyaeu.com und lädt Bilder von images.tuyaeu.com. Es werden beispielsweise Inhalte der App, verbundene Geräte und der Status der Geräte abgefragt.

Da die Übermittlung der Befehle, wie das Auslösen des Alarms oder die Konfiguration des Alarmtons, nicht über diese Verbindungen erfolgt, wird vermutet, dass diese verschlüsselt via TLSv1.2 an m1.tuyaeu.com Port 8883 übertragen werden. Es scheint das MQTT Protokoll verwendet zu werden.

Die Sirene hält eine verschlüsselte Verbindung zu m2.tuyaeu.com Port 8886 aufrecht. Während der Verwendung werden Daten an m2.tuyaeu.com Port 8886 und a3.tuyaeu.com Port 443 übertragen.

Die Sirene schickt ungefähr alle 5 Sekunden eine Broadcast Nachricht per UDP an den Port 6667. Die Nachricht ist wahrscheinlich verschlüsselt und scheint von Tuya für die Geräteerkennung verwendet zu werden.

Ungefähr jede Minute nach dem Startup sendet die Sirene 123 Byte Daten an m2.tuyaeu.com Port 8886 und empfängt eine Antwort mit ebenfalls 123 Byte. Beide Pakete sind per TLSv1.2 verschlüsselt.

Personenbezogene Daten

Bei der Registrierung werden die E-Mail-Adresse und das Land abgefragt.

Die Pakete der Sirene werden verschlüsselt übertragen und konnten nicht inspiziert werden.

Test, ob ein Blocken der Verbindung die Funktionalität der IoT-Geräte einschränkt

Die Sirene benötigt eine Internetverbindung, um mit der Smartphone App bedient werden zu können. Ein Blocken der Internetverbindung verhindert die Bedienung per App.

Ein Blocken der Verbindung zu anderen Netzwerkgeräten per AP Isolation stellt keine Beeinträchtigung dar.

Vergleich der von den Herstellern angegebenen Datenschutz Informationen mit den tatsächlich erhobenen Daten

Folgende Datenschutzrichtlinie wird in der App angezeigt: https://images.tuyaeu.com/policy/policy_168_88002_de.html?_ty_navTitle=Datenschutzrichtlinie

Die während des Tests übermittelten personenbezogenen Daten sind in der Datenschutzerklärung vermerkt.

Informationen zur Datenschutzerklärung

Der Hersteller gibt an Kontodaten wie beispielsweise E-Mail-Adresse, Telefonnummer und Benutzernamen zu erfassen. Weiters könnten Nickname, Profilbild, Ländercode, Sprachpräferenz oder Zeitzone erfasst werden.

Folgende Daten werden automatisch erfasst:

- Geräteinformationen wie MAC-Adresse, IP-Adresse
- Nutzungsdaten von Sites und Diensten
- System- und Ausnahmeprotokolle bei App Nutzung
- Standortinformationen bei speziellen Produkten wie beispielsweise Reinigungsrobotern.

Intelligente Geräte übertragen folgende Daten:

- Grundlegende Informationen wie Gerätename, ID, Onlinestatus, Aktivierungszeit, Firmware-Version und Aktualisierungsinformationen
- Gemeldete Informationen
    - Je nach Gerät könnten unterschiedliche Informationen erfasst werden. Zum Beispiel kann ein Reinigungsroboter den Reinigungsbereich melden.

Smart Valve Controller

Kontaktierte Server

App

- https://a1.tuyaeu.com:443
  - 18.194.156.95
  - 35.156.121.251
  - 3.64.122.223
- https://images.tuyaeu.com:443
  - 99.86.243.10
  - 99.86.243.89
  - 99.86.243.41
- m1.tuyaeu.com:8883
  - 18.196.142.136
  - TLSv1.2
  - secure-mqtt

Smart Valve Controller

- m2.tuyaeu.com:8886
  - 52.57.38.165
  - TLSv1.2
- a3.tuyaeu.com:443
  - 18.195.249.137
  - 18.185.182.159
  - TLSv1.2

Kontaktierte Geräte im Heimnetzwerk

Das Smart Valve schickt ungefähr alle 5 Sekunden eine Broadcast Nachricht per UDP an den Port 6667. Die Nachricht ist wahrscheinlich verschlüsselt und scheint von Tuya für die Geräteerkennung verwendet zu werden.

Zusätzlich wird ungefähr alle 10 Sekunden ein ARP Paket mit der eigenen IP- und MAC-Adresse an alle Geräte im Netzwerk geschickt.

Während der Suche nach neuen Geräten schickt die App viele UDP Pakete an die Broadcast Adresse (255.255.255.255) und diverse Multicast Adressen (224.0.0.0/8) an Port 30011 und 30012. Diese

Pakete enthalten lediglich 0-Bytes, enthalten jedoch eine unterschiedliche Anzahl dieser. Es wurden keine Antworten aufgezeichnet.

Übersicht

- App
  - UDP Discovery
    - 255.255.255.255
    - div. Multicast (224.0.0.0/8)
    - Port 30011 und 30012
    - nur 0x00 Bytes, aber unterschiedliche Anzahl
- Smart Valve Controller
  - 255.255.255.255:6667
    - UDP
  - FF:FF:FF:FF:FF:FF
    - Gratuitous ARP reply
    - schickt eigene IP an ganzes Netzwerk (ohne Anfrage)

Häufigkeit und Größe der Übertragungen

Während der Verwendung überträgt die Android App in der Version `3.13.6` Daten verschlüsselt per HTTPS an a1.tuyaeu.com und lädt Bilder von images.tuyaeu.com. Es werden beispielsweise Inhalte der App, verbundene Geräte und der Status der Geräte abgefragt.

Da die Übermittlung der Befehle, wie Ventil öffnen oder schließen, nicht über diese Verbindungen erfolgt, wird vermutet, dass diese verschlüsselt via TLSv1.2 an m1.tuyaeu.com Port 8883 übertragen werden. Es scheint das MQTT Protokoll verwendet zu werden.

Das Smart Valve hält eine verschlüsselte Verbindung zu m2.tuyaeu.com Port 8886 aufrecht. Während der Verwendung werden Daten an m2.tuyaeu.com Port 8886 und a3.tuyaeu.com Port 443 übertragen.

Das Smart Valve schickt ungefähr alle 5 Sekunden eine Broadcast Nachricht per UDP an den Port 6667. Die Nachricht ist wahrscheinlich verschlüsselt und scheint von Tuya für die Geräteerkennung verwendet zu werden.

Ungefähr jede Minute nach dem Startup sendet das Smart Valve 123 Byte Daten an m2.tuyaeu.com Port 8886 und empfängt eine Antwort mit ebenfalls 123 Byte. Beide Pakete sind per TLSv1.2 verschlüsselt.

Personenbezogene Daten

Bei der Registrierung werden die E-Mail-Adresse und das Land abgefragt.

Die Pakete des Smart Valve werden verschlüsselt übertragen und konnten nicht inspiziert werden.

Test, ob ein Blocken der Verbindung die Funktionalität der IoT-Geräte einschränkt

Das Smart Valve benötigt eine Internetverbindung, um mit der Smartphone App bedient werden zu können. Ein Blocken der Internetverbindung verhindert die Bedienung per App.

Ein Blocken der Verbindung zu anderen Netzwerkgeräten per AP Isolation stellt keine Beeinträchtigung dar.

Vergleich der von den Herstellern angegebenen Datenschutz Informationen mit den tatsächlich erhobenen Daten

Folgende Datenschutzrichtlinie wird in der App angezeigt: https://images.tuyaeu.com/policy/policy_168_88002_de.html?_ty_navTitle=Datenschutzrichtlinie

Die während des Tests übermittelten personenbezogenen Daten sind in der Datenschutzerklärung vermerkt.

Informationen zur Datenschutzerklärung

Der Hersteller gibt an Kontodaten wie beispielsweise E-Mail-Adresse, Telefonnummer und Benutzernamen zu erfassen. Weiters könnten Nickname, Profilbild, Ländercode, Sprachpräferenz oder Zeitzone erfasst werden.

Folgende Daten werden automatisch erfasst:

- Geräteinformationen wie MAC-Adresse, IP-Adresse
- Nutzungsdaten von Sites und Diensten
- System- und Ausnahmeprotokolle bei App Nutzung
- Standortinformationen bei speziellen Produkten wie beispielsweise Reinigungsrobotern.

Intelligente Geräte übertragen folgende Daten:

- Grundlegende Informationen wie Gerätename, ID, Onlinestatus, Aktivierungszeit, Firmware-Version und Aktualisierungsinformationen
- Gemeldete Informationen
    - Je nach Gerät könnten unterschiedliche Informationen erfasst werden. Zum Beispiel kann ein Reinigungsroboter den Reinigungsbereich melden.

Snaptain S5C Drohne

Kontaktierte Server

Es wurden von der App keine Server im Internet kontaktiert, wenn das Smartphone mit dem Heimnetzwerk verbunden war.

Kontaktierte Geräte im Heimnetzwerk

Die Snaptain S5C Drohne öffnet ein eigenes offenes WLAN-Netzwerk, zu welchem das Smartphone verbunden werden muss. Das Smartphone baut dabei eine Verbindung zu der Drohne auf.

Häufigkeit und Größe der Übertragungen

Das Smartphone überträgt Befehle und empfängt Daten von/zu der Drohne, welche immer die IP-Adresse 192.168.0.1 konfiguriert hat. Es werden hierfür die Ports 8060 (TCP), 7060 (TCP) und 50000 (TCP oder UDP) verwendet. Aufgrund des Programmcodes kann angenommen werden, dass der Port 8060 für generelle Befehle, wie etwa starte/stoppe Videoaufnahme, Port 7060 für die Videoübertragung und Port 50000 für die Steuerung der Drohne verwendet werden.

Weiters überträgt die Drohne ungefähr alle 2 Sekunden ein UDP Paket ausgehend von Port 54709 an das Smartphone Port 44000. Diese Pakete enthalten immer 2 Byte Daten und werden vom Smartphone mit einem ICMP Paket Destination unreachable (Port unreachable) beantwortet.

Personenbezogene Daten

Es werden keine personenbezogenen Daten abgefragt. Es werden auch keine anderen Daten wie etwa Videoaufnahmen versandt, nachdem eine Internetverbindung hergestellt wurde.

Test, ob ein Blocken der Verbindung die Funktionalität der IoT-Geräte einschränkt

Die App benötigt eine direkte Verbindung zu der Drohne.

Vergleich der von den Herstellern angegebenen Datenschutz Informationen mit den tatsächlich erhobenen Daten

Es werden in der App keine Datenschutzrichtlinien angegeben.

Die Datenschutzerklärung, welche im Google Play Store Eintrag der App verlinkt ist, enthält lediglich eine Liste von verschiedenen Apps und das Versprechen, dass keine dieser Apps sensitive Benutzer- oder Gerätedaten preis gibt. Die Snaptain Era App ist in dieser Liste nicht enthalten.

Datenschutzerklärung:
https://play.google.com/store/apps/details?id=com.guanxu.technology.snaptain_era_s5c&hl=de_AT&gl=US

Anmerkungen

Auf der Drohne läuft ein Telnet Server auf Port 23, welcher jedoch einen Benutzernamen und ein Passwort benötigt. Es wurden keine Verbindungen zu diesem Telnet Server festgestellt und es konnten keine Zugangsdaten in dem Programmcode der App gefunden werden. Eine Internetrecherche blieb ebenfalls erfolglos.

Weiters ist der Port 6789 auf der Drohne geöffnet, es konnten jedoch keine Verbindungen festgestellt werden. Auf manuelle Verbindungsversuchen erfolgte keine Antwort.

XPLORA 4 Smartwatch

Kontaktierte Server

App

- https://settings.crashlytics.com:443
  - 142.250.185.195
  - 216.58.210.3
- https://clients4.google.com:443
  - 142.250.185.174
- https://csi.gstatic.com:443
  - 142.250.138.94
  - 74.125.138.94
  - 142.250.115.120
  - 172.217.161.95
  - 216.58.199.67
- https://app.myxplora.com:443
  - myxplora-ssl-public-70f7aa8abab5bd4c.elb.eu-central-1.amazonaws
    - 3.121.14.217
    - 3.121.57.122
    - 52.58.96.200
- s3.eu-central-1.amazonaws.com:443
  - 52.219.140.183

Uhr

- xplora3.myxplora.com
  - myxplora-lvs-511369664.eu-central-1.elb.amazonaws.com:443
    - 3.124.65.47
    - 3.127.84.14
    - 18.193.162.104
- kids-ota-rom.s3.eu-central-1.amazonaws.com
  - s3-r-w.eu-central-1.amazonaws.com:443

        - 52.219.140.77
- ec2-35-159-47-65.eu-central-1.compute.amazonaws.com:443
    - 35.159.47.65
- ec2-52-58-40-100.eu-central-1.compute.amazonaws.com:80
    - 52.58.40.100

Kontaktierte Geräte im Heimnetzwerk

Es werden keine Geräte im Heimnetzwerk kontaktiert, außer dem Gateway.

Häufigkeit und Größe der Übertragungen

Beim Start der App wird die Konfiguration für den Firebase Crashlytics Service von settings.crashlytics.com abgefragt. Es wurde ebenfalls eine verschlüsselte Verbindung zu s3.eu-central-1.amazonaws.com hergestellt und ungefähr 8 MB Daten heruntergeladen.

Während der Verwendung der App werden Daten per HTTPS Anfragen verschlüsselt an app.myxplora.com übertragen und empfangen. Die TLS Verbindung wird zusätzlich mittels Client Certificate und Certificate Pinning in der App geschützt. Daten, die an den Server gesandt werden, werden als Base64 codierte Binärdaten per URL Parameter an die HTTP Anfrage angehängt. HTTP Antworten werden im JSON Format übertragen, wobei die eigentlichen Daten im "data" Feld wiederum als Base64 codierte Binärdaten enthalten sind.

Die Xplora 4 Smartwatch überträgt und empfängt während ihrer Verwendung verschlüsselt Daten an myxplora-lvs-511369664.eu-central-1.elb.amazonaws.com.
Weiters wurden einmalig ungefähr 26 MB Daten verschlüsselt von s3-r-w.eu-central-1.amazonaws.com heruntergeladen.

Die Xplora 4 Smartwatch überträgt und empfängt ungefähr alle 2-4 Minuten Daten an/von ec2-35-159-47-65.eu-central-1.compute.amazonaws.com Port 443, es wird jedoch keine TLS Verbindung aufgebaut. Es werden verschiedene Zeitstempel und IDs im Klartext übertragen. Die eigentlichen Daten scheinen verschlüsselt zu sein. Einmalig wurden Daten mit ec2-52-58-40-100.eu-central-1.compute.amazonaws.com Port 80 ausgetauscht. Bei beiden Verbindungen scheint das selbe Protokoll verwendet zu werden.

Personenbezogene Daten

Aufgrund der unbekannten Kodierung der übermittelten Daten und der verschlüsselten Verbindungen der Xplora 4 Smartwatch konnten die übermittelten Daten nicht geprüft werden.

Bei der Registrierung werden folgende Daten abgefragt:

- Telefonnummer
- Länder Code

Test, ob ein Blocken der Verbindung die Funktionalität der IoT-Geräte einschränkt

Die App sowie die Xplora 4 Smartwatch benötigten eine Internetverbindung, um die Funktionalität bereitzustellen.

Ein Blocken der Verbindung zu anderen Netzwerkgeräten per AP Isolation stellt keine Beeinträchtigung dar.

Vergleich der von den Herstellern angegebenen Datenschutz Informationen mit den tatsächlich erhobenen Daten

In der App ist die folgende Nutzungs- und Datenschutzrichtlinie verlinkt: https://support.myxplora.com/hc/de/articles/360003182654

Die während des Tests übermittelten personenbezogenen Daten sind in der Datenschutzerklärung vermerkt.