Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG ZUR CYBER-SICHERHEIT

Sicherheit von Geräten im Internet der Dinge

Netzwerkfähige Geräte sind im Kontext des Internet der Dinge (Internet of Things, IoT) ein potenzielles Sicherheitsrisiko. Dies ist insbesondere darin begründet, dass bei Entwicklung und Betrieb dieser Geräte der Aspekt der Cyber-Sicherheit ein nicht oder nur nachrangig beachtetes Entwurfsziel ist. Kostengründe, möglichst effektive Herstellung und teilweise kurze Produktzyklen – gerade bei Fabrikaten für den Massenmarkt - tragen ebenfalls zu einer Vernachlässigung bei. Solche Geräte können daher zum Sicherheitsrisiko für die eigene Umgebung bzw. Infrastruktur und auch für Dritte werden. Die Vielfalt ist sehr groß. Beispielhaft zu nennen sind hier Geräte des täglichen Gebrauchs wie:

- Überwachungskameras
- Home Router
- Smart Home Geräte und Anwendungen, zum Beispiel
  - Sprachassistenten bzw. digitale Assistenten
  - Mediacenter
  - Thermostate
  - Fernbedienbare Schlösser
  - Küchengeräte
- und vieles mehr

Eingesetzt werden die Geräte in allen möglichen Bereichen, sowohl kommerziell wie auch zunehmend im privaten Umfeld.

In den vergangenen Jahren ist es immer wieder zu Vorfällen im Zusammenhang mit vernetzten bzw. IP-basierten IoT-Geräten gekommen. Besonders häufig waren Überwachungskameras betroffen, hier exemplarisch:

- 2013: Eine russische Hackergruppe kompromittiert im Zuge der Kampagne "Carbanak" mehrere Banken in verschiedenen Ländern und erbeutet einen dreistelligen Millionenbetrag. Bei diesen Angriffen wurden Überwachungskameras innerhalb der Finanzinstitute kompromittiert, um Bildschirminhalte und Tastatureingaben auszuspähen, Mitarbeiter z. B. über Namensschilder/Mitarbeiterausweise als Ziel für Spear-Phishing zu identifizieren sowie Gewohnheiten und Reaktionen der Mitarbeiter in Erfahrung zu bringen.[1]

1 http://newsroom.kaspersky.eu/de/texte/detail/article/der-grosse-bankraub-cybergang-carbanak-stiehlt-eine-milliarde-us-dollar-von-100-finanzinstitu

- 2014: Die Webseite Insecam stellt die Videobilder bzw. -streams von 73.000 unzureichend geschützten Webcams (maßgeblich aus dem privaten Anwendungsbereich) offen zur Verfügung.[2]
- 2015: Die Schadsoftware Conficker aus dem Jahr 2008 infiziert eine Vielzahl von Bodycams verschiedener Polizeien.[3]
- 2016: Eine große Anzahl von durch die Schadsoftware Mirai kompromittierten Überwachungs-/Webkameras wird dazu verwendet, um einen der massivsten DDoS-Angriffe der Geschichte auf den Fachjournalisten Brian Krebs durchzuführen.[4]

Ziel dieses Dokuments ist es, einen Überblick über die elementaren Best Practices zum sicheren Betrieb solcher Geräte zu geben.

1 Produktauswahl

Schon im Rahmen der Produktauswahl sollten bei der Betrachtung von Preis-Leistungs-Verhältnissen auch Aspekte der IT-Sicherheit berücksichtigt werden. Hier spielen vor allem die angebotene Funktionalität des Produktes und die Leistungen des Herstellers nach dem Verkauf (After-Sales-Support) eine wichtige Rolle. Besonderes Augenmerk ist darauf zu richten, welche Sicherheitsmechanismen und Sicherheitsmerkmale das Gerät bietet. Eine ausführliche Dokumentation des Gerätes, seiner Funktionen und der Eigenschaften sollte verfügbar sein.

Grundsätzlich ist von der Verwendung innerhalb eines Cloud-Konzepts abzuraten. In diesem Falle fließen sensible Daten über Dritte (z. B. Hersteller, Diensteanbieter) oder auch an Dritte und werden dort für einen Zugriff über das Internet gespeichert. Sensible Daten sind hier Video- und Audiostreams, Konfigurationen, Messwerte und Umgebungsdaten aus dem jeweiligen Netzwerksegment. Welche Daten erfasst und übertragen werden, muss der Produktbeschreibung zu entnehmen sein.

Auch sollten die Geräte über einen kabelgebundenen Netzwerkanschluss verfügen, um gegebenenfalls die Verwendung von Wi-Fi/WLAN – insbesondere in kritischen Einsatzbereichen – vermeiden zu können. Bei der Verwendung von Wi-Fi/WLAN sind die in Kapitel 5 genannten Empfehlungen zur Absicherung zu beachten.

Ein grundlegendes Ziel zum sicheren Einsatz ist die Minimierung der Angriffsfläche. Um diese von Beginn an gering zu halten, empfiehlt es sich, Geräte zu beschaffen, die nur die für den konkreten Einsatzzweck erforderlichen Dienste/Ports zur Verfügung stellen. Alternativ sollte es möglich sein, nicht benötigte Dienste zu deaktivieren. Ist auch dies nicht möglich, müssen entsprechende Einschränkungen bei der Inbetriebnahme auf Netzwerkebene vorgenommen werden, um die Verwendung von nicht benötigten Diensten und deren Verbindung zum Internet zu verhindern.

Um eine vertrauliche Übertragung von Daten zu gewährleisten, sollte das Produkt ein auf Verschlüsselung basierendes Protokoll (z. B. SSL/TLS bzw. SSH) unterstützen.

Das Gerät bzw. die darauf implementierten Anwendungen sollten eine hinreichende Authentisierung enthalten. Sofern das Gerät ein differenziertes Rollen-/Rechtekonzept für unterschiedliche Benutzer bereitstellt, sollte dies entsprechend genutzt werden. Von Geräten mit festkodierten und nicht veränderbaren Passwörtern ist abzuraten.

2 http://www.networkworld.com/article/2844283/microsoft-subnet/peeping-into-73-000-unsecured-security-cameras-thanks-to-default-passwords.html
3 http://www.goipower.com/?pageId=40
4 https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/

Weiterhin muss der Hersteller für einen hinreichend langen Zeitraum die Bereitstellung von Patches bzw. Updates gewährleisten. Dies wird meist mit End Of Service (EOS) beschrieben – nicht zu verwechseln mit End Of Life (EOL), was das Ende der Herstellung und des Verkaufs eines Produktes bezeichnet.

2 Installation und Inbetriebnahme

Nicht nur für die Beschaffung, sondern auch für die Inbetriebnahme existieren Empfehlungen zum sicheren Einsatz. Grundsätzlich gilt: Embedded Webserver, wie sie in nahezu allen IoT-Geräten vorhanden sind, beispielsweise bei Überwachungskameras, sind typischerweise nicht dazu geeignet, um über das Internet uneingeschränkt erreichbar gemacht zu werden.

Während der erstmaligen Konfiguration des IoT-Gerätes sollten hinreichend sichere Passwörter verwendet werden. Voreingestellte Passwörter müssen geändert werden. Zusätzlich empfiehlt sich die Verwendung von alternativen Authentisierungsmechanismen, wie z. B. zertifikatsbasierter Authentisierung. Weiterhin sollten in diesem Schritt nicht benötigte Dienste der Kamera deaktiviert werden. Dies gilt insbesondere für chronisch unsichere Dienste, wie z. B. Telnet oder SNMPv1/v2.

Allgemein gilt, dass vom Gerät initiierte Verbindungen ins Internet blockiert werden sollten. Valide Ziele, wie z. B. Update-Server des Herstellers, Speicherort der Daten (z. B. Videodaten von Kameras, Audiodaten von digitalen Assistenten) und Managementsystem, können als Ausnahmen in der Firewall konfiguriert werden. Ob und wie die Geräte die Server des Herstellers kontaktieren müssen, um die Verfügbarkeit von Updates zu prüfen, sollte in der Produktdokumentation recherchiert werden. Gegebenenfalls sollte auf eine automatische Updatefunktion verzichtet und Updates und Patches händisch installiert werden. Anschließend sind Funktionen und Einstellungen zu prüfen und im Bedarfsfall erneut anzupassen.

Eine direkte Erreichbarkeit des Gerätes (durch z. B. eine Port-Weiterleitung auf einem Router) sollte nur in Ausnahmefällen ermöglicht werden. Falls die Erreichbarkeit von außen (d. h. aus dem Internet eingehend) erforderlich ist, so sollte dies nur mit hinreichender Authentisierung erfolgen. **Es gilt daher, den Zugriff von außen über Telnet (Port 23) auf keinen Fall freizugeben und den Zugriff über SSH (Port 22) nur freizugeben, wenn dieser mit hinreichend sicheren individuellen Passwörtern geschützt ist.** Eine höhere Sicherheit wird erlangt, wenn der Zugriff nicht über Benutzername und Passwort, sondern durch ein Zertifikat gesichert wird. Die standardmäßig verwendeten Ports (23, 1023, 232) sollten nicht nach außen aktiv sein und für eine Verwendung auf einen Zufallswert im Bereich 10000 bis 65535 gesetzt werden.

Gegebenenfalls sollte der Fernzugriff zusätzlich durch die Verwendung eines VPN abgesichert werden. Dies ist zum Beispiel sinnvoll, wenn das Produkt selbst keine verschlüsselte Übertragungen oder keinen Authentisierungsmechanismus anbietet. Bei der Verwendung von VPN ist darauf zu achten, dass ausreichend starke kryptografische Verfahren und entsprechende Schlüssellängen verwendet werden.

Es empfiehlt sich auch, die Geräte in einem separaten physischen Netzbereich bzw. innerhalb eines separaten Virtual Local Area Networks (VLANs) zu betreiben, um ein laterales Ausbreiten von Schadcode im internen Netzwerk bei einer Kompromittierung zu vermeiden.

Abhängig vom Einsatzort und der Art des Gerätes sollte ein physikalischer Zugriffsschutz umgesetzt werden. Dieser schützt nicht nur vor Vandalismus, sondern auch vor einer Veränderung der Konfiguration, die häufig durch das Zurücksetzen auf den Werkszustand ermöglicht wird.

3 Betrieb

Während des Betriebes sollte regelmäßig überprüft werden, ob neue Updates/Patches zur Installation zur Verfügung stehen. Zusätzlich zur Firmware sollten auch Drittkomponenten, wie z. B. Administrations- oder Managementsoftware, auf Aktualität überprüft werden. Falls neue Updates verfügbar sind, sind diese zeitnah einzuspielen.

Es empfiehlt sich, die Kommunikation (ein- und ausgehende Verbindungen) regelmäßig auf Auffälligkeiten zu kontrollieren. Hierbei können Logfiles von Firewalls genaue Informationen liefern, mit wem das Gerät über welchen Dienst kommunizieren möchte und ob diese Verbindungen erlaubt oder blockiert wurden. Weiterhin kann auch das Gerät selbst oder die dazugehörige Administrations- oder Managementsoftware Informationen liefern, ob das Gerät erwartungsgemäß verwendet wird.

Einige Varianten von Schadsoftware, die auf IoT-Geräten beobachtet wurden, arbeiten oftmals nur im Hauptspeicher, statt sich persistent im System einzunisten. Daher ist ein regelmäßiger Neustart ratsam. Dieser kann eine Infektion bereinigen, wenngleich dies nicht vor einer Neuinfektion schützt.

4 Zusammenfassung der Maßnahmen

- Ungeschützte Erreichbarkeit über das Internet vermeiden
- Ausgehende Kommunikation durch Firewall einschränken
- Selbstgewählte hinreichend starke Passwörter verwenden
- Fernzugriff nur über VPN ermöglichen
- Nur benötigte Dienste aktivieren
- Nur verschlüsselt kommunizieren
- Beachtung des EOS Zeitraums
- Einsatz ausreichend starker Authentisierungsmechanismen
- Netzwerkseparation bzw. Segmentierung einsetzen
- Zeitnahes Einspielen von Updates
- Monitoring der Kommunikation (Logfiles)
- Cloud-Konzepte vermeiden
- Wi-Fi/WLAN in kritischen Bereichen vermeiden
- Optionale Verwendung von Rechte- und Rollenkonzepten
- Optionaler physikalischer Zugriffsschutz

5 Weitere Informationen

Die folgenden Empfehlungen der Allianz für Cyber-Sicherheit sowie die technischen Richtlinien des BSI und die BSI-Standards zur Internet-Sicherheit (ISi-Reihe) liefern zusätzliche Informationen und beschreiben Umsetzungsempfehlungen für die zuvor genannten Maßnahmen:

- Anforderungen an netzwerkfähige Industriekomponenten[5]

  Diese Empfehlung ist neben netzwerkfähigen Industriekomponenten auch auf eine Vielzahl von IoT-Geräten anwendbar. Hierin werden insbesondere auch Anforderungen an den Hersteller bzw. Integrator beschrieben.

- Sichere Passwörter in Embedded Devices v1.0[6]

  Diese Empfehlung beschreibt das allgemeine Problem von festcodierten Zugangsdaten in Embedded Devices, zu denen auch IoT-Geräte zählen. Es werden hier Empfehlungen für Hersteller, Integratoren und Betreiber gegeben.

- Rohde & Schwarz SIT GmbH: Checkliste Netzwerksicherheit[7]

  Diese Empfehlung beschreibt, wie der Netzübergang in das Internet abgesichert werden kann und gibt Empfehlungen, wie sich ein Netzwerk z. B. durch VLANs segmentieren lässt.

- BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen[8]

  Die Technische Richtlinie gibt u. a. Empfehlungen zur Verwendung von kryptographischen Verfahren für TLS, VPN und SSH.

- BSI-Standards zur Internet-Sicherheit (ISi-Reihe)[9]

  Die ISi-Reihe beschäftigt sich mit hier relevanten Themen, wie z. B. Sichere Anbindung von lokalen Netzen an das Internet (ISi-LANA), Wireless LAN (ISi-WLAN) und Virtual Private Network (ISi-VPN).

Darüber hinaus bietet der IT-Grundschutz bzw. das IT-Grundschutz Kompendium weitere Informationen. Die folgenden Bausteine beschreiben Umsetzungsempfehlungen von zuvor genannten Maßnahmen:

IT-Grundschutz Kompendium:

- SYS.4.4 Allgemeines IoT-Gerät[10]
- Umsetzungshinweise zum Baustein SYS.4.4 Allgemeines IoT-Gerät[11]
- NET.2.1 WLAN-Betrieb[12]
- NET.2.2 WLAN-Nutzung[13]
- NET.3.3 VPN[14]

5 https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS/BSI-CS_067.pdf
6 https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS/BSI-CS_069.pdf
7 https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/partner/Partnerbeitrag_Rohde-Schwarz.html
8 https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html
9 https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-Reihe_node.html
10 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/SYS/SYS_4_4_Allgemeines_IoT-Ger%C3%A4t.html
11 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/umsetzungshinweise/SYS/Umsetzungshinweise_zum_Baustein_SYS_4_4_Allgemeines_IoT-Ger%C3%A4t.html
12 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/NET/NET_2_1_WLAN-Betrieb.html
13 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/NET/NET_2_2_WLAN-Nutzung.html
14 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/NET/NET_3_3_VPN.html

IT-Grundschutz:

- B 3.407 Eingebettetes System[15]
- M 2.8 Vergabe von Zugriffsrechten[16]
- M 2.11 Regelung des Passwortgebrauchs[17]
- M 2.109 Rechtevergabe für den Fernzugriff[18]
- M 2.273 Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates[19]
- M 2.384 Auswahl geeigneter Kryptoverfahren für WLAN[20]
- M 2.555 Entwicklung eines Authentisierungskonzeptes für Anwendungen[21]
- M 4.7 Änderung voreingestellter Passwörter[22]
- M 4.488 Deaktivieren nicht benutzter Schnittstellen und Dienste bei eingebetteten Systemen[23]
- M 5.61 Geeignete physische Segmentierung[24]
- M 5.62 Geeignete logische Segmentierung[25]
- M 5.77 Bildung von Teilnetzen[26]

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an **info@cyber-allianz.de** gesendet werden.

15 IT-Grundschutz-Katalog Bausteinkatalog B 3.407
16 IT-Grundschutz-Katalog Maßnahmenkatalog M 2.8
17 IT-Grundschutz-Katalog Maßnahmenkatalog M 2.11
18 IT-Grundschutz-Katalog Maßnahmenkatalog M 2.109
19 IT-Grundschutz-Katalog Maßnahmenkatalog M 2.273
20 IT-Grundschutz-Katalog Maßnahmenkatalog M 2.384l
21 IT-Grundschutz-Katalog Maßnahmenkatalog M 2.555
22 IT-Grundschutz-Kataloge Maßnahmenkatalog M 4.7
23 IT-Grundschutz-Kataloge Maßnahmenkatalog M 4.488
24 IT-Grundschutz-Kataloge Maßnahmenkatalog M 5.61
25 IT-Grundschutz-Kataloge Maßnahmenkatalog M 5.62
26 IT-Grundschutz-Kataloge Maßnahmenkatalog 5.77