LSI-Info T#04

DAS INTERNET DER DINGE - IOT

Version 1.1 vom: 01.10.2024

Management Summary

Mit zunehmender Digitalisierung flankiert von Industry 4.0 ist von einer starken Zunahme von IoT-Geräten (Internet of Things = Internet der Dinge) auszugehen. Zu dieser Geräteklasse zählen Geräte, die nicht unbedingt auf den ersten Blick als vernetzt wahrgenommen werden (Überwachungskameras, Beamer, Haustechnik, Kassenautomaten, Zutritts-Systeme u. v. a. m.). Vor allem im Gesundheitsbereich sind diese IoT-Geräte weit verbreitet. Nach Recherchen des auf Medizintechnik spezialisierten US-amerikanischen IT-Anbieters Medigate sind in einem mittelgroßen Krankenhaus etwa 20.000 IoT-Geräte zu finden. Pro Bett sind dies etwa 10-15 Geräte – davon sind 5-10 medizinische Überwachungsgeräte.[1)]
Das Gefährdungspotenzial dieser Geräte wird oft nicht wahrgenommen oder unterschätzt. Gerade dieses macht diese Geräte für Angreifer interessant. Problematisch sind hier veraltete Softwarestände und nicht geänderte Default-Passwörter. Werden IoT-Geräte kompromittiert, funktionieren diese nicht mehr (Denial of Service) oder sie werden als fernsteuerbare Drohne Teil eines Botnet, greifen andere an und liefern Daten nach außen.
Nachstehend folgen Tipps, wie IoT-Geräte abgesichert werden können.

1) Security-Insider, 15.06.2020, Cyberangriffe auf Krankenhäuser nehmen zu, https://www.security-insider.de/cyberangriffe-auf-krankenhaeuser-nehmen-zu-a-938595/, gelesen am 16.06.2020

Ändern von Standardpasswörtern

Die Standardpasswörter der Geräte stehen meist in der Bedienungsanleitung, welche im Internet frei verfügbar ist. Diese Passwörter werden unmittelbar genutzt bzw. in Passwortlisten hinterlegt und für Brute-Force-Angriffe genutzt.

Tipp:

Ändern Sie das Standardpasswort sofort bei der Inbetriebnahme. Für die Ablage der Passwörter sollte ein Passwortsafe genutzt werden.

Regelmäßige Updates von Firmware, Betriebssystem, Software, Treiber

Sobald ein Hersteller für eine Schwachstelle ein Patch bzw. Update zur Verfügung stellt, sollten diese zeitnah installiert werden, um die Sicherheitslücke zu schließen. Bekannt gewordene Sicherheitslücken werden schnell öffentlich bekannt und es dauert nicht lange bis eine Schadsoftware vorliegt, die diese Sicherheitslücke nutzt.
IoT-Geräte bringen eine Vielzahl an Software-Bibliotheken mit, die jeweils eine Angriffsmöglichkeit bieten könnten.

Tipp:

Halten Sie Ihre verwendeten Geräte auf dem aktuellen Softwarestand. Informieren Sie sich über Patches und Sicherheitslücken, z. B. über ein Newsletter-Abonnement des Herstellers.

IT-Systeme ganzheitlich schützen

Nach dem Minimalprinzip sollten nur benötigte Schnittstellen und Funktionen aktiviert werden. Die Konfiguration muss – falls möglich - mit einem Kennwort gesichert werden. Beispielsweise können bei Computersystemen sicherheitsrelevante Systemeinstellungen wie die Startreihenfolge der Laufwerke im BIOS/UEFI vorgenommen werden und diese mit einem Kennwort vor Manipulationen geschützt werden.

Tipp:

Konfigurieren Sie Ihre IT-Systeme nach dem Minimalprinzip und schützen sie gegen Manipulation mit einem Passwort.

Netzwerksegmentierung

Erfolgreiche Angriffe mit Schadsoftware gefährden i.d.R. auch andere Systeme im gleichen Netzwerksegment. In der Netzwerktechnik sind Netzwerksegmente vergleichbar mit Brandabschnitten in Gebäuden.

Tipp:

IoT-Geräte sollten Sie ggf. nach Einsatzgebiet gruppiert in eigenen technischen Netzwerksegmenten betreiben. Regeln Sie die Kommunikation zwischen den Netzwerksegmenten und legen Sie ein besonderes Augenmerk auf die Systeme, die vom Internet erreichbar sind. Lassen Sie einen Fernzugriff möglichst nur über VPN zu.

Supportzeitraum beachten

Sicherheitsupdates werden für Geräte einer bestimmten Baureihe oder eine bestimmte Betriebssystemversion nur eine gewisse Zeit zur Verfügung gestellt. Ein bekanntes Beispiel ist das Ende des Windows 7 Supports im Januar 2020.

Tipps:

Berücksichtigen Sie Aspekte der Informationssicherheit wie den Supportzeitraum bereits bei der Planung und Beschaffung neuer Geräte und ersetzen Sie vernetzte Geräte, für die es keinen Support mehr gibt. Aufgrund der Vielzahl an IoT-Geräten empfiehlt sich hier eine entsprechende Dokumentation. Beziehen Sie bei allen Gerätebeschaffungen Ihren ISB mit ein und beachten Sie die Beschaffungskriterien für IoT-Geräte des BSI-Bausteins SYS.4.4.A8:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/07_SYS_IT_Systeme/SYS_4_4_Allgemeines_IoT_Geraet_Edition_2023.pdf

Ergreifen Sie angemessene Schutzmaßnahmen, falls sich ein temporärer Betrieb von IoT mit abgelaufenem Support definitiv nicht vermeiden lässt (Trennung vom Internet, Firewall/Gateway, Sprung- oder Rendezvous-Server, Virtualisierung und ergänzende Sicherheitsvorkehrungen am Hostsystem, erweiterte Protokollierung und Überwachung, Härtung). Denken Sie auch an Funktechnogien (WLAN, Zigbee, BLE, Mobilfunk).

Der Austausch von IoT kann teuer und logistisch komplex sein, insbesondere wenn er nicht frühzeitig im Beschaffungslebenszyklus berücksichtigt wurde. Jedoch kann eine Verzögerung des Austauschs die Kosten und technischen Herausforderungen in Zukunft nur noch verschlimmern. Je länger veraltete IoT in der Kommune verbleibt, desto schwieriger wird es, Mitarbeiter oder Dienstleister mit dem nötigen Know-How zu finden, um sie sicher zu betreiben und abzulösen.

Ausschalten der Geräte, wenn diese nicht benötigt werden

Stromlos geschaltete Geräte sind über das Netzwerk nicht mehr erreichbar.
Viele Geräte unterstützen den WOL-Standard (Wake-on-LAN). Damit können softwareseitig ausgeschaltete Geräte über ihre Netzwerkkarte wieder eingeschaltet werden. Die WOL-Einstellung kann im BIOS/UEFI oder in der Firmware aktiviert werden. Sollten Sie diese Funktion nicht nutzen, deaktivieren Sie diese.

Tipp:

Schalten Sie unbenutzte Geräte aus und vermeiden Sie damit unnötige Risiken einer Schadsoftwareinfektion.

Entsorgung der Geräte

Auf IoT-Geräten können interne Informationen, wie bspw. WLAN-ID, WLAN-Schlüssel gespeichert sein. Mit Hilfe dieser Informationen könnten Angriffe durchgeführt werden.

Tipp:

Sie sollten alle Daten auf den zu entsorgenden Geräten sicher löschen. Dies kann durch zurücksetzen auf Werkseinstellung oder durch Zerstörung des Geräts erfolgen.

IoT-Geräte im Gesundheitssektor

Selbst einfache medizinische Geräte wie Fieberthermometer und Blutdruckmessgeräte können inzwischen über Bluetooth und WLAN kommunizieren. Für komplexere Geräte wie Herzschrittmacher oder bildgebende Geräte sind diese Möglichkeiten längst Standard. Es existieren zahlreiche auf IoT-Systeme spezialisierte Schadsoftware-Varianten wie z. B. Mirai und Gafgyt.

Tipp:

Aufgrund des hohen Schutzbedarfs bei medizinischen Geräten, sollten Sie hier äußerst sorgfältig vorgehen. Denken Sie an Geräte in abseits gelegenen Bereichen und Außenstellen, welche über WLAN kommunizieren. Richten Sie Ihre Aufmerksamkeit auch auf mobile IoT, Reservegeräte oder Fremdgeräte wie Leihinfusionspumpen.

Einige Beispiele von IoT-Geräten (ohne klassische IT-Geräte und ohne Anspruch auf Vollständigkeit)

- Zutrittssysteme, Fluchttürensteuerung, Schließanlagen, Gegensprechanlagen
- Beleuchtung, Licht- und Audiosteuerung
- Überwachungs- und Meldesysteme
  (Alarmanlagen, Überwachungskameras, -mikrofone)
- Brandmeldeanlagen, Lösch- und Entrauchungsanlagen

- Sensoren und Thermostate für Wärme, Luftfeuchte, Wasser, Gase
- Gebäudeautomation
  (Mess-, Steuer- und Regelsysteme für Heizung, Klima, Lüftung, Jalousie, Sprinkler)
- Stromversorgung (auch USV)
- Chemische Laborsysteme
- Prozessleittechnik für Anlagen (Wasseraufbereitung, Wetter, Verkehrstechnik)
- Kassensysteme und -automaten
- Aufrufanlagen
- Kiosk-Systeme und Veranstaltungstechnik (Auskunftssysteme, digitale Wegweiser und Beschilderung, Besucherzähler, Lautsprecher)
- Hausgeräte mit IT-Schnittstellen (Waschmaschinen, Kühlschränke, Staubsauger)
- Werkzeugmaschinen mit IT-Schnittstellen
- Mobile Roboter
- Navigations-, Kommunikations- und Multimedia-Systeme in Fahrzeugen
- Telefonanlage, Session Border Controller (SBC), Telefonendgeräte, Faxgeräte
- Mobile Endgeräte (Smartphone, Tablet, Notebook, Surface)
- Beamer (Achtung vor gleichzeitiger Nutzung von LAN und WLAN-Anschluss)
- Dokumentenkameras mit Netzwerkanschluss
- Digitalkameras mit WLAN-Anschluss
- MDE–Geräte (Mobile Datenerfassung) wie Barcodescanner
- Smart-TV, Internetradio

Denken Sie auch an Geräte in Schulungsräumen, Testsystemen, Systemen für Qualitätssicherung und Umgebungen für Software-Installationen.

KONTAKT

Weitere Informationen finden Sie unter:
https://lsi.bayern.de/kommunen/
Für Unterlagen und Beratung wenden Sie sich bitte per E-Mail an:
Beratung-Kommunen@lsi.bayern.de.
Gerne ist das kommunale Beratungsteam auch telefonisch unter 0911 21549-523 für Sie erreichbar.

Landesamt für Sicherheit in der Informationstechnik – Leitfaden T#04 Das Internet der Dinge – IoT (Stand: 01.10.2024)