KLEINE DINGE – GROSSE WIRKUNG

Security@IoT

München, 20.2.2018

Dr. Helmut Petritsch

MOTIVATION

CONFIDENTIALITY

TELEGRAPH.CO.UK

INTEGRITY

HEISE.DE

AVAILABILITY

THEHACKERNEWS.COM

The Hacker News™
Security in a serious way

An Army of Million Hacked IoT Devices Almost Broke the Internet Today

Friday, October 21, 2016 Mohit Kumar

3 SCHUTZZIELE

CONFIDENTIALITY

Vertraulichkeit

Babyfon, Fernseher (Mikrofon und Kamera) ...

Sensordaten, Betriebsspionage ...

INTEGRITY

Integrität

Türschloss, Herzschrittmacher ...

Produktmanipulation, Haftungsfragen ...

AVAILABILITY

Verfügbarkeit

Wirtschaftliche Schäden bei Ausfall

Distributed Denial of Service (DDoS)

Keine Möglichkeit der Verteidigung
(bei ausreichend großen Angriffen)

FEHLT DA NICHT NOCH ETWAS?

PRIVACY

dilbert.com/strip/2013-08-15

PRIVACY

Kontrollverlust

Welche Daten werden wann bzw. wie oft erhoben und wo gespeichert, kopiert, verkauft?

Aber: **keine** Security-Frage!

HAFTUNG

xkcd.com/1807

HAFTUNG

Hersteller vs. Betreiber

DDoS

Fehlende Zustimmung

Juristische Fragen

Gesellschaftliche Probleme

SAFETY

WAS IST ANDERS?

für Security@IoT

KONFIGURATION

Kein GUI

Kein Benutzer, der Passwörter setzt

BILLIG

Device muss billig sein

Kein Geld für Software (Updates)

Keine Ressourcen für aufwändige Schutzmechanismen

QUALIFIKATIONEN

Hardware- und Software-Wissen erforderlich

Interdisziplinär

SICHERHEIT DURCH REDUNDANZ

Wenn es viele Sensoren gibt, müssen viele Geräte übernommen werden

Stimmige Daten zu fälschen ist schwierig

WAS (ANDERS) MACHEN?

VERTRAUENSGRENZEN

Identifzieren und absichern

Syntaktische und semantische Input-Validierung

Vertrauensfragen entscheiden können

UPDATES

Erstellen (Abhängigkeiten 3rd Party)

Verteilen (Infrastruktur / Erreichbarkeit)

Fälschungssichere Updates

Kein Downgrade auf alte (unsichere) Version

SICHERE KONFIGURATION

Inbetriebnahme

Anpassungen im Betrieb

Besitzerwechsel

ANGRIFFE

Erkennen: Gerät wurde korrumpiert

Reagieren: Daten verwerfen, Gerät entfernen

FRAGENKATALOG

BOOTSTRAPING

Sichere Integration in Umgebung

BUILDS

Patches vs. Upgrades

Abhängigkeit von 3rd Party (Patches)

UPDATES

Updates können (zeitnah) ausgespielt werden

Geräte können nicht durch (gefälschte) Updates korrumpiert werden

Geräte können nicht auf unsichere Versionen zurückgesetzt werden

KEINE SHARED SECRETS

Auslesen eines Gerätes kompromitiert nicht alle anderen Geräte

AUTHENTIFIZIERUNG VON GERÄTEN

Daten einzelner Geräte können verworfen werden

Einzelne Geräte können aus dem Netz entfernt werden

AUTORISIERUNG

Verteilung von Daten nur an berechtige Geräte

VERSCHLÜSSELUNG

Sensible Daten sind abhörgesichert

SIGNIERTE NACHRICHTEN

In das Netzwerk injizierte Nachrichten können als solche erkannt und gefiltert werden

KEINE REPLAY-ATTACKEN

Erkennen mehrfacher Aufrufe

Idempotenz

ENTSORGUNG

Ein entsorgtes Gerät kann wiederverwendet werden

CONCLUSIO

Unsicheres Design bleibt auch
mit Verschlüsselung unsicher

Security@IoT bringt nichts fundamental Neues

Interdisziplinär

DISKUSSION

iteratec

KOMPETENZ, DIE ENTLASTET

Kontakt:

Dr. Helmut Petritsch
helmut.petritsch@iteratec.de
St.-Martin-Str. 114
81669 München