Stiftung Neue Verantwortung

Protokoll IT-Sicherheit im Internet der Dinge – Workshop, 20. September 2016.

Clustering: Zentrale Herausforderungen für IoT-Sicherheit

Rot = Dringlichkeit, Blau = Politische Handlungsmöglichkeiten

1. **Größere Angriffsfläche** ●
   a. Verbreiterung / Diffusion der Angriffsvektoren (größere Schäden durch kleinere Gegner)
   b. Diffusion der Verteidigung/Sicherung militär. Systeme (Konsequenzen für nationale Sicherheit) ●

2. **Fehlende Updates** ●●●●●● ●●●●
   a. Fehlende Update-Mechanismen ●●●
   b. Upgrade Capabilities ●●● ●●●●
   c. Patchmanagement (Mangel an automatisiertem Management)
   d. Verantwortung der Nutzer (Kein Problemverständnis, wie „updaten“?)
   e. Oft veraltete Software, kaum Kontrolle für Nutzer, kaum Patchmöglichkeiten

3. **Standardisierung** ●●●●●●●●●● ●●●●●●●●
   a. Übergreifende Sicherheitsstandards finden (Security + Safety) ●
   b. Establishing clear standards (security + testing) ●●● ●●●●
   c. Internationale Dimension: Wo findet Standardisierung statt? (aktuell Asien) ●●● ●●●
   d. Mangelnde Vereinheitlichung aufgrund wirtschaftlicher Interessen (unique selling point)
   e. Verfügbarkeit hinreichender und offener technischer Sicherheitsstandards / Skalierbarkeit von (teurer) Sicherheitstechnologie ●● ●
   f. IoT bei den Diensten / Militär (Zertifizierung, Lagebild)
   g. Zertifizierung ● ●

4. **Welche Rolle übernimmt der Staat?** ●● ●●●●●
   a. Verpflichtung zur Einhaltung von Sicherheitsstandards
   b. Gewährleistung der bürgerlichen Freiheitsrechte
   c. Verfügbarkeit vertrauenswürdiger Lieferanten
   d. Gewährleistung der öffentlichen Sicherheit

5. **Paradigmenwechsel (alte Konzepte vs neue Probleme)** ●●●●●●●●●●●●● ●●●●●●●●●●
   a. Paradigmenwechsel IT-Sicherheit ●● ●●
   b. Hersteller von IoT-HW/SW müssen Sicherheitsprinzipien mit-designen und implementieren (für alle Komponenten, Cloud-Dienste und physische Systeme) ●●●●●● ●●●

c. Fehlende Budgetierung von IT-Sicherheit ●● ●
d. Illusion der „sicheren Zonen“
e. Skalierbarkeit ●
f. New Understanding of (IoT)Ecosystem (Manufacturer, Developer, Deployer, Operator)
g. Mainstreaming risk analysis (privacy impact assessment)
h. Inhärente Sicherheitseigenschaften neuer Technologien (Security by Design) ●● ●●●
i. Unterschiedliche Geschwindigkeiten (Old vs New Economy)
j. Steigende Lebensdauer der Geräte ●●
k. Data Integrity ●
l. Autonome Sicherheit („Teilnetze“)

6. Capacity Building und Informationsaustausch ●● ●●●●●

a. IT-Security Know-How fachfremder Branchen ●
b. Communication with end-users about data usage and risks
c. Mangelnde Capacity (nicht nur Endnutzer)
d. Informationsaustausch („Kultur der Offenheit“) ● ●●●
e. Bewusstsein, Transparenz, Vernetzung ● ●

7. Komplexität vernetzter Systeme ●●●● ●●●●

a. Strukturelle Komplexität und Dynamik
b. Kontrollverlust ●● ●
c. Fehlende (analoge) Fallback-Mechanismen ●●
d. Entkopplung: Sicherheit / Wettbewerb (Monopolstruktur)
e. Horizontalisierung (System of Systems) ●●
f. Monokultur der Betriebssysteme (fast alles nur OEM)
g. Multinationale Vernetzung und entsprechende „fehlende“ Kontrolle ●

Stiftung Neue Verantwortung

Notizen

- Vernetzung in der Industrie wird immer komplexer. Diese **„Systeme von Systemen“** setzen sich aus den unterschiedlichsten Herstellern zusammen, nutzen unterschiedlichste Protokolle und Standards und entziehen sich immer stärker der Kontrolle des Unternehmens.

- Hersteller haben oft kein (wirtschaftliches) Interesse daran, Zugriff auf die **Rohdaten** der Sensoren und Geräte zu geben.

- Es fehlt eine „Kultur der Offenheit“ hinsichtlich des **Informationsaustauschs**. Viele Branchen fingen erst an Threat Intelligence zu teilen, als sie dazu gesetzlich gezwungen wurden.

- IT-Sicherheit fokussiert vorrangig auf den Schutz der Vertraulichkeit und Verfügbarkeit von Daten – Schutz der **Datenintegrität** wird jedoch immer wichtiger im Internet der Dinge.

- Wenn zunehmend Systeme mit langen Produktlebensdauern vernetzt werden (Industrie-Maschinen, Autos, etc.) wächst die Diskrepanz zwischen Produktlebensdauer und **Supportzeitraum**.

- IoT-Hersteller stehen in der Verantwortung bei neuen Produkten von Anfang an einen **Security-by-Design** Ansatz zu verfolgen – sowohl für das Gerät selbst als auch für eingesetzte Cloud-Dienste und Schnittstellen.

- Wir stehen hinsichtlich IoT-Security vor einem **Paradigmenwechsel**: Es braucht Lösungen, die für Milliarden von Geräten skalieren.

- Unklar ist, wie **IoT-Hardware Hersteller** einzubeziehen sind, die vorrangig in **Asien** (Taiwan) sitzen und daher nicht direkt reguliert werden können.

- Kurz- und mittelfristig ist eine harte Regulierung in bestimmten Bereichen (Upgrades, Security-by-Design, etc.) evtl. nicht nötig sondern das Entwickeln von **Best Practices und Guidelines** zielführender. (siehe I am the Cavalry, OWASP)

- **Siegel** wurden kritisch betrachtet, da die Systeme zum einen zu komplex sind und eine Überprüfung zur Erlangung eines Siegels lediglich eine Momentaufnahme darstellt. Gleichzeitig fehle es an pragmatischen, handhabbaren Zertifizierungsmechanismen.

- Dem Problem der mangelnden Update/Upgrade-Möglichkeiten könnte durch **Softwarehaftung** begegnet werden.