softScheck
we identify vulnerabilities others don't

12 Grundregeln zur Informationssicherheit in Embedded Systems

1. **Völlige physische und logische Abkopplung vom Internet**

   Embedded Systems sollten wenn irgend möglich vom Internet völlig getrennt sein. Durch die Abkopplung vom Internet sind Angriffe entscheidend erschwert (stark eingeschränkte Attack Surface).

2. **Kommunikationsverbindungen**

   Die Zahl der Kommunikationsbeziehungen muss generell minimiert werden. Wartungsverbindungen zu Embedded Systems sollten grundsätzlich nicht von Seiten des Wartungsunternehmens initiiert werden. Initiieren der Verbindungen darf nur lokal am Embedded System vom Betreiber - zeitlich und organisatorisch stark eingeschränkt - zulässig sein. Durch diese Einschränkungen werden Angriffe über die Wartungsschnittstelle erschwert.

3. **Firewall, IDS, IPS**

   Grundsätzlich sollten nach Außen nur Dienste angeboten werden, die unverzichtbar zur Produktion gebraucht werden. Weitere Restriktionen (z.B. dedizierter IP-Adressbereich) sind über (gern auch mehrere!) Firewalls möglich. IDS und IPS wirken hierbei unterstützend, um Anomalien in den Zugriffen auf die angebotenen Dienste zu erkennen und damit Angriffe zu erschweren. Teilnetze sollten stark segmentiert und untereinander durch Firewalls abgeschottet werden.

4. **Identifizierung und Authentifizierung**

   Konfigurierungen an Embedded Systems sollten nur nach erfolgreicher Authentifizierung möglich sein. Hierbei sollten nur starke Authentifizierungsverfahren (z.B. Passwort, Smartcard inkl. Verschlüsselung) verwendet werden, um Zugriffe Unberechtigter zu erschweren.

5. **Passwörter**

   Zur Authentifizierung sind Passwörter unverzichtbar – mindestens 8 Zeichen lang bestehend aus alphabetischen Zeichen, Ziffern und Sonderzeichen (#`*+~ etc.) und je nach Wert und Bedeutung des zu steuernden Prozesses nach jedem Zugriff (!), stündlich, täglich, wöchentlich, monatlich gewechselt werden. Passwörter müssen verschlüsselt gespeichert werden – besser noch wird nur der Hashwert (Prüfsumme) gespeichert.

6. **Protokollierung und Auswertung**

   Jede Änderung an Embedded Systems sollte automatisch protokolliert werden. Das protokollierende System darf nur erweiternd (appending) in die Protokolle schreiben. Auswertungssysteme dürfen nur lesenden Zugriff haben. Protokolle sind (Tool-gestützt) auszuwerten. Damit können Angriffe wenigstens erkannt werden.

7. **Software-Entwicklung**

   Entwicklungsumgebungen sind als System mit direkter Verbindung zum Embedded System zu sehen und sollten entsprechend gut abgesichert werden.

8. **Least Privilege**

   Jeder Prozess sollte mit den geringst-nötigen Rechten ausgeführt werden, um bei Kompromittierung die Auswirkungen zu minimieren.

9. **Eingabe Validierung**

   Alle Eingabedaten sind als nicht-vertrauenswürdig anzusehen und müssen durch Filter validiert werden.

10. **Security Testing**

    Sicherheitstest sollten in den Entwicklungsprozess integriert werden, damit sie fortlaufend, vollständig und möglichst automatisch durchgeführt werden. Umgehen der Sicherheitstest darf zu keiner Zeit möglich sein. Getestet werden darf nicht von den Programmierern. Die Sicherheitsprüfungen beginnen in der Requirements-/Designphase und enden beim implementierten Code.

11. **Vertrauenswürdige Umgebung (Trusted Environment)**

    Alle gekoppelten angrenzenden Systeme sollten mindestens dem Sicherheitsniveau des Embedded Systems entsprechen. Die angrenzenden Systeme sollten auf ein notwendiges Minimum reduziert werden. Private Geräte inkl. Mobile Devices wie USB-Sticks, -Platten und Handys dürfen nicht angeschlossen werden können. Ihre Nutzung ist in kritischen Umgebungen zu unterbinden.

12. **Sicherheitsrichtlinie**

    Alle diese Maßnahmen müssen in einer Sicherheitsrichtlinie zusammengefasst und kontrolliert werden.