**Vernetzte Komponenten (IoT) sind das Rückgrat der digitalen Zukunft – und benötigen angemessenen Cyber-Schutz**

**Risikoadäquater Cyber-Schutz-Katalog für Komponenten und Systeme**

Die digitale Transformation und die damit verbundene Vernetzung von Geräten und Komponenten verändert unsere Wirtschaft und Gesellschaft bereits heute dramatisch. In den nächsten Jahrzehnten wird dieser Trend noch gravierend zunehmen. Diese Vernetzung der Geräte spielt sich dabei im Wesentlichen im Internet der Dinge (IoT) ab. Dort lassen sich durch die geschickte Kombination von Sensoren und Aktoren, der Programmierung und Datenauswertung zusehends neue Anwendungsgebiete erschließen. Die Geschwindigkeit, mit welcher diese neuen Anwendungsgebiete entstehen, ist dabei teils atemberaubend und viel zu oft geht diese Schnelligkeit der Weiterentwicklung zu Lasten der Gründlichkeit auf technischer Seite.

Gründlichkeit in Sachen technischer Ausgereiftheit, Stabilität und Sicherheit von Anwendungen sind nicht nur – aber besonders - im sicherheitskritischen Umfeld unabdingbar, wie z. B. im Brand- oder Einbruchschutz. Viel zu oft kann man in jüngerer Vergangenheit den Medien entnehmen, dass es Sicherheitsforschern wieder einmal gelungen ist, eine Komponente aus der Ferne zu überlisten und diese z. B. außer Betrieb zu setzen. Erforscht man die Ursachen dieser Hacks wird oft schnell klar, dass die Hersteller solcher Produkte das Thema Cyber-Sicherheit im Entwicklungsprozess sehr vernachlässigt haben. Fehlende Absicherung von Benutzerzugängen, unzureichend geschützte Datenübertragungen oder Softwarebugs, die durch fehlendes Patch-Management Angreifern über Jahre hinweg Tür und Tor offen lassen, sind dabei leider an der Tagesordnung.

VdS Schadenverhütung ist deshalb als 100%ige Tochtergesellschaft des Gesamtverbandes der Deutschen Versicherungswirtschaft (GDV) beauftragt worden, das Niveau der Cyber-Sicherheit bei IoT-Produkten mit Fokus auf den Bereich der Brandschutz- und Sicherheitstechnik maßgeblich zu erhöhen. Mit ihrem fundierten Wissen in diesem Wirtschaftsbereich und der langjährigen Erfahrung bei der Prüfung und Zertifizierung von Errichtern und Produkten des Sicherheitssektors entwickelt VdS zur Zeit Richtlinien, welche nachweislich die Cyber-Sicherheit der Produkte steigern werden und für die Anwendung in der Sicherheitstechnik maßgeschneidert sind.

Wesentliche Anforderungen sind:

**1. Allgemeine Cyber-Sicherheitsaspekte**

* Anforderungen an die Verwaltung von Schnittstellen zu Netzwerk und Komponenten
* konsequente Anwendung des „Security by Design“-Prinzips
* Herstellung eines sicheren Grundzustandes
* sichere Handhabung von Fehlfunktionen und Störungen

**2. Sicheres Benutzer- und Zugriffsmanagement**

* risikoadäquat gesicherte Authentisierung von Benutzern (auch Multi-Faktor-Authentifizierung)
* Integritätsprüfung von Eingaben
* Beschreibung eines Rechtemanagements für Mensch- und Maschinezugriffe
* Berücksichtigung des Minimalprinzips

**3. Sicherstellung von Vertraulichkeit und Integrität**

* Verschlüsselte Übertragung und Speicherung der Daten
* Integritätsprüfung für eingehenden Daten und Befehle

**4. Erfassung von Ereignissen und Protokollierung**

* Erfassung sicherheitskritischer Ereignisse
* fälschungssicheres Logbuch
* unmittelbare Meldung kritischer Vorgänge und Zustände

**5. Begleitende Maßnahmen**

* transparente Angabe, bis wann die Komponente mit Sicherheitsupdates versorgt wird
* Sicherstellung eines risikoadäquaten Updatemanagements
* transparente Einstellungen zur automatisierten Datenübertragung an Hersteller oder Drittverwerter (sog. „Call-Home“-Funktionen)
* DSGVO-konforme Datenverarbeitung

Um die Akzeptanz der Anforderungen sicherzustellen, dürfen die Anforderungen nicht über das Ziel hinausschießen, vielmehr müssen sie risikoadäquat nivelliert werden. Hierzu wird auf das bewährte VdS-Klassenkonzept zurückgegriffen. Klasse A markiert dabei die Baseline für alle Produkte, Klasse C entsprechend das höchste Niveau. Im Rahmen einer individuellen Risikoanalyse können einzelne Sicherungsmaßnahmen neu bewertet und an den speziellen Anwendungsbereich angepasst bzw. durch anderweitige Maßnahmen ersetzt werden. So ist größtmögliche Flexibilität gewährleistet.

Die Richtlinien VdS 3836 „Cyber-Sicherheit für softwaregesteuerte Systeme und Komponenten der Brandschutz- und Sicherheitstechnik“ werden mit den Verbänden gemeinsam erarbeitet und berücksichtigen relevante Bausteine der Edition 2019 des aktuellen Grundschutz-Kompendiums des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ebenso wie international anerkannte Standards. So wird größtmögliche Akzeptanz sichergestellt. Vor der endgültigen Veröffentlichung durchlaufen die Richtlinien ein öffentliches Konsultationsverfahren. Die Veröffentlichung ist noch im Jahr 2019 geplant.