VdS Whitepaper

VdS 3836 – Cyber-Sicherheit für Systeme und Komponenten Risikoorientierter Cyber-Security-Nachweis für Ihre IoT-Produkte

Elementare Bedeutung der Cyber-Security

Die Ausstattung vieler Systeme und Komponenten (im Weiteren Komponenten genannt) mit Netzwerkfunktionalität (z. B. IoT-Produkte) schreitet voran. Aufgrund der zunehmenden Vernetzung softwarebasierter Komponenten und dem damit verbundenen zunehmenden Datenaustausch untereinander steigt auch das potentielle Schadensrisiko bei Ausfall solcher Komponenten.

Komponenten, die in

- Überfall- und Einbruchmeldeanlagen
- Brandmelde- und Sprachalarmanlagen
- Wächterkontroll- und Sicherungsanlagen
- Feuerlöschanlagen
- Zutrittskontrollanlagen
- Videosicherheitsanlagen und -managementsystemen
- anderen Gefahrenmelde- und -alarmierungsanlagen

zum Einsatz kommen, müssen nicht nur sicher und zuverlässig ihren eigentlichen Zweck erfüllen. Wenn sie vernetzt werden, muss auch die Cyber-Sicherheit dieser Komponenten gewährleistet sein. Damit wird die Cyber-Security zu einer weiteren elementaren Säule bei der Betrachtung der Wirksamkeit und Zuverlässigkeit von Systemen und Komponenten der Brandschutz- und Sicherheitstechnik.

Nachweis durch VdS-Anerkennung

Zum Nachweis eines angemessenen Cyber-Sicherheitsniveaus für diese Komponenten bietet VdS Schadenverhütung GmbH eine hervorragende Möglichkeit zur Anerkennung der Cyber-Sicherheit für Komponenten der Brandschutz- und Sicherheitstechnik: Die Richtlinien VdS 3836. Die Prüfung und Zertifizierung wird zusätzlich zur zugrundeliegenden Produktanerkennung durchgeführt. Dies kann parallel oder nachträglich erfolgen.

Erfolgreich auf Grundlage der VdS 3836 geprüfte und zertifizierte Komponenten dürfen mit dem eigens für dieses Verfahren zur Verfügung gestellten Logo vom Anerkennungsinhaber gekennzeichnet werden.

Struktur und Inhalt der VdS 3836

Die Richtlinien VdS 3836 berücksichtigen dabei bereits etablierte Regelwerken auf diesem Gebiet. Durch die Berücksichtigung etablierter Methoden dieser Regelwerke und die Adaption der Anforderungen an die speziellen Bedürfnisse der Brandschutz- und Sicherheitstechnik, garantiert die VdS 3836 somit neben der Cyber-Sicherheit auch die Kompatibilität der Verfahren untereinander. Dazu zählen insbesondere:

- IEC 62443, Normenreihe Industrial communication networks – Network and system security
- Positionspapier des Gesamtverbandes der Deutschen Versicherungswirtschaft (GDV) zu den Anforderungen an Smart Home Installationen sowie Geräten des „Internet der Dinge“
- ETSI TS 103 645 Technical Specification, Cyber; Cyber Security for Consumer Internet of Things

Die Anforderungen an Komponenten und Systemen in diesen Richtlinien sind in drei unterschiedliche Klassen (im Sinne von Sicherheitsleveln) strukturiert: Klasse A, Klasse B und Klasse C. Je nach Einsatzzweck der Komponenten sind die Anforderungen risikoadäquat gestaffelt und bilden somit für unterschiedliche Anwendungsfälle passende Anforderungsprofile ab. Ausschlaggebend für die Einstufung sind u. a. der übliche Anwendungsfall und dessen Schutzziel sowie die bei dem Anwendungsfall zu erwartende Gefährdung der Komponente.

Im Vergleich zu den Anforderungen der Normenreihe IEC 62443 ergibt sich folgende Korrelation:

- Klasse A orientiert sich an Security Level 1
- Klasse B orientiert sich an Security Level 2
- Klasse C orientiert sich an Security Level 3

Sie haben Fragen?

Für Rückfragen stehen wir Ihnen gerne zur Verfügung.

Christian Metzmacher
Produktmanagement Brandschutz / Security
IT-Security & IoT
+49 (0) 221-7766-370
cmetzmacher@vds.de

VdS Schadenverhütung GmbH
Amsterdamer Str. 172–174 | 50735 Köln

vds.de/de/3836

Die nachstehende Tabelle stellt die klassenabhängig gestalteten Anforderungen der Richtlinien VdS 3836 übersichtlich dar (Seite1/2):

Anforderungen	Klasse A	Klasse B	Klasse C
Allgemeine Anforderungen			
Gewährleistung von Offline-Funktionalität („Notbetrieb“)	op	m	m
Herstellung eines sicheren Zustandes (Security by Default)	m	m	m
Anpassung der Konfiguration	op	m	m
Handhabung von Fehlfunktionen und Störungen	op	m	m
Vorbestimmter Zustand von Schnittstellen	op	m	m
Funktionalität für sichere Außerbetriebnahme der Komponente	op	m	m
Manipulationssicherheit	m	m	m
Minimierung von Auswirkungen eines Denial-of-Service-Vorfalls	op	m	m
Notstromversorgung	op	m	m
Anforderungen an Benutzer-/Zugriffsmanagement			
Zugriffsschutz durch Authentisierung	op	m	m
Verzicht auf fest codierte Zugangsparameter	op	m	m
Individualisierte Benutzerkonten	op	m	m
Minimale Zugriffsrechte von Benutzerkonten	m	m	m
Zusätzlicher Zugriffsschutz bei (sicherheits-)kritischen Daten	op	op	m
Beendigung der Kommunikationssitzung bei Inaktivität	op	m	m
Anforderungen an die Vertraulichkeit und Integrität			
Verschlüsselung von Daten bei der Übertragung (Transportverschlüsselung)	m	m	m
Integrität von Daten bei der Übertragung	m	m	m
Gewährleistung der Integrität der Software	op	op	m
Plausibilität von Benutzereingaben/-aktionen	op	m	m
Sicherung von System-/Konfigurationsdaten	op	m	m
Sicherung von Nutzdaten	op	m	m

op = fakultativ (optional), m = obligatorisch (mandatory)

Sie haben Fragen?

Für Rückfragen stehen wir Ihnen gerne zur Verfügung.

Christian Metzmacher
Produktmanagement Brandschutz / Security
IT-Security & IoT
+49 (0) 221-7766-370
cmetzmacher@vds.de

VdS Schadenverhütung GmbH
Amsterdamer Str. 172–174 | 50735 Köln

vds.de/de/3836

Die nachstehende Tabelle stellt die klassenabhängig gestalteten Anforderungen der Richtlinien VdS 3836 übersichtlich dar (Seite 2/2):

Anforderungen	Klasse A	Klasse B	Klasse C
Protokollierung/Ereigniserfassung			
Überwachung/Protokollierung von Ereignissen (Audit Log)	m	m	m
Benachrichtigung bei sicherheitsrelevanten Ereignissen	op	op	m
Weitergehende Behandlung von protokollierten Ereignissen	op	m	m
Erfassung von Telemetriedaten	op	m	m
Zeitstempel und Zeitsynchronisation	m	m	m
Anforderungen an den Datenfluss			
Pairing mit weiteren Systemen/Komponenten	m	m	m
Fremdprodukte/-dienste	op	m	m
„Call Home"-Funktion	m	m	m
Verwaltung von Schnittstellen	op	m	m
Konfiguration von Remote-Zugängen	m	m	m
Begleitende Maßnahmen			
Vollständige Dokumentation der Komponente	m	m	m
Umfassende Bereitstellung Support	m	m	m
Automatische Update-Prüfung	op	m	m

op = fakultativ (optional), m = obligatorisch (mandatory)

Beratung

Viele Hersteller und VdS-Anerkennungsinhaber sind seit vielen Jahren erfolgreich in der Entwicklung und Konstruktion von Brandschutz- und Sicherheitskomponenten. Die Implementierung einer wirksamen Cyber-Sicherheit stellt dabei neue und zusätzliche Herausforderungen. VdS stellt die hohe fachliche Kompetenz zur Verfügung, um Sie dabei zu unterstützen. Wir bewerten vorab Ihre Lösung und leisten Hilfestellung dabei, Ihre Produkte und das Gesamtsystem wirksam abzusichern und auf die anschließende Prüfung durch versierte VdS-Kollegen vorzubereiten.

Sie haben Fragen?

VdS 5586 : 2021-02 (01)

Für Rückfragen stehen wir Ihnen gerne zur Verfügung.

Christian Metzmacher
Produktmanagement Brandschutz / Security
IT-Security & IoT
+49 (0) 221-7766-370
cmetzmacher@vds.de

VdS Schadenverhütung GmbH
Amsterdamer Str. 172–174 | 50735 Köln

vds.de/de/3836