

# Sächsisches Know-how setzt sich durch!

## Produktsicherheit in der Automobilindustrie

Von Peter Liebing

Die Rahmenanforderungen der ISO 27001 sind dadurch gekennzeichnet, dass bei der Entwicklung oder beim Testbetrieb von Prototypen oder Fahrzeugkomponenten ein besonderer Schutz des Designs und der Innovation erforderlich ist.

Die Unternehmen haben somit sicherzustellen, dass die der Geheimhaltung unterliegenden Prototypen sowie die sich in der Entwicklung befindlichen Konzepte sicher in unterschiedlichen Umgebungen entwickelt und getestet werden können.

Die Zertifizierung des Prototypenschutzes in Ergänzung zur ISO 27001 umfasst drei Säulen, wobei der Schwerpunkt klar auf die ersten beiden Punkte zu legen ist:

1. Strategische und organisatorische Kriterien des Informationsschutzes (Verfügbarkeit, Vertraulichkeit, Integrität)
2. Technische Kriterien der IT-Systeme (Verfügbarkeit, Vertraulichkeit, Integrität)
3. Klassische Sicherheitsaspekte: Prototypenschutz

Seit geraumer Zeit häufen sich die Anfragen bei digitronic nach entsprechenden Sicherheitslösungen unter dem Stichwort: Audit – 2-Faktor-Authentifizierung (2FA) und Schutz von vertraulichen Daten. Grund ist, dass die Automobilhersteller konsequent Ihre Zulieferer audieren, um sicher zu stellen, dass diese Betriebe die hohen automobilspezifischen Standards erfüllen.

Die Zwei-Faktor-Authentifizierung (kurz 2FA) dient dem Identitätsnachweis eines Nutzers mittels der Kombination zweier verschiedener Komponenten. Das kann etwas sein, was er weiß, etwas, was er besitzt, oder etwas, was untrennbar zu

ihm gehört. Aus dem Alltag ist dies z.B. vom Geldautomaten bekannt. Erst die Kombination aus Bankkarte und PIN ermöglicht die Transaktion. Die bekannteste Lösung zur 2-Faktor-Authentifizierung sind Hardware-Token. Das Wissen eines Passwortes wird hierbei um den Besitz eines Hardware Schlüssels ergänzt und ermöglicht so unternehmensweit die sichere Anmeldung der Benutzer am Windows Betriebssystem und schützt gleichzeitig vor Zugriff durch nicht berechtigte Personen.

digitronic bietet für diese Anforderung die clientbasierte Software Secure Logon an, welche diesen Zugriffsschutz unter Unterstützung des digitronic Security USB-Token mit integrierter Smartcard Technologie gewährleistet.

In Ergänzung zur 2FA Anforderung wird zusätzlich der Schutz von vertraulichen Daten verlangt und hier kommt nun die Verschlüsselung von Netzlaufwerken zum Tragen. Vielen der Unternehmen war bis dato die Gefahr durch Diebstahl von vertraulichen Daten nicht bewusst. Zwar schützen sich viele Unternehmen gegen Angriffe von außen, aber dies reicht heute nicht mehr aus. Auch der Schutz gegen „Angriffe“ von innen ist mehr als gefragt und inzwischen auch ein sehr wichtiges Kriterium der Audits geworden.

Mit dem digitronic® Produkt HiCrypt™ werden vertrauliche Daten auf Netzlaufwerken verschlüsselt, ermöglicht aber den Benutzern durch seine Architektur den gemeinsamen Zugriff auf verschlüsselte Dateien und Ordner. Die Ver- und Entschlüsselung findet am Arbeitsplatz-Computer statt. Dadurch ist sowohl die Datenübertragung zum Ablageort, als auch die Dateiablage selbst verschlüsselt. Unberechtigte Personen haben keine Möglichkeit, die verschlüsselten Informationen einzusehen. Die Verschlüsselung

der Daten erfolgt mit standardisierten, anerkannten Verschlüsselungsverfahren.

digitronic® bietet nach einer kritischen Bestandsaufnahme Best-Practice-Lösungen, die im Rahmen eines Audit-basierenden Roll-Outs an allen Standorten realisiert werden kann.

### Über digitronic®

Matthias Kirchhoff (55) gründete 1990 in Chemnitz die digitronic® computer-systeme gmbh und führt sie seitdem mit seinen Partnern. Seit 2011 ergänzt Stefan Ranft, Mitbegründer und langjähriger Kopf der Entwicklung, die Geschäftsführung. Das Unternehmen entwickelt seit nunmehr 23 Jahren Softwarelösungen für Polizeibehörden, Ministerien sowie mittlere und große Unternehmen.

Die Kernkompetenzen sind sichere Kommunikations-, Speicher- und Zugangslösungen. Verlässlich verrichten diese Systeme Nachrichtenübermittlungen und Datentransfers im normalen Geschäftsbetrieb der Behörden, aber eben auch in kritischen Situationen. Bei Katastrophen wie dem letzten Jahrhundert-Hochwasser, bei Terrorgefahren und schweren Unfallsituationen sorgen die von den digitronic-Ingenieuren entwickelten Lösungen für eine ausfallsichere Kommunikation.

Foto: fotolia

