Produktsicherheit bei Zulieferern der Automobilindustrie

Der Schutz von Geschäftsprozessen und vertraulichen Informationen ist eine der zentralen Aufgaben einer Unternehmensführung. Besonders durch die zunehmende Globalisierung und enge Zusammenarbeit von Unternehmen kommen zusätzliche Anforderungen hinzu – die Vernetzung von Geschäftsprozessen über Unternehmensgrenzen hinweg erfordert ein vergleichbares Schutzniveau aller Beteiligten. Gerade in der Automobilindustrie birgt diese Vernetzung nicht nur viele Chancen, sie macht auch anfälliger für externe und interne Bedrohungen.

Von Peter Liebing, TeleTrusT-Mitglied digitronic computersysteme gmbh (TeleTrusT Regionalstelle Chemnitz)

Zuliefererbetriebe, die in der Automobilindustrie erfolgreich sein wollen, müssen die ISO TS 16949 erfüllen. Speziell für die Automobilindustrie hat der Verband der Automobilindustrie e. V. (VDA) zudem Leitlinien und Richtlinien zur Implementierung von Standards in der Automobilzulieferindustrie und der Umsetzung von OEM-Anforderungen veröffentlicht (VDA 6.3). Ein Teilaspekt sind Audits, insbesondere gemäß der Rahmenanforderungen der ISO 27001: Diese 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 das Augenmerk klar auf die ersten beiden Punkte zu legen ist:

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

In unserer digitalen Zeit ist die Validierung von Identitäten und Zugriffskontrollen unerlässlich. Unter den Bedingungen der ISO 27001 sind die Einhaltung von IT-Sicherheitsrichtlinien (Virencheck, Datensicherung, Verschlüsselung, Multi-Faktor-Authentifizierung, Diebstahlschutz etc.) für PCs und Laptops mehr als nur eine grundlegende Anforderung, sondern unumgänglich. Für die Bereiche Verschlüsselung von vertraulichen Daten sowie Zwei-Faktor-Authentifizierung sind die im Folgenden beschriebenen Lösungen unerlässlich.

Authentifizierung

Die Zwei-Faktor-Authentifizierung (kurz auch 2FA genannt) dient dem Identitätsnachweis eines Nutzers mittels der Kombination zweier unterschiedlicher Komponenten. Die bekannteste Lösung zur 2FA sind Hardware-Token mit integrierter Smartcard-Technologie: Das Wissen einer PIN wird hierbei um den Besitz eines Hardwareschlüssels ergänzt und ermöglicht so die sichere Anmeldung des Benutzers und schützt gleichzeitig vor Zugriff durch unberechtigte Personen.

Geheime Passwörter (nur ein Faktor), die noch immer weitgehend zur Identifikation dienen, sind zu unsicher: Sie können erraten, weitergegeben oder bei der Übertragung mitgehört und dann missbräuchlich eingesetzt werden. Damit stellen klassische Passwörter eine bedrohliche Sicherheitsschwachstelle bei ansonsten guten Netzwerkprodukten und Serversystemen dar. Security-Verantwortliche über alle Unternehmensgrößen hinweg wissen um die Wichtigkeit einer starken 2FA-Lösung als Bestandteil einer umfassenden Strategie zum Informationsschutz – insbesondere in der Automobilzuliefererindustrie wird eine solche Lösung zum Standard.

Verschlüsselung

In Ergänzung zur 2FA-Anforderung wird zusätzlich der Schutz von vertraulichen Daten verlangt und hier bekommt die Verschlüsselung von Netzlaufwerken einen großen Stellenwert: Vielen Unternehmen war bis dato die Gefahr durch den Diebstahl vertraulicher Daten nicht hinreichend bewusst. Zwar schützen sich viele Unternehmen gegen Angriffe von außen, aber dies reicht heute nicht mehr aus: Besonders der Schutz gegen Bedrohungen von innen ist mehr als gefragt und inzwischen auch ein sehr wichtiges Kriterium der Audits geworden.

Wie wird dies umgesetzt? Vertrauliche Daten werden durch Softwarelösungen auf Netzlaufwerken verschlüsselt, ermöglichen aber den Benutzern dennoch einen gemeinsamen Zugriff auf verschlüsselte Dateien und Ordner. Die Ver- und Entschlüsselung findet am Arbeitsplatz-Computer statt, wodurch sowohl die Datenübertragung zum Ablageort als auch die Dateiablage selbst verschlüsselt erfolgt. Mit der „Schlüssel-Alleinbesitzgarantie" wird ein unbefugter Zugriff – beispielsweise durch eigene Mitarbeiter, Administratoren oder externe Dienstleister – sicher verhindert. Die Verschlüsselung der Daten erfolgt mit standardisierten, anerkannten Verschlüsselungsverfahren.

Fazit

Datenschutzverletzungen finden fast jede Woche statt – im vorigen Jahr sind mehr als 660 Millionen Datensätze aufgrund von Datenlecks in falsche Hände geraten (Quelle: www.privacyrights.org, Dezember 2013). Auf einen weiteren wichtigen Punkt sollten die Verantwortlichen Wert legen: dass der Anbieter von Lösungen die Kriterien der TeleTrusT-Initiative „IT Security made in Germany" (ITSMIG) erfüllt! ■