Vorfahrt für Informationssicherheit

Umfassender Schutz vertraulicher und geheimer Daten wird für Zulieferer immer wichtiger

Laut einer aktuellen Studie des BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. sind 51 Prozent aller Unternehmen in Deutschland in den letzten zwei Jahren Opfer von digitaler Wirtschaftsspionage, Sabotage oder Datendiebstahl geworden. Die deutsche Automobilindustrie war mit 68 Prozent der betroffenen Unternehmen der Wirtschaftszweig, der am stärksten gefährdet ist. Das ist sicherlich keine Überraschung, denn die deutschen Fahrzeugbauer und deren Zulieferer gehören zu den innovativsten Unternehmen nicht nur in Deutschland, sondern weltweit.

Interessant sind die Ursachen dieser Attacken: Bei fast zwei Drittel der befragten Unternehmen sind diese „vor Ort" verursacht worden. Dabei handelt es sich um gezielten Datendiebstahl durch aktuelle oder ehemalige Mitarbeiter. Neben Patenten, Bauplänen oder Konzepten für Produkte und Dienste sind auch Marketingaktionen, Kundendaten, Produktionspläne oder Mitarbeiterprofile von sehr starkem Interesse. Der Schaden, der aus digitaler Wirtschaftsspionage, Sabotage oder digitalem Datendiebstahl in Unternehmen hervorgeht, beläuft sich laut Studie auf 51 Milliarden Euro pro Jahr.

Große Herausforderung für Automobilzulieferer

Der umfassende Schutz von vertraulichen und geheimen Informationen, nämlich die Informationssicherheit, spielt in der heutigen globalen Welt eine immer größere Rolle und ist eine große Herausforderung für Zulieferer in der Automobilindustrie. Dank der großen Automobilhersteller wird in diesem Wirtschaftszweig beispielhaft mehr Wert auf Sicherheitsstandards gelegt. Zur Erfüllung dieser strengen Auflagen müssen sich Dienstleister, Zulieferer und Entwicklungspartner diesen Herausforderungen stellen.
Mit gutem Beispiel geht die Volkswagen AG bei diesem Thema voran. Ihr Ziel ist es, bei sensiblen Projekten ausschließlich nur mit Partnern zusammenzuarbeiten, die eine angemessene Informationssicherheit nachweisen können. Dieser Nachweis ist zwingende Voraussetzung dafür, dass die Partnerfirmen Zugriff auf vertrauliche und geheime Daten, Komponenten oder Prototypen von Volkswagen erhalten.

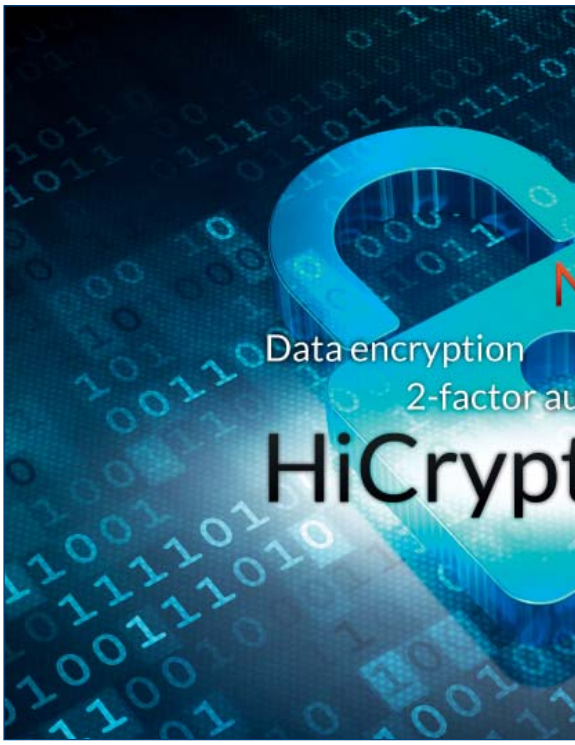
Nachweis angemessener Maßnahmen durch ISO 27001-Zertifikat

Dass eine Zulieferfirma angemessene Maßnahmen zur Informationssicherheit bei ihren Prozessen etabliert hat, kann durch ein ISO 27001-Zertifikat nachgewiesen werden. Alternativ haben die Automobilhersteller im VDA auch eine umfassende Selbstauskunft auf Basis der Anforderungen der ISO 27001 erarbeitet, anhand deren die Zuliefererfirmen den Reifegrad ihrer Informationssicherheit ermitteln können. Bei VW wird diese Selbstauskunft durch die Firma Operational Services geprüft und bei Bedarf ein Audit zur Überprüfung der Angaben bei der Partnerfirma durchgeführt. Anschließend wird über eine Freigabe der Partnerfirma entschieden.

Individuelle Lösungen für erfolgreiche Auditierungen parat

Das Chemnitzer Unternehmen digitronic computersysteme GmbH berät und begleitet seit mehr als zwei Jahren erfolgreich deutsche Automobilzulieferer, die sich den Audit-Anforderungen stellen müssen. Gemäß den Anforderungen eines Audits können individuelle Lösungen zum Einsatz kommen. Zum Beispiel kann für eine Zwei-Faktor-Authentifizierungslösung eine clientbasierte Software Secure Logon und ein digitronic USB Smartcard Token mit EAL 5+ Zertifizierung eingesetzt werden. Dank der Flexibilität der Software sind Lösungen auch bei schon vorhandenen Mitarbeiter-Ausweisen zur Anmeldung an Zeiterfassungssystemen oder Türöffnungssystemen umsetzbar.
Ergänzend zur Zwei-Faktor-Authentifizierung (Wissen und Besitz) wird zusätzlich der Schutz von geheimen und vertraulichen Daten verlangt. Insbesondere der Schutz gegen „Angriffe" von innen erhält immer höhere Priorität. Auch hier bietet digitronic Chemnitz mit HiCrypt 2.0 eine Daten-Verschlüsselung, welche die Anforderungen des Audits erfüllt und in der neuen Version auch eine Zwei-Faktor Authentifizierung mittels eines USB Smartcard Token oder Smartcard unterstützt.
Vor dem Hintergrund der Globalisierung, der Vernetzung von Geschäftsprozessen, der Zunahme von digitaler Wirtschaftsspionage und Datendiebstahl wird es immer dringender, sich den Herausforderungen des Schutzes von materiellen und immateriellen Werten zu stellen.

www.digitronic.net
www.hicrypt.com



Das Chemnitzer IT-Unternehmen digitronic hat ein Zwei-Faktor-Authentifizierungssystem entwickelt, das automobile Innovationen schützt.

Grafik: digitronic

ISO 27001 im Überblick

Die internationale Norm ISO/IEC 27001 geht auf den British Standard BS7799 zurück und wurde 2005 als international anerkannter und zertifizierbarer ISO-Standard veröffentlicht. Sie ist zentraler Bestandteil der ISO-27000-Normenreihe, die Sicherheitsmaßnahmen für den Schutz der IT in den Bereichen Vertraulichkeit, Verfügbarkeit und Integrität definiert.

Information security is the No. 1 priority

Comprehensive protection for confidential and secret data is becoming increasingly important for suppliers

The Chemnitz-based IT company digitronic has developed a two-factor authentication system which protects automotive innovations.

Graphic: digitronic

According to a recent study by BITKOM, the Federal Association for Information Technology, Telecommunications and New Media, 51 per cent of all companies in Germany have been victims of digital industrial espionage, sabotage or data theft in the last two years. The German automotive industry was the economic sector most at risk with 68 per cent of companies being affected. This is certainly no surprise, given that German vehicle manufacturers and their suppliers are amongst the most innovative companies not just in Germany but worldwide.

The sources of these attacks are especially interesting: At almost two-thirds of the companies surveyed, they were "inside jobs." These kinds of attacks were targeted thefts of data by current or former employees. Alongside patents, construction diagrams and concepts for products and services, thieves showed a great interest in marketing campaigns, customer data, production plans and employee profiles. The damage caused by digital economic espionage, sabotage or electronic data theft in companies amounts to 51 billion euro annually according to the study.

Enormous challenge for automotive suppliers

Comprehensive protection for confidential and secret information (information security for short) is playing an increasingly important role in today's globalized world and poses an enormous challenge for suppliers in the automotive industry. Thanks to the large automobile manufacturers, greater importance is being placed on security standards, and the sector is exemplary in this respect. To fulfill the stringent requirements, service providers, suppliers and development partners must face up to the challenges.
Volkswagen AG provides a good example as to how to tackle this issue. Its objective is to only collaborate on sensitive projects with partners who can demonstrate an appropriate level of information security. Proving this is an essential requirement if the partner company is to have access to Volkswagen's confidential and secret data, components or prototypes.

ISO 27001 certification provides proof of suitable measures

A supplier company can demonstrate that it has taken appropriate measures to ensure information security in its processes through ISO 27001 certification. As an alternative, the members of the German Association of the Automotive Industry (VDA) have drawn up an extensive self-certification scheme, based on the requirements of ISO 27001. Supplier companies can use this to assess their level of information security. At VW, this self-certification is reviewed by the company Operational Services, and an audit is performed where necessary to verify the information provided by partner company. Following this, a decision on whether to approve the partner company is taken.

Individual solutions for successful auditing at hand

The Chemnitz-based company digitronic computersysteme GmbH has been advising and supporting German automotive suppliers who have to meet audit criteria and helping them achieve success for more than two years. In line with the audit criteria, individual solutions can be applied. For example, the client-based software solution Secure Logon and a digitronic USB smartcard token with EAL 5+ certification can be used as a two-factor authentication solution. The flexibility of the software means that solutions can be put in place using existing employee passes for logging into time tracking systems or for door security systems.
In addition to two-factor authentication (something the user knows and something the user has), protection of secret and confidential data is required. Protection against inside "attacks" in particular is increasingly being prioritized. Here digitronic Chemnitz offers HiCrypt 2.0, which provides data encryption that meets the audit criteria, and the latest version also supports two-factor authentication using a USB smartcard token or smartcard.
Against the backdrop of globalization, the networking of business processes, the growth of digital economic espionage and electronic data theft, the need to rise to the challenges of protecting material and immaterial assets is becoming ever more pressing.

www.digitronic.net
www.hicrypt.com

ISO 27001 at a glance

The international standard ISO/IEC 27001 is based on the British Standard BS7799 and was published as an internationally recognized and certifiable ISO standard in 2005. It is a central part of the ISO 27000 series of standards, which defines security measures for the protection of IT in the areas of confidentiality, availability and integrity.