

Wer wir sind und was wir für Sie tun ...

digitronic[®]
net



Software-Entwicklung.
IT-Security-Beratung.
Innovationen.

Wer wir sind ...

Die digitronic[®] computersysteme gmbh (Sitz in Chemnitz) realisiert seit 1991 IT-Lösungen auf den Gebieten Kommunikation und digitale Vertraulichkeit. Mit klarem Fokus auf Zuverlässigkeit, Kundenfreundlichkeit und Funktionalität erarbeitet unser Team innovative Softwarelösungen. Wir sind Softwareentwickler und Dienstleister aus Leidenschaft. Unabhängig von der Art der Herausforderung, vor die Sie uns stellen: Wir konzentrieren uns auf das Lösen Ihrer Aufgabenstellung.

Mit mehr als 25 Jahren Erfahrung sind wir als Softwareentwickler etabliert, bestens vernetzt und kooperieren mit kompetenten Partnern. Mobile, plattformunabhängige Vertraulichkeit in Verbindung mit Smartphone-Technologie, die auch im Umfeld von Industrie 4.0 einsetzbar ist - das ist ein aktueller Forschungs- und Entwicklungsschwerpunkt in enger Zusammenarbeit mit Großkunden. digitronic[®] ist Regionalstelle im Bundesverband IT-Sicherheit e.V. TeleTrust und trägt das Siegel - IT-Security made in Germany -.

Was wir tun ...

Wir sehen unsere Aufgabe darin, den Schutz Ihrer Daten so zu gestalten, dass innerhalb bestehender Informationssicherheitskonzepte die Vertraulichkeit sensibler Daten gestärkt wird. Dafür entwickeln und vertreiben wir seit mehr als 15 Jahren erfolgreiche Produkte und Lösungen zur sicheren und komfortablen Anmeldung an Betriebssystemen sowie zur Verschlüsselung vertraulicher Daten auf Netzlaufwerken.

Unsere **All-In-One-Sicherheitspakete** verbinden diese Technologien mit Unterstützungsleistungen bei Ihnen vor Ort. Hier begleiten wir Sie bei den notwendigen Analysen und der Lösungserarbeitung ebenso, wie bei Testinstallationen und Implementierungsschritten. So wurden die Anforderungen an 2-Faktor-Authentifizierung und Teamverschlüsselung im Zuge von Zertifizierungen nach ISO 27001, Auditierungen nach VDA ISA und anderen Prüfungen der Informationssicherheit bei unseren Kunden bereits hundertfach erfüllt. Wir machen unser Know-how zu einem Mehrwert für Sie und Ihr Unternehmen.

Unser Beitrag für Sie im Bereich Automotive ...

Automobilzulieferer müssen ihre Informationssicherheit nach **VDA ISA** prüfen lassen, wenn sie Prototypen-, Entwicklungs- und Konstruktionsdaten mit Automobilherstellern austauschen. Seit 2017 finden solche Prüfungen herstellerübergreifend unter dem Dach der ENX Assoziation über **TISAX** statt. Es geht nicht mehr nur um den Zugang zum Konstruktionsdaten- und Verwaltungssystem (KVS) von Volkswagen, sondern um Zugänge zu den sensiblen Daten aller europäischen OEMs.

Gemäß den Prüfkriterien der VDA ISA sind sowohl Verfahren für einen abgesicherten Zugang zu Netzwerken, Applikationen und Daten als auch für die Verschlüsselung von Informationen bei deren Speicherung und Transport umzusetzen. Dabei unterstützen wir Sie mit prüfungsfesten, in über 15 Jahren ausgereiften, weiterentwickelten und stabilen Lösungen sowohl zur Verschlüsselung sensibler Daten auf Netzlaufwerken als auch zur sicheren und komfortablen Anmeldung an Betriebssystemen und Applikationen.

Bei welchen Controls der VDA ISA wir Sie mit unseren anerkannten Lösungen unterstützen können, haben wir auf der folgenden Seite zusammengestellt.

VDA ISA–Controls und unsere All-In-One-Lösungen

Control 9.1 (Access Control - Zugang zu IT-Systemen)

Zusätzlich bei sehr hohem Schutzbedarf:

- + Daten mit sehr hohem Schutzbedarf sind durch starke Authentifizierung (z. B. 2-Faktor-Authentifizierung) abzusichern.
Unsere starke 2-Faktor-Authentifizierung ermöglicht eine sichere und komfortable Anmeldung an Betriebssystemen. Die eingesetzten Token sind mindestens nach EAL 4+ (Common Criteria) zertifiziert und entsprechen damit den Anforderungen.

Control 9.5 (Access Control - Zugriff auf Informationen und Applikationen)

Zusätzlich bei sehr hohem Schutzbedarf:

- + Verschlüsselte Ablage von Daten zur Vermeidung von Zugriff und Kenntnisnahme durch nicht autorisierte Personen/Rollen (z. B. Administratoren) mindestens auf Dateiebene
Unserer Verschlüsselungslösung ermöglicht es, mittels einer separaten Benutzerverwaltung unautorisierte Zugriffe auf die zu schützenden Informationen auszuschließen, auch solche von Administratoren. Optional kann dieser Schutz verstärkt werden, in dem sich berechnigte Benutzer mittels einer 2-Faktor-Authentifizierung an der Verschlüsselungslösung authentifizieren müssen.

Control 10.1 (Cryptography)

Zusätzlich bei hohem Schutzbedarf:

- + Folgende Aspekte müssen dokumentiert sein:
 - Beschreibung der Schlüsselhoheit
Mit Hilfe der separaten Benutzerverwaltung unserer Verschlüsselungslösung wird die alleinige Hoheit über die Vergabe von Schlüsseln ausschließlich an einen Verantwortlichen (oder an mehrere Verantwortliche) für die Sicherheit der zu schützenden Informationen übergeben.
 - Hoheit der Verwaltung des Schlüsselmaterials bei externer Verarbeitung (z. B. in der Cloud)
Die Hoheit der Verwaltung des Schlüsselmaterials liegt stets bei dem (den) Verantwortlichen für die Sicherheit der Informationen, unabhängig davon, ob die Daten auf internen oder externen Servern gespeichert werden.
- + Informationen mit hohem Schutzbedarf sollten verschlüsselt transportiert oder übertragen werden.
Unsere clientbasierte Verschlüsselung von Daten auf Netzlaufwerken verschlüsselt und entschlüsselt die zu schützenden Informationen immer auf dem Client. Damit werden die Daten auch stets verschlüsselt transportiert und übertragen.

Zusätzlich bei sehr hohem Schutzbedarf:

- + Informationen mit sehr hohem Schutzbedarf **werden verschlüsselt gespeichert.**
Unsere Verschlüsselungslösung realisiert ein verschlüsseltes Speichern der zu schützenden Informationen mit sicheren und anerkannten Verfahren.

Kontakt

digitronic® computersysteme gmbh
Oberfrohaer Str. 62
09117 Chemnitz

Tel: +49 371 81539 0
Fax: +49 371 81539 900
E-Mail: vertrieb@digitronic.net
Internet: www.digitronic.net