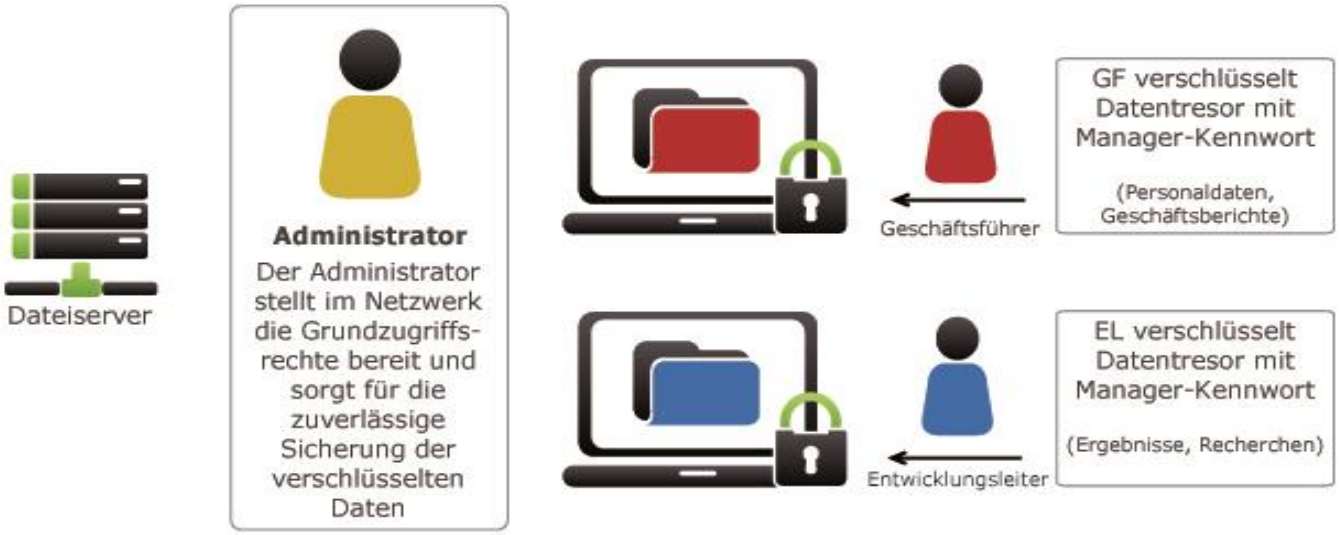
Datenblatt

Netzwerkverschlüsselung

HiCrypt™ 2.0



- ☑ *jahrelange Erfahrung auf dem Gebiet Datenverschlüsselung für Netzlaufwerke und 2-Faktor-Authentifizierung*
- ☑ *keine zusätzliche Infrastruktur nötig*
- ☑ *individuelle Schlüsselvergabe*
- ☑ *unterstützt moderne Authentifizierungsmethoden*
- ☑ *terminalserverfähig oder mit Floating License anwendbar*
- ☑ *Auszeichnungen:*

IPACSO AWARDS FINALIST OF THE 2015 EDITION · 2015 RUNNER UP SVC awards · 2014 RUNNER UP DCS awards · SVC awards 2013 WINNER

Herausforderung:

Der Zugang zu sensiblen und vertraulichen Daten sollen nur den berechtigten Personen ermöglicht werden. Der Schutz vor potentiellen „Eindringlingen" von außen aber auch unautorisiertem Zugriff von innen soll gewährleistet werden. Die Verschlüsselung soll dabei im Hintergrund bereitgestellt und eine Teamarbeit dennoch voll umfänglich durchführbar sein.

Lösung:

Mit HiCrypt™ 2.0 halten Sie den Schlüssel zur Sicherheit Ihrer Daten wieder selbst in der Hand. HiCrypt™2.0 bietet die Chance, als Eigentümer und Verantwortlicher ein oder mehrere vertrauliche Laufwerke gegenüber jeglichen nicht gewollten Einblicken abzusichern (administrative Serversicht, Backupsicht, Konkurrenz, etc.). Die bewusste Entscheidung Daten auf einem bestimmten Laufwerk abzulegen ist der einzige Mehraufwand während des Arbeitsprozesses, da die Verschlüsselung automatisiert erfolgt.

Produkt:

HiCrypt™ 2.0 bietet die „Schlüssel-Alleinbesitzgarantie" und ein Höchstmaß an Vertraulichkeit der Daten, verbunden mit komfortabler Nutzbarkeit, genialer Einfachheit und Flexibilität.

HiCrypt™ 2.0 läuft per Standardlizensierung oder auf Terminalserver (Desktop as a Service, Software as a Service), ist aber auch als Floating License erhältlich. Die IT-Administration stellt die Infrastruktur bereit. Sie übernimmt jedoch nicht die Schlüsselvergabe.

Leistungsumfang:

Zur Erhöhung der Sicherheit Ihrer Daten unterstützt HiCrypt™ 2.0 die 2-Faktor-Authentifizierung mittels Security Tokens. Dabei sind auch Szenarien umsetzbar, bei denen der Zugriff zu Ihren geschützten Daten exklusiv nur mit Token und passender PIN möglich sind. Dabei werden Standards wie MS CAPI, PKCS#11 und Verschlüsselungsalgorithmen nach AES, Blowfish und IDEA eingehalten.

Um, die in Unternehmensumgebungen häufig benötigten Sicherheitsrichtlinien in Bezug auf Kennworte auch in HiCrypt™ 2.0 automatisiert durchsetzen zu können, bietet es die Möglichkeit, individuelle Kennwortrichtlinien zu definieren. Die diversen Kriterien eines Kennworts wie Länge, Komplexität und die Gültigkeitsdauer ermöglichen eine flexible Umsetzung.

Unserer Lösung ist Bestandteil unseres All-In-One Compliance-Paket und liefert so das fehlende Puzzlestück zum Bestehen des Audits nach ISO 27001 hinsichtlich der verschlüsselten Ablage sensibler Daten auf Servern oder Storages Systemen.

Mobiler Zugriff mit HiCrypt™ 2.0 Viewer-App:

Sie möchten auch mit mobilen Endgeräten auf Ihre verschlüsselten Daten zugreifen? HiCrypt™ 2.0 bietet hierfür eine Erweiterung für mobile Endgeräte. Die Lösung ist auf Ihrem Smartphone oder Tablet installierbar. Damit können Sie immer und überall auf Ihre verschlüsselten Datenspeicher zugreifen.

TECHNISCHE DETAILS

HiCrypt™ 2.0:

Betriebssystem:	ab Windows XP
Standards:	CIFS/SMB
Verschlüsselungsalgorithmen:	AES, Blowfish, IDEA
Download:	www.hicrypt.com

USB Smartcard-Token

Betriebssystem:	Windows, Linux, Mac OS X
Standards:	MS CAPI, PKCS # 11
Smart Chip Zertifizierungen:	EAL 5+, EMV, ISO7816
Elektrische Zertifizierung:	FCC, CE, RWTÜV

HiCrypt™ 2.0 Viewer-App:

Betriebssystem:	Android, iOS
Standards:	FTP, WEBDAV
Verschlüsselungsalgorithmen:	AES, Blowfish, IDEA
Download:	Play Store, App Store

CITRIX® READY

Kurzportrait:

Die digitronic® computersysteme gmbh mit Sitz in Chemnitz realisiert seit 1991 IT-Lösungen auf den Gebieten Kommunikation, IT-Sicherheit und digitale Vertraulichkeit. Mit einem klaren Fokus auf Zuverlässigkeit, Kundenfreundlichkeit und Funktionalität erarbeitet ein dynamisches und hochmotiviertes Team innovative Lösungen.
Mit digitronic® All-In-One Compliancepaketen werden Auditanforderungen nach 2-Faktor-Authentifizierung und Teamverschlüsselung erfüllt.
Mobile, plattformunabhängige Vertraulichkeit zum Beweis nicht manipulierter Bildinformationen und sensible Steuerungsprozesse im Umfeld von Industrie 4.0 sind aktuelle Forschungs- und Entwicklungsschwerpunkte in enger Zusammenarbeit mit Großkunden. digitronic® ist Regionalstelle im Bundesverband IT-Sicherheit e.V. TeleTrusT und trägt das Zeichen –IT-Security made in Germany.

Kontakt:

digitronic® computersysteme gmbh
Oberfrohnaer Str. 62
09117 Chemnitz

Tel.:	+49 371 - 815390
Fax:	+49 371 - 81539900
E-Mail:	info@digitronic.net
Web:	www.digitronic.net

SecurITy made in Germany
TeleTrusT Quality Seal www.teletrust.de/itsmig

digitronic® .net

Anwenderbericht: Medizinischer Dienst Polizei Saarland

Gesundheitswesen – Erhöhte Sicherheit dank HiCrypt™

Der ärztliche Dienst der Polizei Saarland beschäftigt 9 Mitarbeiterinnen und Mitarbeiter als ärztliche Gutachter, Pflegefachkräfte und in der Verwaltung. Für die Sicherheit aller Personendaten gegenüber unbefugtem Zugriff Dritter nutzt das Landespolizeipräsidium in Saarbrücken jetzt die Verschlüsselungslösung HiCrypt™ von digitronic® aus Chemnitz.

Da persönliche und insbesondere medizinische Daten strengsten Datenschutz-bestimmungen unterliegen, bedarf es eines besonders hohen Sicherheitsstandards. Im Rahmen von Umstrukturierungen entstand die Herausforderung, alle medizinischen Daten der Polizeibediensteten elektronisch so abzulegen, dass die berechtigen Mitarbeiter des ärztlichen Dienstes diese auch selbst administrieren können, um dadurch den Postulaten zur Wahrung der ärztlichen Schweigepflicht zu genügen.

So musste es selbst für die Administratoren der Polizei unmöglich sein, dass sie zufällig oder bewusst auf Dateninhalte, die die Gesundheit ihrer Kollegen betreffen, stoßen.

Herr Krämer, Verantwortlicher für die technische Umsetzung des Vorhabens, bestimmte im ersten Schritt zwei Administratoren des medizinischen Dienstes zu „Schlüsselverwaltern" von HiCrypt™. Er selbst ist froh, dass er diese Verantwortung in Zukunft nicht noch zusätzlich tragen muss. Die beiden Administratoren, welche auch bisher den „Hut der Verantwortung" auf hatten, verwalten die Zweitschlüssel und sind jederzeit in der Lage, diese wieder einzuziehen oder auch neue Schlüssel zu vergeben. Damit ist die gesamte Verantwortung für den Schutz der medizinischen Daten aller Polizeibediensteten in der Hand der Verantwortlichen."

HiCrypt™ ist nun seit etwa einem Jahr im Einsatz. Laut Krämer hat die Installation nur wenige Minuten in Anspruch genommen und konnte ohne Probleme durchgeführt werden. Die Unterstützung des Herstellers war schnell und kompetent.

Seit einem Jahr arbeiten die Mitarbeiter des ärztlichen Dienstes mit diesem Programm. Irgendwelche „Reibungsverluste" können nicht berichtet werden. Das Programm startet beim Hochfahren des Computers, läuft im Hintergrund völlig unauffällig und störungsfrei. Es gelingt jederzeit auf verschlüsselt abgelegte Datensätze ohne Zeitverzögerung wieder zuzugreifen, ein und derselbe Datensatz kann beliebig oft geändert, verschlüsselt und erneut bearbeitet werden.

Herr Krämer und sein Team sind überzeugt: *„Es gibt keine absolute Sicherheit, aber wir haben alles was möglich ist dafür getan. Die Lösung sorgt dafür, dass die medizinischen Daten der Polizeibediensteten sicher verwaltet werden können und nur berechtigten Personen zugänglich sind."*

Kurzportrait digitronic®

Die digitronic gmbh mit Sitz in Chemnitz realisiert seit 1991 IT-Lösungen auf den Gebieten Sicherheit und gesicherte Kommunikation. Mit einem klaren Fokus auf Zuverlässigkeit und Funktionalität erarbeitet ein dynamisches und hochmotiviertes Team innovative Lösungen. Das breite Angebotsspektrum für die unterschiedlichsten Einsatzzwecke umfasst neben Authentifizierung und Zugriffsschutz auch formelle Kommunikation sowie Systeme zur schnellen und flexiblen Benachrichtigung.

Ansprechpartner:

digitronic computersysteme gmbh
Peter Liebing
Oberfrohnaer Str. 62
09117 Chemnitz
Tel.: 0371 – 81539 – 243
Fax: 0371 – 81539 – 900
E-Mail: pl@digitronic.net
Web: www.digitronic.net

BÜRO FÜR BRANDSCHUTZ

"Die Implementierung von HiCrypt™ half uns, äußerst sensible Daten vor unerlaubtem Zugriff zu schützen. Der Schutz vertraulicher Daten hat für uns höchste Priorität. Besonders überzeugend ist die einfache Installation sowie die professionelle Unterstützung durch digitronic-Mitarbeiter. HiCrypt™ ist sehr übersichtlich, flexibel sowie einfach zu handhaben. Wir sind sehr zufrieden und können das Produkt ruhigen Gewissens weiterempfehlen."

Chemieanlagenbau Chemnitz

"Als weltweit agierendes Unternehmen stellen wir hohe Ansprüche an jegliche Softwarelösung. HiCrypt™ hat uns in der Testphase überzeugt. Deshalb haben wir das Produkt zum Einsatz gebracht. Wir waren beeindruckt von der Flexibilität des Services bei der Umsetzung unseres Projektes. Mittlerweile sind wir uns durch die tägliche Benutzung sicher: Mit HiCrypt™ haben wir die richtige Entscheidung getroffen."

GOTTSCHOL ALCUILUX S.A.

"HiCrypt™ hat mich und meine Mitarbeiter begeistert. Sowohl in der Qualität, in der einfachen Handhabung, im Design als auch im Preis-Leistungs-Verhältnis. Für mich ein optimal zusammengestelltes Verschlüsselungsprodukt, das unser Hause überzeugt hat."

CONTURN – Analytical Intelligence Group GmbH

"Die kriminellen Methoden, um an sensible, unternehmenskritische Daten heranzukommen, werden täglich raffinierter. Das Spektrum der Delikte reicht dabei von Datendiebstahl, Betrug und Sabotage über Spionage und Korruption bis hin zur Internet-Kriminalität. Der Schutz sensibler Daten hat in unserem Unternehmen oberste Priorität und setzt daher hohe Ansprüche voraus. HiCrypt™ ist sehr übersichtlich, flexibel sowie intuitiv bedienbar. Die ausgezeichnete Servicehotline garantiert zu jeder Zeit eine kompetente Unterstützung. Wir sind sehr zufrieden mit den angebotenen Funktionen. Eine Zusammenarbeit mit digitronic können wir als langjähriger Kunde ruhigen Gewissens weiterempfehlen."

Wimmer Wohnkollektionen e. K.

"In unserer IT-Abteilung läuft alles störungsfrei. Wir suchten nach einer Lösung, die funktioniert, flexibel, übersichtlich und einfach zu handhaben ist. HiCrypt™ bietet die nötige Sicherheit, Verfügbarkeit, Kontrolle und Effizienz und ist damit die perfekte Antwort auf IT-Security. HiCrypt™ erfüllt all unsere Ansprüche."

SLM Kunststofftechnik GmbH

"Als weltweit agierender A-Lieferant für Volkswagen, Audi, Porsche, Daimler-Chrysler und BMW sowie als System-Lieferant für Rehau, Peguform, Plastal zählt unser Unternehmen zu den führenden Systemlieferanten. Vor einiger Zeit standen wir vor der Aufgabe, uns einem Audit eines Herstellers zu stellen. Die Anforderungen an die IT lagen insbesondere in den Bereichen 2-Faktor-Authentifizierung sowie Datenverschlüsselung. Um sicherzustellen, dass das Audit kurzfristig erfolgreich abgeschlossen werden konnte, suchten wir nach einem professionellen und flexiblen Lösungsanbieter, den wir mit digitronic® fanden. digitronic® konnte uns beide Lösungen anbieten und erste Erfahrungen im Automobilbereich vorweisen.
Mittels Secure Logon wurde die normale Windows-Anmeldung ersetzt durch Anmeldung mittels Token und PIN. Nur wenn der Token am Rechner steckt und die richtige PIN eingegeben wird, kann man arbeiten. Eine Anmeldung an dem Rechner ist also nur noch durch den Besitz des Tokens und dem Wissen der entsprechenden PIN möglich. Durch HiCrypt™ werden die Netzlaufwerke verschlüsselt. Durch seine geniale Architektur erlaubt die Software den Benutzern den gemeinsamen Zugriff auf verschlüsselte Dateien und Ordner. Die Ver- und Entschlüsselung findet am Arbeitsplatz-Computer statt. Unberechtigte Personen haben somit keine Möglichkeit, die verschlüsselten Informationen einzusehen.

Mit diesen beiden Lösungen und dem hervorragenden Reaktionsvermögen der Mitarbeiter von digitronic® konnten wir die Anforderungen des externen Audits vollends erfüllen."

Dietmar Helms GmbH – IT Consulting

"Bei meinem Kunden mit ca. 75 Mitarbeitern setzen wir HiCrypt™ auf einem Windows 2012 Terminalserver ein. Nach schneller Installation und einfacher Einrichtung tut das Verschlüsselungstool unauffällig seinen Dienst. Der schnelle, nette Support begeistert. Von mir eine klare Empfehlung für die Verschlüsselung sensibler Daten."

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.

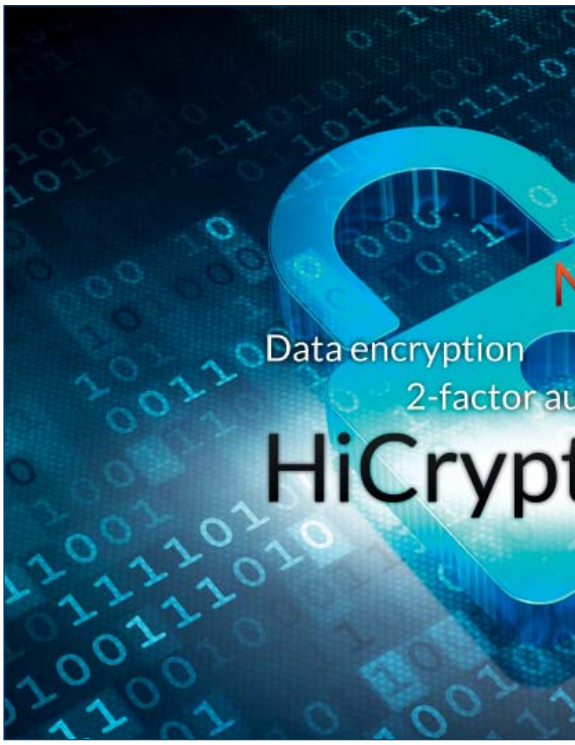
Nachweis angemessener Maßnahmen durch ISO 27001-Zertifikat

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.