

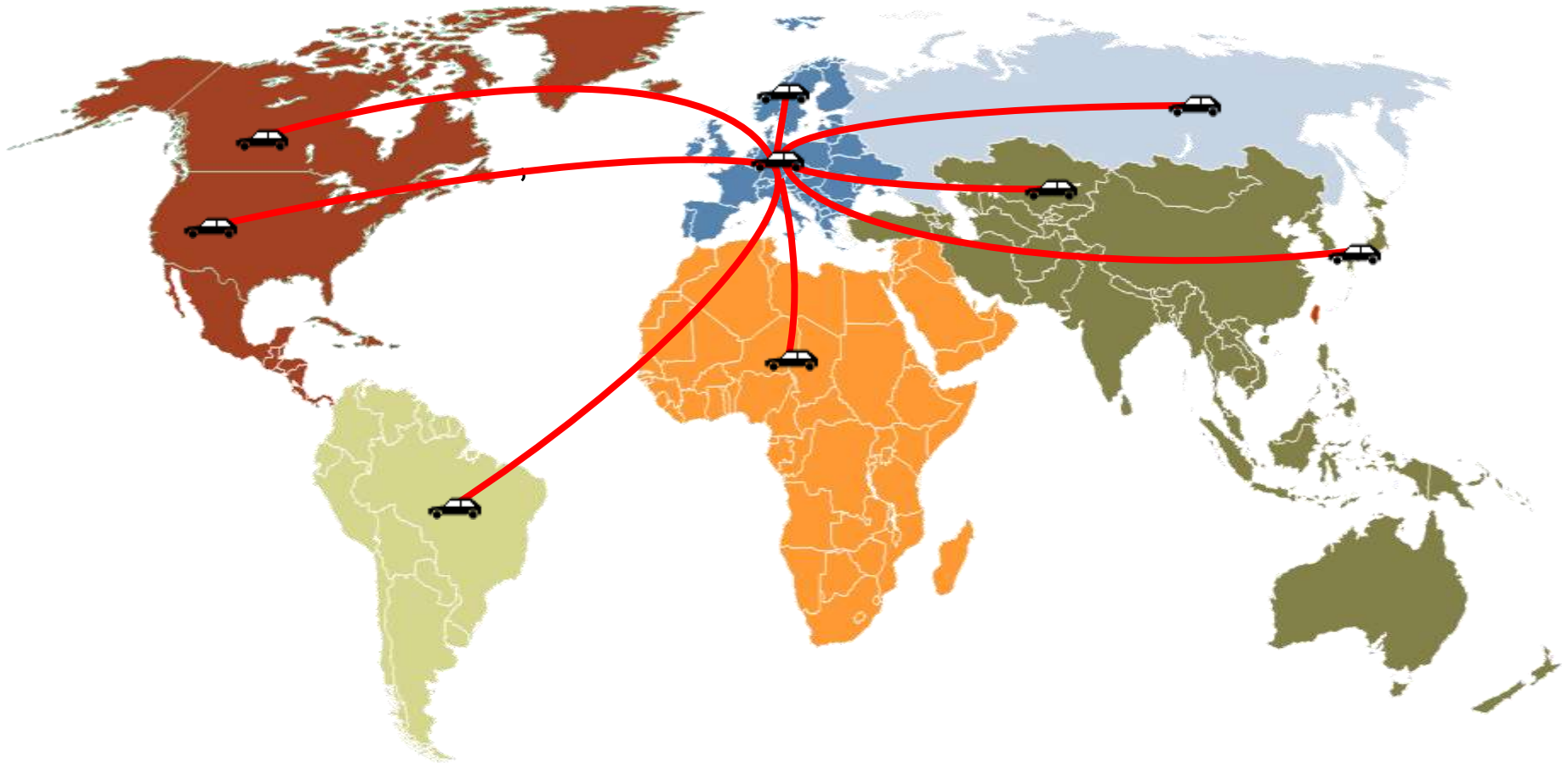
it-sa 2014 Auditorium Bundesverband IT-Sicherheit e.V.

Nürnberg, 08.10.2014

Produktsicherheit bei Zulieferern der Automobilindustrie

**Dipl.-Ing. Matthias Kirchhoff, Geschäftsführender Gesellschafter
digitronic® computersysteme gmbh**

Die Herausforderung

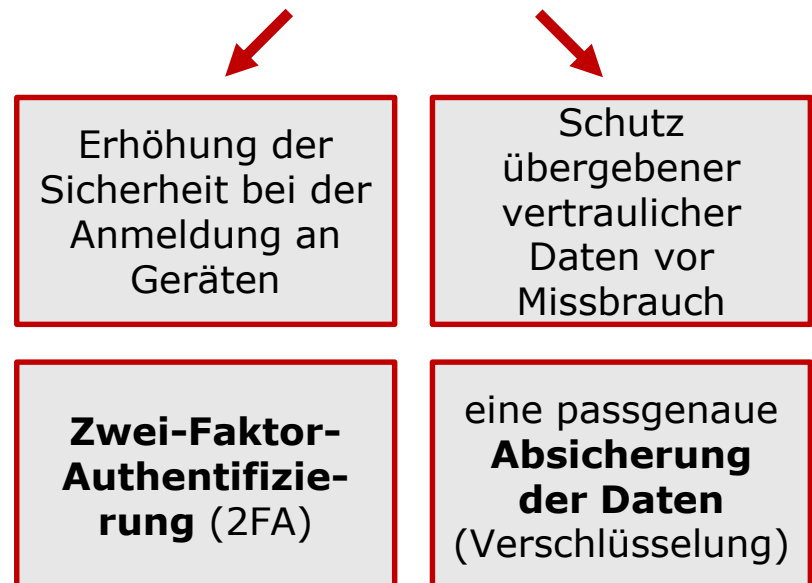


Zwei Forderungen im Bereich Automotive

Erhöhung der Produktsicherheit:

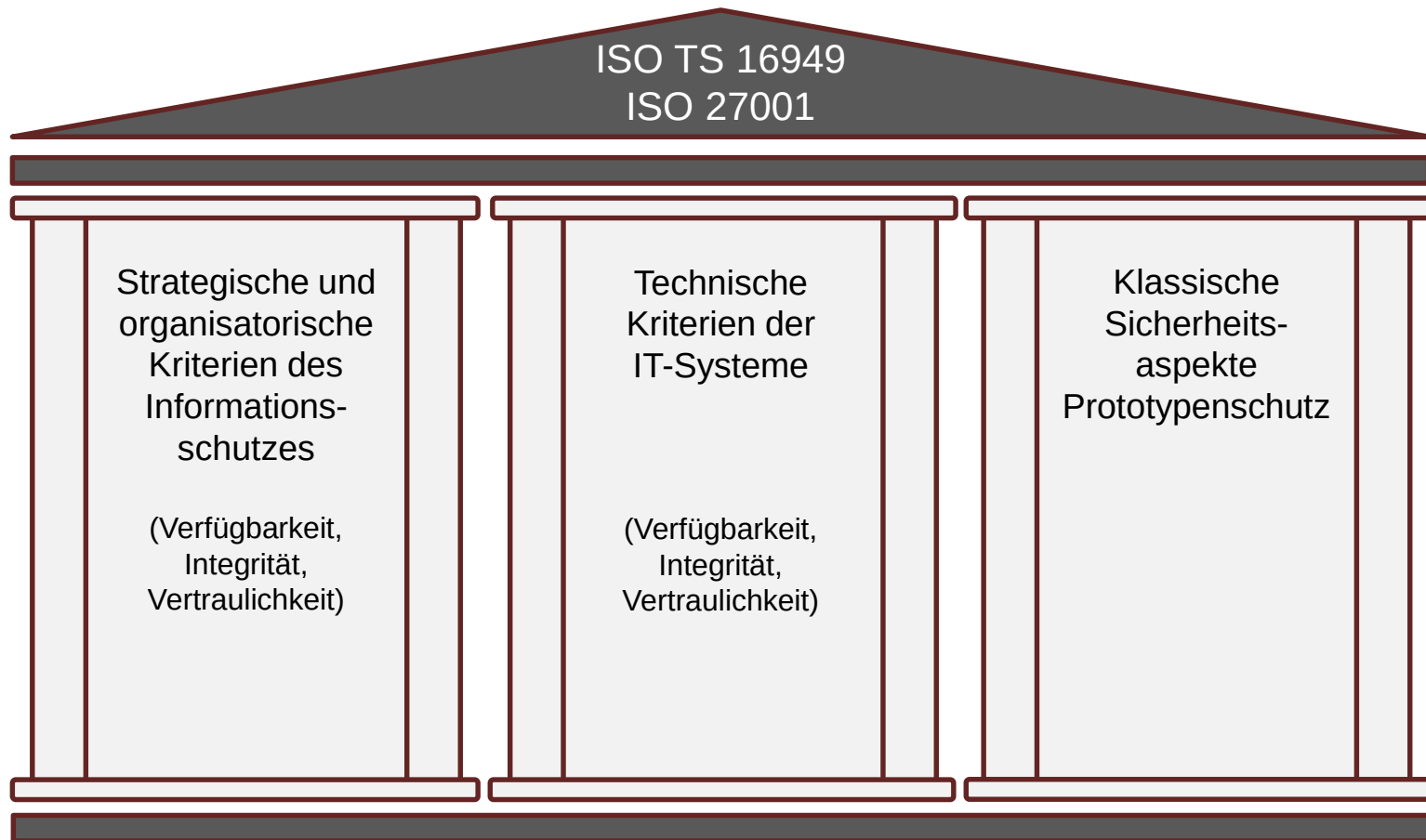


Automobilhersteller fordern die
Zertifizierung ihrer Zulieferer nach
Norm ISO 27001 und
Prozessaudit nach VDA 6.3.



z.B.: in der Prototypen-Entwicklung

Audits als Mittel zum Ziel



Konsequenz



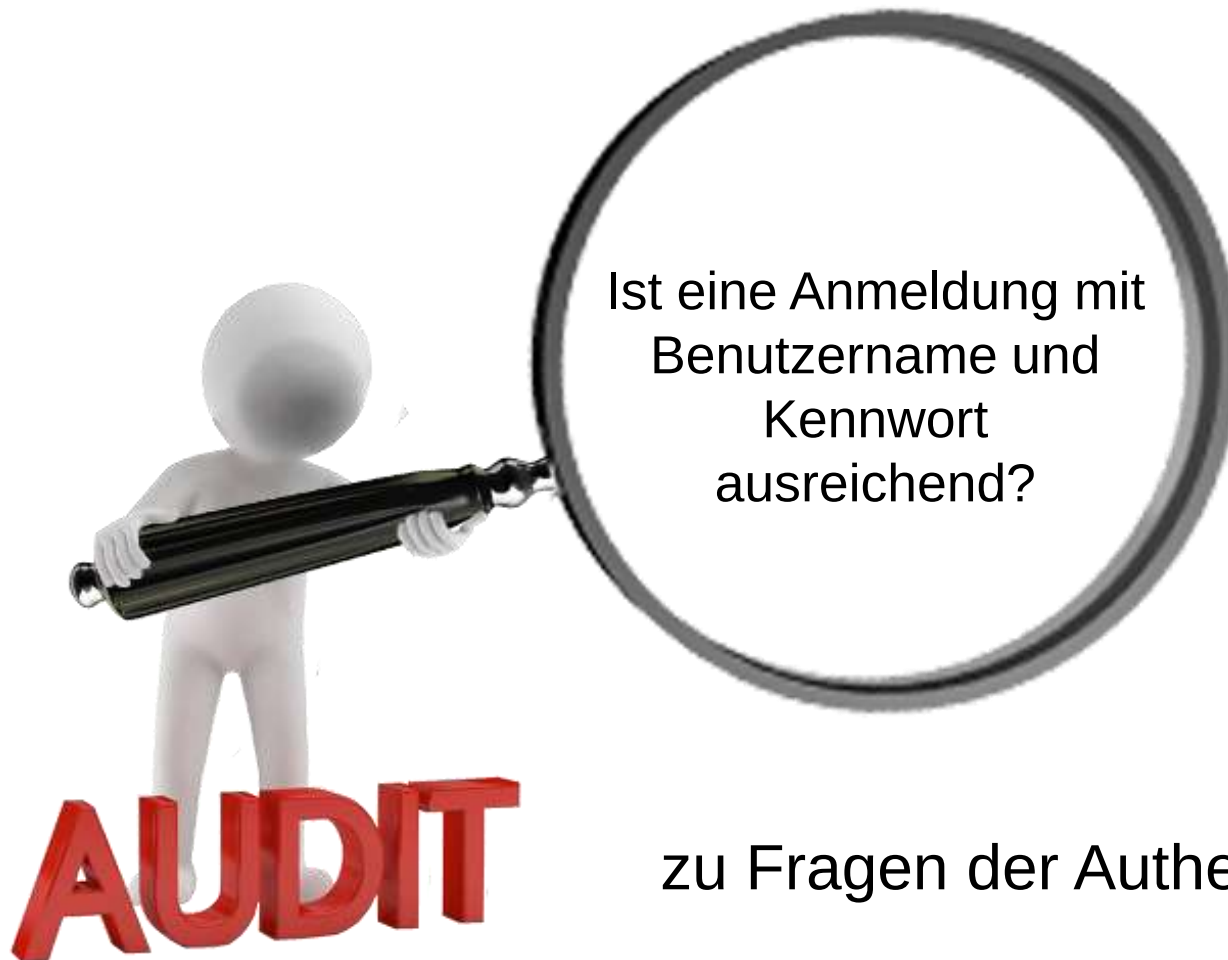
Tipps für Zulieferer vor dem Audit



Checkliste abarbeiten:

- Erfolgt die Anmeldung an Systemen mit 2 Faktoren (Besitz und Wissen)?
- Sind die schützenswerten Daten des Auftraggebers verschlüsselt abgelegt?
- Wer trägt die Verantwortung für Dateninhalte?
- Wer ist im Besitz eines Wiederherstellungsschlüssels?
- Wie wird eine ungehinderte, vertrauliche Teamarbeit ermöglicht?
- Wie vereinfacht man die Handhabung und Verwaltung der Schlüsselvergabe?
- Wie kombiniert und vereinfacht man 2-Faktor-Authentifizierung mit Schlüsseingabe für Verschlüsselung?

Fragen, denen man sich stellen muss



zu Fragen der Authentifizierung

Schlagzeilen – gute Gründe zum Handeln

NEWS

Neuer Fall von großflächigem Identitätsdiebstahl: BSI informiert Betroffene

BSI - 07.04.2014

Die digitalen Identitäten sind im Rahmen eines laufenden Ermittlungsverfahrens gefunden worden. Mit den E-Mail-Adressen und den zugehörigen Passwörtern versuchen Kriminelle mithilfe eines Botnetzes, sich in E-Mail-Accounts einzuloggen und diese für den Versand von SPAM-Mails zu missbrauchen. Das Botnetz ist noch in Betrieb, die gestohlenen Identitäten werden aktiv ausgenutzt. Es ist davon auszugehen, dass es sich bei den gefundenen Adressen und Passwörtern sowohl um Zugangsdaten zu E-Mail-Konten, als auch um Zugangsdaten zu anderen Online-Accounts wie Online-Shops, Internet-Foren oder Sozialen Netzwerken handelt.

BSI –Milliardenfacher Datenklau dürfte auch Deutschland treffen

Thomson Reuters - 06.08.2014

Berlin (Reuters) - Von dem mutmaßlichen milliardenfachen Datendiebstahl durch russische Hacker dürfte nach Einschätzung des Bundesamts für Sicherheit in der Informationstechnik (BSI) auch Deutschland betroffen sein.

Google: Millionen Login-Daten von Mail-Nutzern gestohlen

Handelsblatt - 11.09.2014

Berlin - Unbekannte haben massenhaft Einwahldaten von Google-Profilen im Internet veröffentlicht. Die Kombinationen aus E-Mail-Adresse und Passwort tauchten laut Medienberichten in russischen Internet-Foren auf. Dort seien fast fünf Millionen Datensätze veröffentlicht worden, hieß es.

2-Faktor-Authentifizierung

- Probleme:**
- Benutzername & Kennwort reichen nicht aus
 - Zugriff auf einen Arbeitsplatz-PC oder Laptop durch unberechtigte Personen

Lösung: **Software zur 2-F-Authentifizierung**

- Nutzen:**
- Schutz vor unbefugter Nutzung
 - Kennwort Weitergabe unmöglich



z.B.: Secure Logon

Tipps für Zulieferer vor dem Audit



Checkliste abarbeiten:

- Erfolgt die Anmeldung an Systemen mit 2 Faktoren (Besitz und Wissen)? ✓
- Sind die schützenswerten Daten des Auftraggebers verschlüsselt abgelegt?
- Wer trägt die Verantwortung für Dateninhalte?
- Wer ist im Besitz eines Wiederherstellungsschlüssels?
- Wie wird eine ungehinderte, vertrauliche Teamarbeit ermöglicht?
- Wie kombiniert und vereinfacht man 2-Faktor-Authentifizierung mit Schlüsseleingabe für Verschlüsselung?
- Wie vereinfacht man die Handhabung und Verwaltung der Schlüsselvergabe?

Fragen, denen man sich stellen muss



Verschlüsselung

- Probleme:**
- Daten liegen offen auf Dateiservern und Storages
 - Bei Überwindung der Betriebssystemrechte ist Datenklau möglich
 - „Ungeladene Gäste“ stehen vor Klartextdaten

Lösung: **Komfortable Teamverschlüsselung für Storages z.B.: LW V:**

- Nutzen:**
- Schlüssel-Alleinbesitzgarantie für Verantwortliche (auch Wiederherstellungsschlüssel)
 - Schutz der Administratoren bzw. Provider vor dem Verdacht des Datenmissbrauchs
 - Simple, vorbeugend wirksame Maßnahme gegen unbefugten Datenmissbrauch
 - Automatischer Backupschutz



Datenverschlüsselung

- Funktionsweise der Verschlüsselungslösung



Computer

Daten verlassen den Computer

Der Nutzer vergibt z.B. für Laufwerk T:
selbst einen Schlüssel!

Danach werden Daten, die über Laufwerk T:
gelesen oder geschrieben vollautomatisch
ver- bzw. entschlüsselt

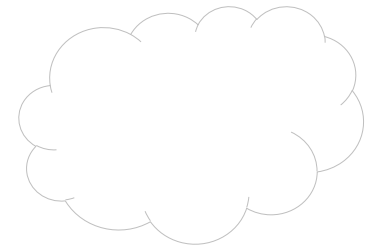
Dabei ist egal, ob Laufwerk T: mit einer lokalen
Festplatte, einem Netzwerk Server oder einem
ONLINE-Speicher verbunden ist!



Ablage „Lokal“



Ablage „Server“



Ablage „Cloud“

Datenverschlüsselung



z.B.: HiCrypt™

Tipps für Zulieferer vor dem Audit

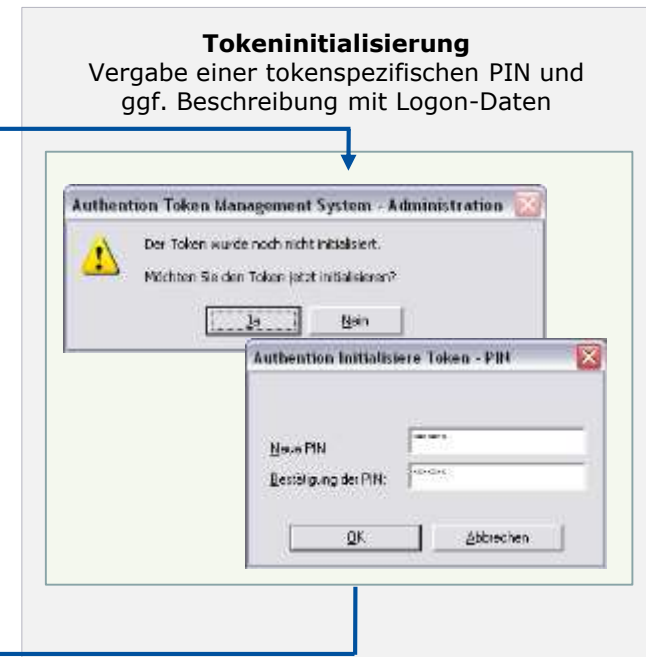


Checkliste abarbeiten:

- Erfolgt die Anmeldung an Systemen mit 2 Faktoren (Besitz und Wissen)? ✓
- Sind die schützenswerten Daten des Auftraggebers verschlüsselt abgelegt? ✓
- Wer trägt die Verantwortung für Dateninhalte? ✓
- Wer ist im Besitz eines Wiederherstellungsschlüssels? ✓
- Wie wird eine ungehinderte, vertrauliche Teamarbeit ermöglicht? ✓
- Wie vereinfacht man die Handhabung und Verwaltung der Schlüsselvergabe?
- Wie kombiniert und vereinfacht man 2-Faktor - Authentifizierung mit Schlüsseingabe für Verschlüsselung?

Token Management System

- Erstellung eines Token (bspw. Mitarbeiterausweis)



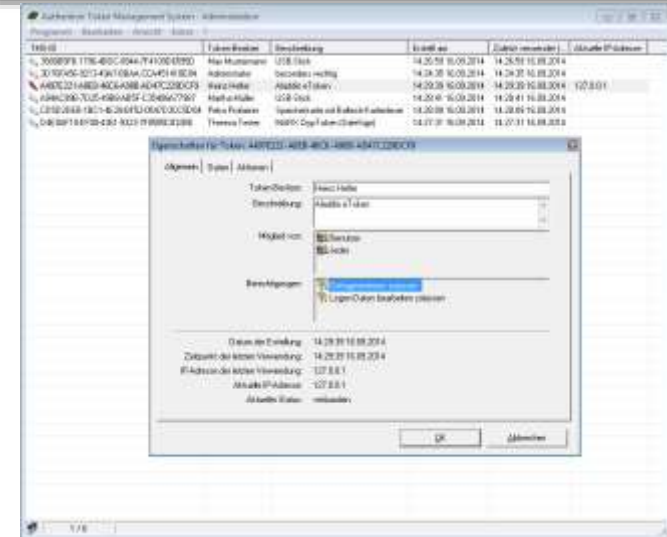
Token Management System

- Probleme:**
- Verwaltung mehrerer Token
 - Wiederherstellen verlorener oder defekter Token

Lösung: Token Management Software

- Nutzen:**
- Zentrale Möglichkeit bei der Wiederherstellung von Daten, Erhöhung der Profitabilität
 - Automatisiertes Sperren
 - Backup von Inhalten

Das Token Management System ist ein leistungsstarkes Verwaltungssystem für die Implementierung, Zuweisung, Verwaltung und Personalisierung von Token und Smartcards in einem Unternehmen.



z.B.: TMS

Tipps für Zulieferer vor dem Audit



Checkliste abarbeiten:

- Erfolgt die Anmeldung an Systemen mit 2 Faktoren (Besitz und Wissen)? ✓
- Sind die schützenswerten Daten des Auftraggebers verschlüsselt abgelegt? ✓
- Wer trägt die Verantwortung für Dateninhalte? ✓
- Wer ist im Besitz eines Wiederherstellungsschlüssels? ✓
- Wie wird eine ungehinderte, vertrauliche Teamarbeit ermöglicht? ✓
- Wie vereinfacht man die Handhabung und Verwaltung der Schlüsselvergabe? ✓
- Wie kombiniert und vereinfacht man 2-Faktor-Authentifizierung mit Schlüsseleingabe für Verschlüsselung? ✓

Kombination Zugang(2FA) und Vertraulichkeit von Daten!



Tipps für Zulieferer vor dem Audit



Checkliste abarbeiten:

- Erfolgt die Anmeldung an Systemen mit 2 Faktoren (Besitz und Wissen)? ✓
- Sind die schützenswerten Daten des Auftraggebers verschlüsselt abgelegt? ✓
- Wer trägt die Verantwortung für Dateninhalte? ✓
- Wer ist im Besitz eines Wiederherstellungsschlüssels? ✓
- Wie wird eine ungehinderte, vertrauliche Teamarbeit ermöglicht? ✓
- Wie vereinfacht man die Handhabung und Verwaltung der Schlüsselvergabe? ✓
- Wie kombiniert und vereinfacht man 2-Faktor-Authentifizierung mit Schlüsseingabe für Verschlüsselung? ✓



Gut gerüstet zum Audit! - „Secure Logon & HiCrypt™-Automotive Paket“

Ihre Zielstellung ist unser Ansporn!

Besuchen Sie uns am Stand unseres Distributors

Jakobsoftware

Halle 12 / Stand 12-209

www.hicrypt.com

www.digitronic.net