DataGuard

SO KLAPPT'S MIT DEM TISAX®-ASSESSMENT

20. Mai 2021

Christian Taube

TISAX ist eine eingetragene Marke der ENX Association

CHRISTIAN TAUBE

Team Lead Information Security

Zertifizierter ISMS Security Officer
und Auditor nach ISO 27001

ICO-CERT
International Certification Organization

ERFAHRUNG

Geschäftsführer, LanguageWire München GmbH

Chief Solutions Officer, Xplanation NV (Leuven)

Mitgründer, Technischer Leiter und Aufsichtsrat,
Matrix Communications AG (München)

Einführung von DS-GVO + ISO 27001 Compliance und erfolgreiche Audits nach TISAX® und ISO 27001 in internationalen Unternehmen

AUSBILDUNG

Studium in Stuttgart,
Eugene (Oregon) und München

AGENDA

- Warum Informationssicherheit?
- Wie funktioniert TISAX®?
- TISAX® und ISO 27001
- Was passiert beim Audit?
- Takeaways aus der Praxis
- Zeit für Ihre Fragen!

TISAX® ist eine eingetragene Marke der ENX Association

WARUM INFORMATIONSSICHERHEIT?

Feuer im Rechenzentrum

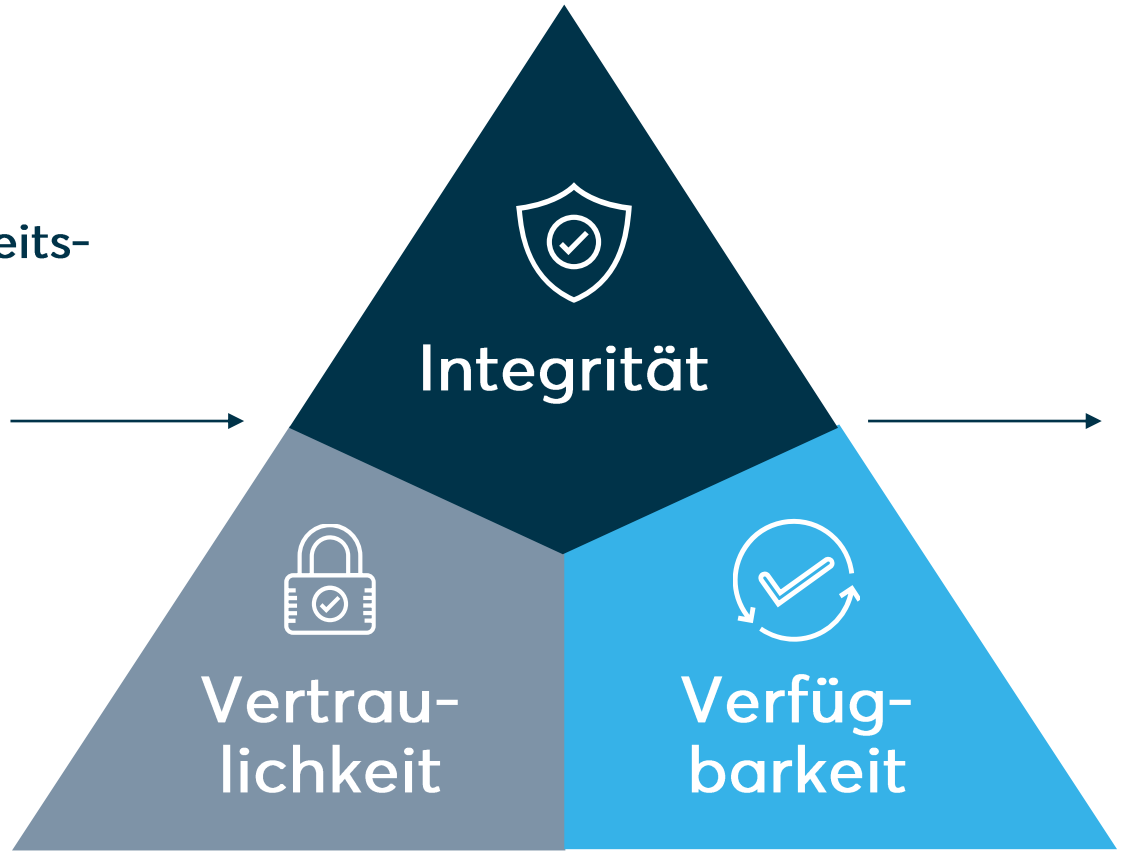
3,4 Millionen Webseiten von Brand beim größten französischen Cloudbetreiber betroffen

„Nach Angaben des französischen Webzeitung „Le Journal du net" gab es in dem zerstörten Datenzentrum nur Alarmsysteme, doch keine Sprinkleranlagen oder ähnliche automatische Mittel zur Feuerbekämpfung."

*Quelle: FAZ online

Was versteht man unter Informationswerten?

Das Informationssicherheits-Managementsystem schützt die



Ihrer Informationswerte vor Risiken und Schwachstellen

WIE FUNKTIONIERT TISAX®?

Warum TISAX®?

- Ihr Kunde („Business Partner“) besitzt vertrauliche Informationen.
  Er will sie mit dem Zulieferer – Ihnen - teilen.
- Informationen, die Ihr Kunde mit Ihnen teilt, sind wichtiger Teil
  der Wertschöpfung → angemessener Schutz ist notwendig!
- Er möchte sicher sein, dass Sie Informationen
  mit der gleichen Sorgfalt behandeln. → Er braucht Nachweise.

- *Was bedeutet* „sicherer Umgang“ / „Sorgfalt“?
- Dafür gibt es einen Standard!
- Für den VDA = Verband der Automobilindustrie:
  Das „VDA ISA“ = *Information Security Self Assessment*
- *Wie* können Sie den sicheren Umgang nachweisen, z.B. anderen OEMs?
- Über TISAX® = *Trusted InformationSecurity Assessment Exchange*

Wie läuft ein TISAX®-Assessment ab?

Ein OEM fordert Sie auf, Ihr Informationssicherheits-Management nach TISAX® nachzuweisen.

Formale Schritte:

1. Registrierung* > Sammeln von Informationen, Festlegen des Prüfumfangs (Scope) auf Basis der Anforderungen Ihres Partners.

   **Die Registrierung ist kostenpflichtig*

2. Prüfung durch einen Prüfdienstleister
3. Teilen Ihres Prüfergebnisses

Tatsächliche Schritte:

- Einführung des ISMS > hier steckt der meiste Aufwand (mind. 4 Monate, 6 bis 9 wären normal)
- Registrierung bei ENX und Scope-Festlegung
- Interner Audit Ihres ISMS > Maßnahmenumsetzung aus internem Audit
- Prüfung durch Prüfdienstleister > Maßnahmenplan
- Abhängig von den Abweichungen und erfolgten Korrekturen ggf. weitere Prüfschritte erforderlich (max. Prüfungsdauer 9 Monate)
- Nach drei Jahren erneuter Audit

TISAX® – Prüfziele, Anforderungen…

Die Prüfziele…

verbinden einen der drei Kriterienkataloge Informationssicherheit, Prototypenschutz und Datenschutz mit einem Schutzbedarf:

1. Informationen mit hohem Schutzbedarf
2. … mit sehr hohem Schutzbedarf
3. Prototypenschutz: Bauteile
4. Prototypenschutz: Fahrzeuge
5. Prototypenschutz: Erprobungsfahrzeuge
6. Prototypenschutz: Veranstaltungen / Shootings
7. Datenschutz
8. Datenschutz bei sog. „besonderen Kategorien" personenbezogener Daten

Die Anforderungen…

Modul	„Muss"	„Sollte"	Zusatz „Hoch"	Zusatz „Sehr hoch"
Informations-sicherheit	98	91	25	6
Prototypen-schutz	58	6	3	0
Datenschutz	23	0	0	0
Gesamt	179	97	28	6

➔ Ihr **Kunde** gibt Ihnen in der Regel vor, welche Kriterienkataloge und welchen Schutzbedarf Sie erfüllen müssen.

➔ Denken Sie daran, auch Ihre Lieferanten im Blick zu haben.

… und TISAX® Assessment Level

Prüfziele werden anhand eines Assessment Levels geprüft:

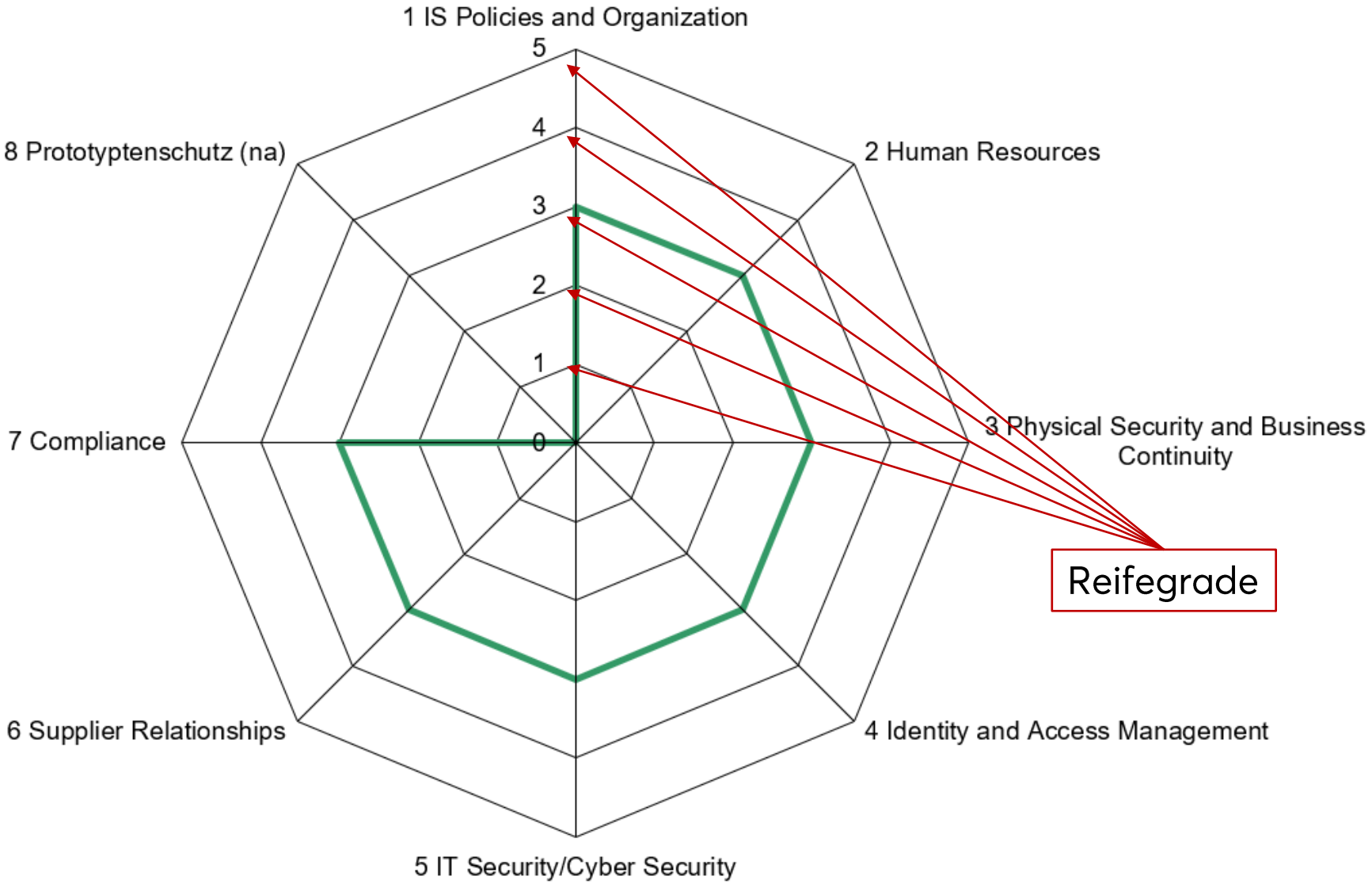
AL 1 – Reine Selbsteinschätzung

AL 2 – Plausibilitäts- und Nachweisprüfung, in der Regel remote

AL 3 – Eingehende Vor-Ort-Prüfung

Erfüllung dieses Prüfziels…	…möglich mit diesem AL
Informationen mit hohem Schutzbedarf	AL 2
Informationen mit sehr hohem Schutzbedarf	AL 3
Prototypenschutz - Bauteile	AL 3
Prototypenschutz – Fahrzeuge	AL 3
Prototypenschutz – Erprobungsfahrzeuge	AL 3
Prototypenschutz – Veranstaltungen	AL 3
Datenschutz	AL 2
Datenschutz bei besonderen Kategorien	AL 3

TISAX® – Maßnahmenziele und Reifegrade



Umfassendes Management-system – nicht nur IT-Sicherheit!

TISAX® UND ISO 27001

TISAX® und ISO 27001

ISO 27001

Enthält allgemeine Anforderungen – normativer MUSS-Katalog an Maßnahmen.
Branchenübergreifend.

Prüfung: Erfüllung (ja/nein) der Controls?
Prüfung: Befragen ggf. mehrerer Mitarbeiter.
Maßnahmenumsetzung 3 Monate nach Prüfung.
Nächster Audit nach 12 Monaten.
Frei definierbarer Scope.
Zertifikat.
Sie können frei damit werben.

TISAX®

Ableitung der ISO 27001 für Automobil-Industrie, mit konkreten Reifegraden.
Kleinerer Maßnahmenumfang, mehr Anforderungsbereiche.

Prüfung: Reifegrad der Umsetzung?
Prüfung: Befragen der Hauptverantwortlichen.
Maßnahmenumsetzung max. 9 Monate.
Nächster Audit nach 3 Jahren.
Vorgegebener Scope.
Kein Zertifikat (!!).
Sie können nur eingeschränkt damit werben.

Sie können den selben Satz an Dokumenten und Nachweisen für beide verwenden.

WAS PASSIERT BEI EINEM AUDIT?

Audit-Ergebnisse

Konformität	Wirksamkeit des ISMS ist erwiesen.
Beobachtung	Wirksamkeit des ISMS ist erwiesen. Detailaspekt könnte verändert > verbessert werden.
Nebenabweichung	Wirksamkeit des ISMS ist insgesamt erwiesen. Jedoch fehlen einzelne Nachweise für die Umsetzung der beschriebenen Maßnahme in einem gegebenen Kontrollbereich / ist eine Maßnahme nur teilweise wirksam umgesetzt. => Temporäres TISAX®-Label bis „Heilung“ (max. Dauer 9 Monate)
Hauptabweichung	Wirksamkeit des ISMS ist *nicht* erwiesen. Es fehlen wirksame Richtlinien in einem gegebenen Kontrollbereich / Maßnahmen sind in einem kompletten Kontrollbereich nicht vorhanden oder nachweisbar. => Maximale Dauer des Prüfprozesses 9 Monate => dann kein TISAX®-Label

Was darf / wird ein Prüfer tun und was nicht?

DARF / WIRD:

- Den gesamten Standort des Unternehmens sehen / begehen.
- Auf Einhaltung des Zeitplans bestehen.
- Seine Fragen erklären.
- So lange fragen, bis die Antwort für seine Bewertung hinreicht.
- Im Rahmen der Vertraulichkeit jedes Dokument sehen, das Prüfinhalte betrifft.
- Auf Mängel hinweisen.

DARF NICHT / WIRD NICHT:

- Den Zeitplan nicht einhalten.
- Sie beraten.
- Annahmen treffen.
- Trickfragen / verdeckte Fragen stellen.
- Selbst Hand anlegen.

Was sollte ich im Audit tun und lassen?

OK:

- Die eigenen Dokumente kennen.
- Die Fragen vollständig beantworten.
- Wenn die Antwort „Ich weiß es nicht" ist – dann ist das die Antwort.
- Nichts verheimlichen.
- Bei Zweifeln nachfragen.
- Dem Auditor Zeit geben.
- Schweigen aushalten.

NICHT EMPFEHLENSWERT:

- Fragen beantworten, die nicht gestellt wurden.
- Nachfragen persönlich nehmen.
- Interne Audits nicht durchführen.
- Ihr Team nicht involvieren.
- Den Auditor überraschen.
- Bewusst täuschen.

TAKEAWAYS AUS DER PRAXIS

Einige Irrtümer

- „Informationssicherheit bekämpft Hacker und Malware – mehr ist nicht notwendig."
- „Die Einführung eines ISMS ist ein IT-Projekt."
- „Das ISMS richten wir nebenbei ein."
- „Wir haben keine Zeit, das ISMS vergeben wir an einen Dienstleister."
- „Das TISAX®-Assessment ist nur eine Lückenanalyse."
- „Die Informationswerte erfassen wir in der Anlagenbuchhaltung."
- „Organisationsfremde IT-Dienste setzen wir nicht ein."
- „Wir haben ein Onboarding neuer Mitarbeiter – wir wissen, wer wo Zugriff hat."

Top 5 Takeaways zum erfolgreichen TISAX®-Assessment

Sicherheit ist ein Prozess – keine Eigenschaft

Mandat und Zeit der Mitarbeiter

„Dies ist jetzt leichter, weil …"

Keine falschen Annahmen treffen

Management mitnehmen

Ressourcen einplanen

Mitarbeiter mitnehmen

Positive Erlebnisse schaffen

Buy-In der Geschäftsführung sichern

Nicht nur die Aufgabe des Informationssicherheits-Beauftragten

FRAGEN?

Vielen Dank für Ihr Interesse!
Sie haben weitere Fragen?
So erreichen Sie mich.

E-Mail:

ctaube@dataguard.de

LinkedIn

https://www.linkedin.com/in/christiantaube/