secuvera

BSI-zertifizierter IT-Sicherheitsdienstleister und Prüfstelle

Vortrag:

Erfolgreiche Umsetzung der ISO 27001 in KMU

verinice.XP 2019

Berlin, 26. - 28. Februar 2019

secuvera

Inhalt

- Über uns
- Motivation
- Rahmenbedingungen
- Umsetzung
- Resümee
- Diskussion

secuvera

Inhalt

- Über uns
- Motivation
- Rahmenbedingungen
- Umsetzung
- Resümee
- Diskussion

secuvera

Über uns

- gegründet 1. Juli 1982
- Gäufelden bei Stuttgart
- IT-Sicherheit seit 1988
- heute reiner IT-Sicherheitsdienstleister
- aktuell ca. 24 Mitarbeitende
- inhabergeführt
- herstellerunabhängig

secuvera

- BSI-zert. IT-Sicherheitsdienstleister
- Geschäftsbereiche
  - Sicherheitsberatung (BSI-Grundschutz / ISO 27001)
  - Penetrationstests / Webanwendungsprüfungen
  - BSI-Prüfstelle für Common Criteria
- akkreditiertes Prüflabor für IEC 62443 beim TÜV Nord

secuvera

Über mich

- Björn Lemberg
- seit 2012 bei der secuvera
- leitender Sicherheitsberater ISMS verantwortlich für
  - ISO 2700x
  - VDA-ISA & ENX/TISAX
  - Datenschutz
- CISSP, 27001 Auditor, DSB

secuvera

Inhalt

- Über uns
- Motivation
- Rahmenbedingungen
- Umsetzung
- Resümee
- Diskussion

secuvera

Ausgangslage ISO 27001

- führender ISMS-Standard
  - ~ 1.350 Zertifikate in Deutschland
  - ~ 39.500 Zertifikate weltweit *
- international anerkannt
- branchen- und anwendungsspezifisch erweiterbar

➢ schwer umsetzbar?

➢ für große Organisationen?

* Quelle: ISO-Survey 2017 (https://www.iso.org/the-iso-survey.html)

secuvera

In der Praxis

- KMU betreiben ISMS nach ISO 27001
  - nachhaltig
  - lebendig
  - effizient
  - gezielt
  - nutzen Chancen
  - verbessern sich fortlaufend

➢ gerade kleine Unternehmen fallen in der Praxis positiv auf

secuvera

Inhalt

- Über uns
- Motivation
- Rahmenbedingungen
- Umsetzung
- Resümee
- Diskussion

secuvera

ISMS nach ISO 27001

- Zertifizierung ab 1 Person möglich
- Prozesse zur Wahrung der Schutzziele
  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit
- risikobasierter Ansatz
- nach individuellen Bedürfnissen
- kontinuierliche Verbesserung

secuvera

Maßnahmen

- Referenzmaßnahmen in Anhang A
  - normative „3-Zeiler“
    - 114 Maßnahmen
      - zur Erreichung von 35 Maßnahmenzielen
        - in 14 Abschnitten
  - Mindest-Maßnahmen - bei Bedarf zu erweitern
- Umsetzungsempfehlungen in 27002
- VDA-ISA / TISAX konkreter

secuvera

Rückschluss

- ISMS ist flexibel nach Kontext der Organisation zu gestalten
- Sicherheitsniveau / Ziele individuell
- Anforderungen an Sicherheits-maßnahmen allgemein gehalten
- Dokumentationen angemessen für Organisation

➢ ISMS muss sich der Organisation anpassen und nicht umgekehrt

secuvera

Inhalt

- Über uns
- Motivation
- Rahmenbedingungen
- Umsetzung
- Resümee
- Diskussion

secuvera

Anwendungs-bereich

- Anwendungsbereich beschreiben
  - Dienstleistungen, Geschäftsprozesse und Unterstützungsprozesse
    - diesbezügliche Herausforderungen
  - Interessierte Parteien und ihre Anforderungen an die IS (intern/extern)
  - Abhängigkeiten und Schnittstellen nach Außen

➢ individuelle Anforderungen bestimmen

➢ Zweck des ISMS festlegen

secuvera

Politik

- Leitlinie zur IS (Politik)
  - Informationssicherheitsziele
    auf Grundlage des Anwendungsbereiches
    festlegen
  - Stellenwert der IS beschreiben

➢ ISMS betreiben, um individuelle IS-Ziele zu erreichen

secuvera

Rollen

- IS-Team bilden
  - Leitung
  - ISM (ISB, CISO, SiBe…)
  - Interessen- und Kompetenzträger einbinden, z.B. Abteilungsleiter, IT
  - bDSB,
  - …
- externe Unterstützung
  - Training-on-the-Job nachhaltiger als externe Besetzung

secuvera

Risiko-management

- Identifikation
- Analyse und Bewertung
- Behandlung
- Restrisiken

➢ Risiken verstehen und handhaben
➢ Paretoprinzip (80-20-Regel) beachten
➢ Synergien zur DSFA nutzbar

secuvera

Risiko-identifikation

- Fokus während Erst-Umsetzung:
  - Grundabdeckung
    z.B. analog zu Anhang A
  - spezifische Risiken
    für **konkrete** kritische Geschäftsprozesse
- Später kontinuierliche Verbesserung, z.B. entlang
  - IT-Struktur
  - kritischer Systeme
  - praktischer Fragestellungen

secuvera

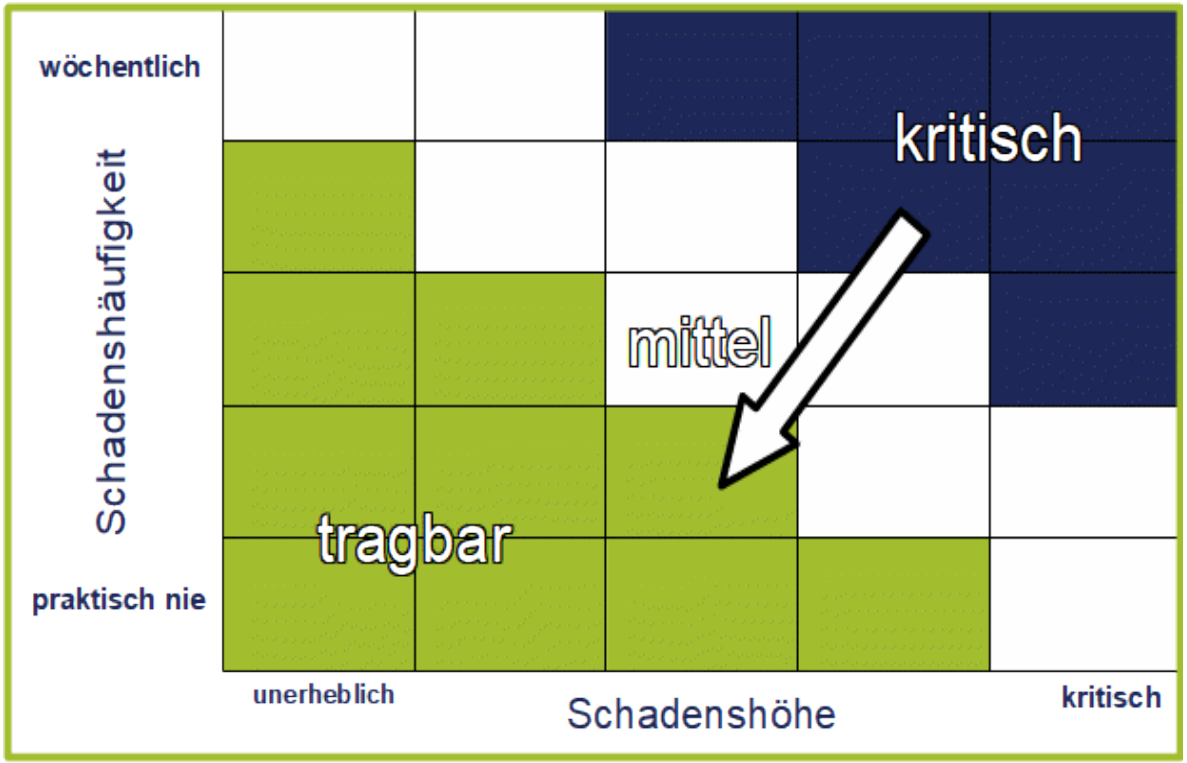
Analyse & Bewertung

- Risiko ergibt sich aus
  - Schadenshöhe
  - Eintrittswahrscheinlichkeit
- untragbare Risiken müssen behandelt werden
  - i.d.R. durch Maßnahmen (⇨Anhang A)

➢ Abschätzung in 10er-Potenzen!

secuvera

Risikomatrix



secuvera

Behandlung

- Reduzieren von
  - Schadenshöhe und/oder
  - Eintrittswahrscheinlichkeit
- Referenzmaßnahmen aus Anhang A
- Behandlungsplan erstellen
  - priorisiert Behandlung kritischer Risiken

➢ Behandlung realistisch planen

➢ Prio: Quick-wins & kritische Bereiche

secuvera

Richtlinien & Vorgaben

- Richtlinien für notwendige Vorgaben
  - Vorgaben nach Anhang A, z.B.
    - Rechteverwaltung
    - Datensicherung
    - Entsorgung
  - ggf. zielgruppenspezifische Vorgaben

➢ Qualitätskriterium: Anwendbarkeit
- ➢ angemessen statt umfangreich
- ➢ umsetzbar statt ideal

secuvera

Bewertung Restrisiken

- Neubewertung der Risiken unter Berücksichtigung der Behandlung
  - belegt angemessenes IS-Niveau
  - dokumentiert Restrisiken
  - zeigt Potentiale auf

➢ Ziele aus Leitlinie erfüllt?

secuvera

RM-Tool

- zu Anfang
  - meist nicht notwendig
  - erst RM-Prozess gestalten
- Möglichkeit zur Verbesserung des RM, wenn Ansprüche bekannt

➢ Tool soll RM-Prozess abbilden, nicht umgekehrt

secuvera

Ziele bis Erst-zertifizierung

- MS im Regelbetrieb
- Behandlung aller hohen Risiken
- Nachweisbare Berücksichtigung der Referenzmaßnahmen aus Anhang A
- Abdeckung Richtlinien
- Realistische Planung
- Identifikation Verbesserungspotentiale

secuvera

Vorteile KMU

- begrenzte Komplexität im Anwendungsbereich
- Hohes Verständnis für Geschäftsprozesse & Anforderungen
- Fokussierung auf konkrete Ziele
- Identifikation mit Unternehmenszielen
- Mitgestaltung & Einbindung
- sichtbarer Nutzen

secuvera

Inhalt

- Über uns
- Motivation
- Rahmenbedingungen
- Umsetzung
- Resümee
- Diskussion

secuvera

Resümee

- Umsetzung und Zertifizierung eines ISMS stellt Herausforderung für jede Organisation dar
- gerade kleine Unternehmen profitieren von Flexibilität der ISO 27001
- lebendiges ISMS durch Mitgestaltung und angemessene Lösungen
- Mehrwert durch Steuerung der begrenzten Ressourcen

secuvera

Inhalt

- Über uns
- Motivation
- Rahmenbedingungen
- Umsetzung
- Resümee
- Diskussion

secuvera

BSI-zertifizierter IT-Sicherheitsdienstleister und Prüfstelle

Vielen Dank für die Aufmerksamkeit!

Bei Fragen und Anregungen sprechen Sie mich an

Ihr Ansprechpartner:

Björn Lemberg

blemberg@secuvera.de

+49 7031 9758 19