TeleTrusT Information Security Professional

TeleTrusT Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

T.I.S.P. Community Meeting 2023

Berlin, 07. - 08.11.2023

Das organisationsfreundliche ISMS
Der Weg vom Bremsklotz zum Empowerment

Neda Pashah / Infodas GmbH

Das organisationsfreundliche ISMS

Principal IT-Security Consultant
Security Standards und Audit
n.pashah@infodas.de

Ausbildung & Beruf

- Informatikerin
- Anwendungsentwicklung, Projektmanagement, Informationssicherheitsberatung

Schwerpunkte

- Audits und IS-Revisionen
- Sicherheitskonzeption nach BSI-Grundschutz
- Risikomanagement
- Aufbau ISMS nach ISO27001 und BSI 200-1
- Projektmanagement

Qualifikationen

- ISO27001 Lead Auditor
- BSI-Grundschutz Beraterin
- Zertifizierte Projektmanagerin (PMP)
- Zertifizierte Business Continuity Manager

Branchen

- KRITIS
- Industrie
- Behörden

infodas

Agenda

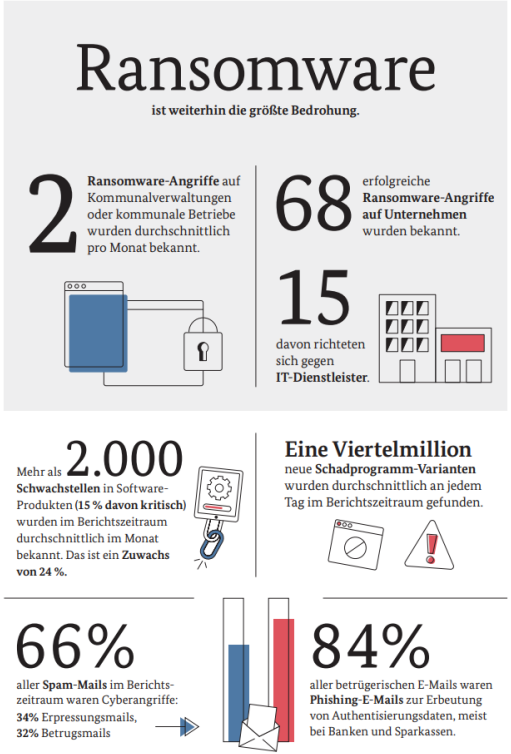
- Aktuelle Zahlen und Daten
- Was wird mit ISMS assoziiert?
- Hürden und Hindernisse aus der Praxis
- Verwendete Tools & Hilfsmittel
- Zusammenfassung & Fazit

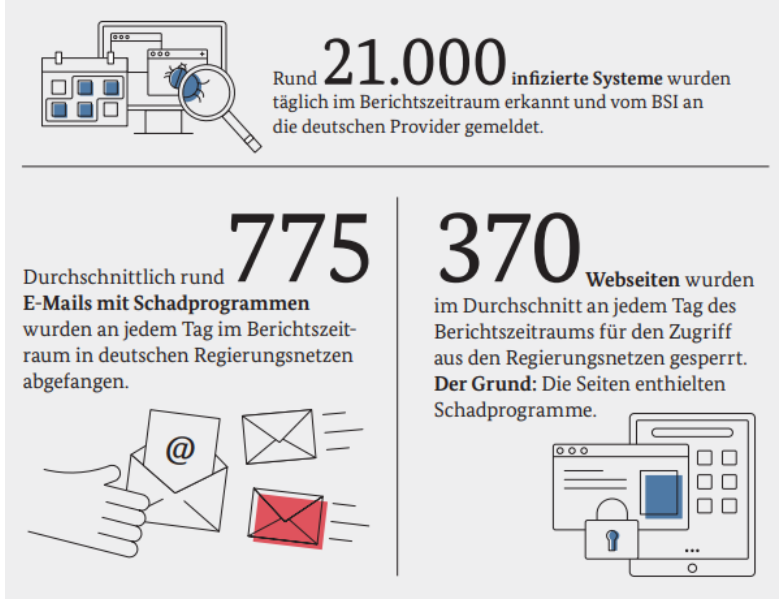
infodas

Aktuelle Zahlen und Daten

infodas

Aktuelle Zahlen und Daten





Quelle: BSI
Die Lage der IT-Sicherheit in Deutschland 2023

Berichtszeitraum: 1. Juni 2022 bis 30. Juni 2023

infodas

Aktuelle Zahlen und Daten

Schaden

206 Milliarden Euro Schaden pro Jahr durch Datendiebstahl, Spionage und Sabotage *

Bedrohungen

Jedes zweite Unternehmen fühlt sich durch Cyberangriffe existentiell bedroht *

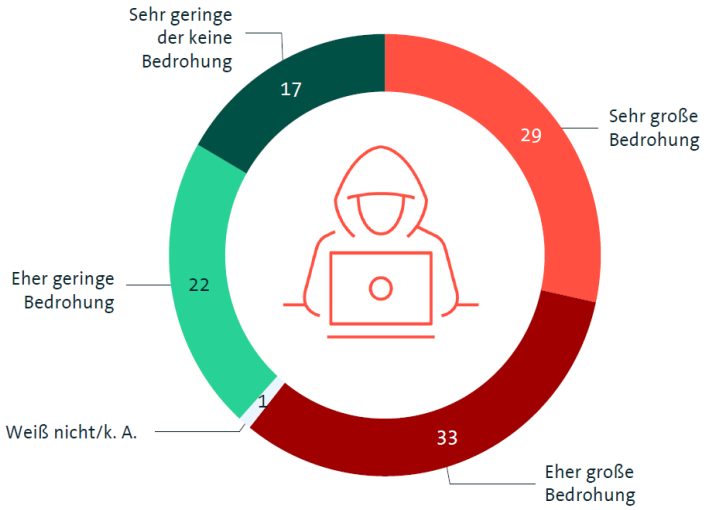
Compliance

NIS2-Umsetzungsgesetz betrifft etwa 30.000 Unternehmen

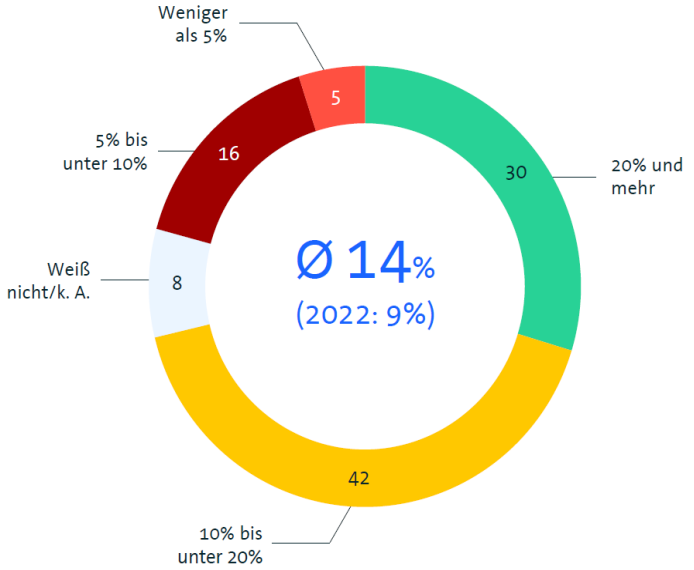
*Bitkom-Studie „Wirtschaftsschutz 2023“

infodas

Aktuelle Zahlen und Daten



6 von 10 Unternehmen sehen große Bedrohung durch analoge und digitale Angriffe



Cybersicherheit: Investitionsbereitschaft steigt

Basis: Alle Unternehmen (n=1.002) | rundungsbedingt kann die Summe der Prozentwerte von 100 abweichen | Quelle: Bitkom Research 2023

infodas

Aktuelle Zahlen und Daten

Die häufigsten Arten von IT-Angriffen

31 %
Phishing

29 %
Angriffe auf Passwörter

28 %
Schadsoftware

23 %
Ransomware

21 %
SQL Injection

Spoofing
14 %

DDoS
12 %

Cross-Site-Scripting
10 %

Man-in-the-Middle
7 %

CEO Fraud
6 %

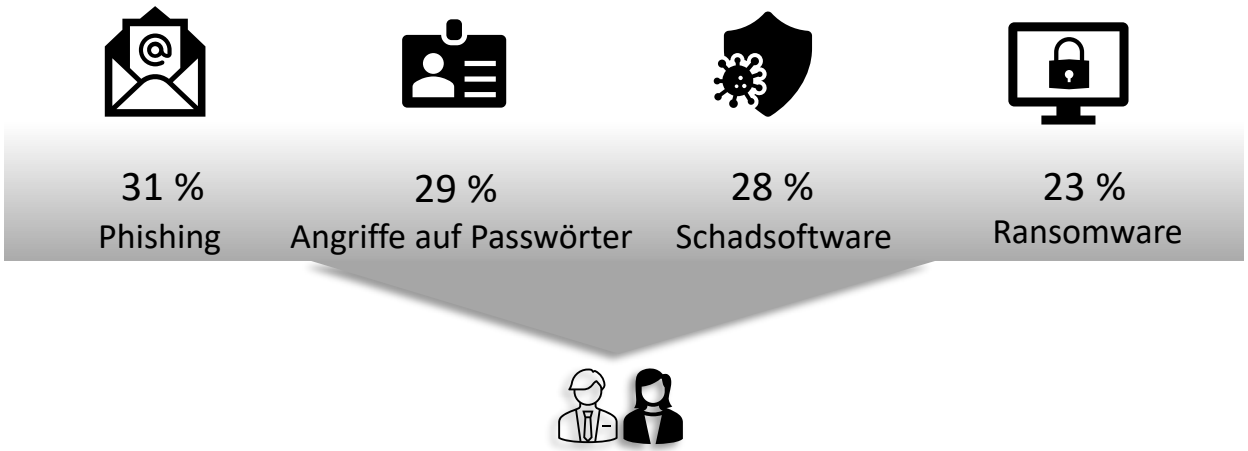
2021-2023

Basis: Alle Unternehmen (n=1.002) | Mehrfachnennungen möglich| Quelle: Bitkom Research 2023

infodas

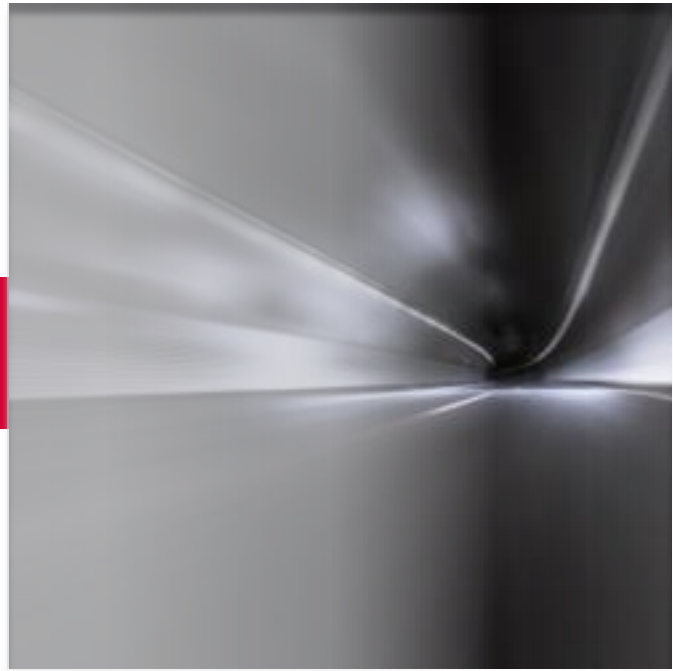
Aktuelle Zahlen und Daten

Die häufigsten Arten von IT-Angriffen



infodas

Was wird mit ISMS assoziiert?



infodas

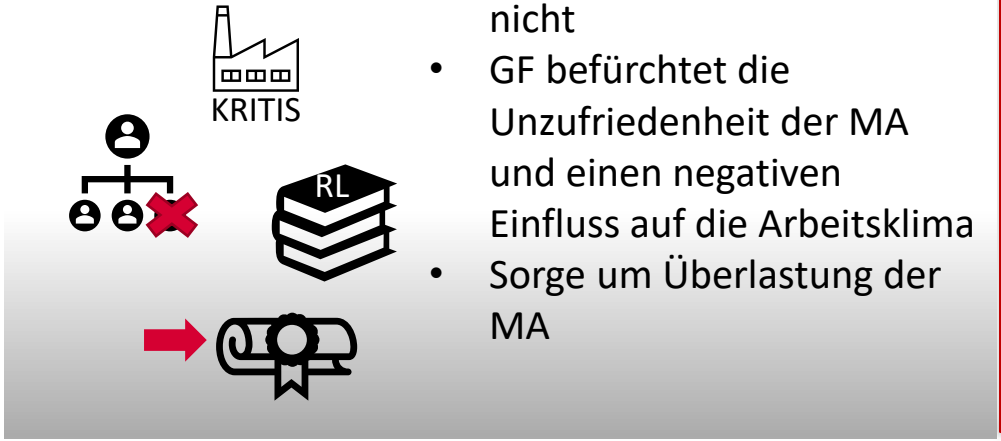
Was wird mit ISMS assoziiert?

infodas

Hürden und Hindernisse aus der Praxis

infodas

Vorbehalt der Geschäftsführung

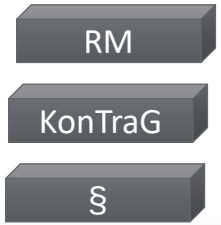


- Die GF unterschreibt die RL nicht
- GF befürchtet die Unzufriedenheit der MA und einen negativen Einfluss auf die Arbeitsklima
- Sorge um Überlastung der MA

- Einbindung der GF in den Prozess
- Konsequentes Stakeholder-Management
- Schaffung von Transparenz durch bewährte PM-Methoden ggü. der GF

infodas

Unternehmensrisikomanagement vs. Informationssicherheits-Risikomanagement

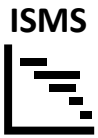


- Die aus dem ISMS resultierenden Risiken sind für das übergeordnete RM zu detailliert
- Die Methodik und Paramater sind teilweise unterschiedlich

- Klärung der organisatorischen und technischen Schnittstellen
- Abstimmung und Erstellung einer ISMS-Risikomanagementrichtlinie in Einklang mit dem übergeordneten RM
- Erstellung einer Mappingtabelle
- Schulungen und Informationsveranstaltungen für die Betroffenen

infodas

Abstrakte und organisationsfremde Formulierungen



- Keine Freigabe der RL durch das Management
- Problem: Die Dokumentationssprache passt nicht zur Unternehmenskultur
- Es gibt ein begrenztes Verständnis der RL

- Einbindung der Fachabteilungen
- Überarbeitung aller RL
- Orientierung an die bestehende Dokumentenlandschaft und Dokumentationskultur der Organisation

infodas

Herausforderung „Maßnahmenplan“

ISMS √

GS-Check √

+ RM

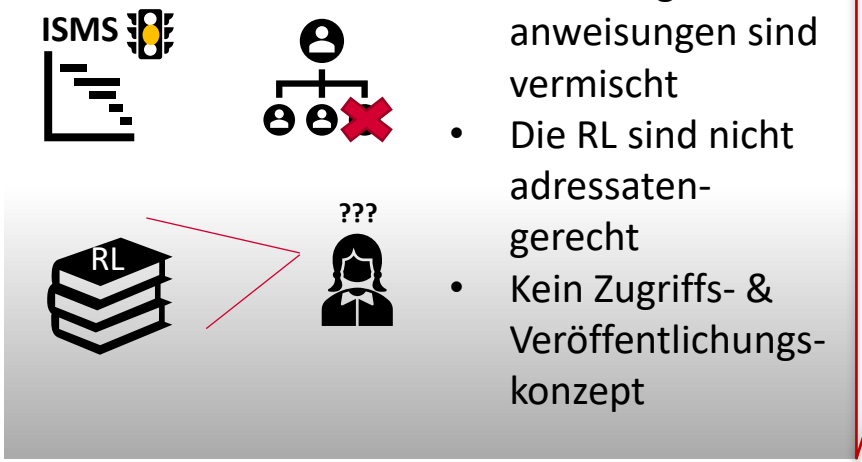
Audit 1st & 2nd Party √

- ToDos und Maßnahmen befinden sich in diversen Formaten
- Zuweisung von Zuständigkeiten fehlt
- Keine Kontrolle über die Überfälligkeit der Maßnahmen

- Klärung der Zuständigkeiten für die Umsetzung und Kontrolle der Maßnahmen
- Vollständige und transparente Dokumentation des Prozesses

infodas

Fehlende Definition von Dokumentenstruktur & -hierarchie



- RL, Verfahren und Handlungs-anweisungen sind vermischt
- Die RL sind nicht adressaten-gerecht
- Kein Zugriffs- & Veröffentlichungs-konzept

- Definition der Dokumentenhierarchie
- Aufteilung der RL in RL, Verfahren und Handlungsanweisungen
- Überarbeitung des Berechtigungskonzeptes für das Intranet

infodas

Definition des Scopes / Informationsverbundes

- Geltungsbereich zu klein gewählt
- Es fehlen dokumentierte Prozesse
- Sehr viele interne Schnittstellen zur Muttergesellschaft (HR, RM, Einkauf,…)
- Das ISMS ist nicht zertifizierbar

- Umfeldanalyse
- Dienstleistungskatalog Mutter- / Tochtergesellschaft
- Erstellung von OLA (Operational-Level-Agreement)

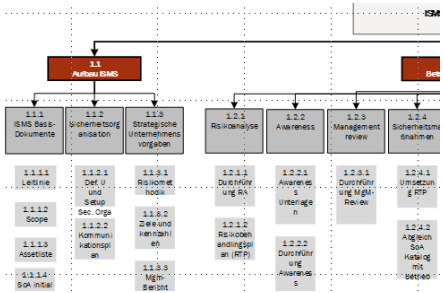
infodas

Verwendete Tools und Hilfsmittel

infodas

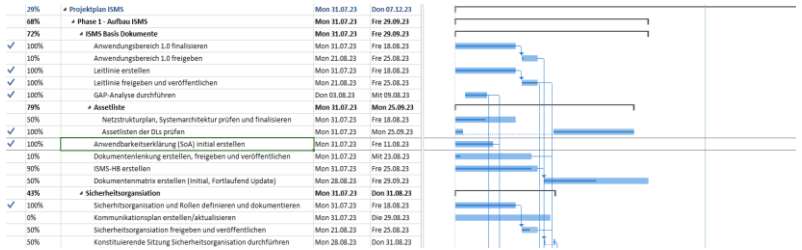
Tools und Hilfsmittel

PSP – Aufbau ISMS



- Durch einen Projektstrukturplan die Komplexität reduzieren
- Das Management mit bekannten Instrumenten überzeugen

Projektplan – Aufbau ISMS



	29%	Projektplan ISMS	Mon 31.07.23	Don 07.12.23
	68%	Phase 1 - Aufbau ISMS	Mon 31.07.23	Fre 29.09.23
	72%	ISMS Basis Dokumente	Mon 31.07.23	Fre 29.09.23
✓	100%	Anwendungsbereich 1.0 finalisieren	Mon 31.07.23	Fre 18.08.23
	10%	Anwendungsbereich 1.0 freigeben	Mon 21.08.23	Fre 25.08.23
✓	100%	Leitlinie erstellen	Mon 31.07.23	Fre 18.08.23
✓	100%	Leitlinie freigeben und veröffentlichen	Mon 21.08.23	Fre 25.08.23
✓	100%	GAP-Analyse durchführen	Don 03.08.23	Mit 09.08.23
	79%	Assetliste	Mon 31.07.23	Mon 25.09.23
	50%	Netzstrukturplan, Systemarchitektur prüfen und finalisieren	Mon 31.07.23	Fre 18.08.23
✓	100%	Assetlisten der DLs prüfen	Mon 31.07.23	Mon 25.09.23
✓	100%	Anwendbarkeitserklärung (SoA) initial erstellen	Mon 31.07.23	Fre 11.08.23
	10%	Dokumentenlenkung erstellen, freigeben und veröffentlichen	Mon 31.07.23	Mit 23.08.23
	90%	ISMS-HB erstellen	Mon 31.07.23	Fre 25.08.23
	50%	Dokumentenmatrix erstellen (Initial, Fortlaufend Update)	Mon 28.08.23	Fre 29.09.23
	43%	Sicherheitsorganisation	Mon 31.07.23	Don 31.08.23
✓	100%	Sicherhitsorganisation und Rollen definieren und dokumentieren	Mon 31.07.23	Fre 18.08.23
	0%	Kommunikationsplan erstellen/aktualisieren	Mon 31.07.23	Die 29.08.23
	50%	Sicherheitsorganisation freigeben und veröffentlichen	Mon 21.08.23	Fre 25.08.23
	50%	Konstituierende Sitzung Sicherheitsorganisation durchführen	Mon 28.08.23	Don 31.08.23

- Die Aktivitäten planen und tracken
- Zuständigkeiten zuweisen
- Prioritäten festlegen
- Meilensteine planen und verfolgen

infodas

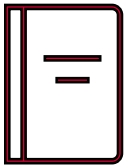
Tools und Hilfsmittel

ISMS-Handbuch

- Anker-Dokument für das ISMS
- Überblick über wichtigste Themen und Prozesse
- Leitfaden für den Auditor
- Je nach Organisation: ein umfassendes mächtiges Gesamtdokument über Informationssicherheit

Dokumentenmatrix

- Übersicht aller ISMS-Dokumente
- Planung und Dokumentation der Aktualisierungen
- Angaben über den Ablageort
- Überblick über die Aktualität und Verantwortlichkeiten der Dokumente

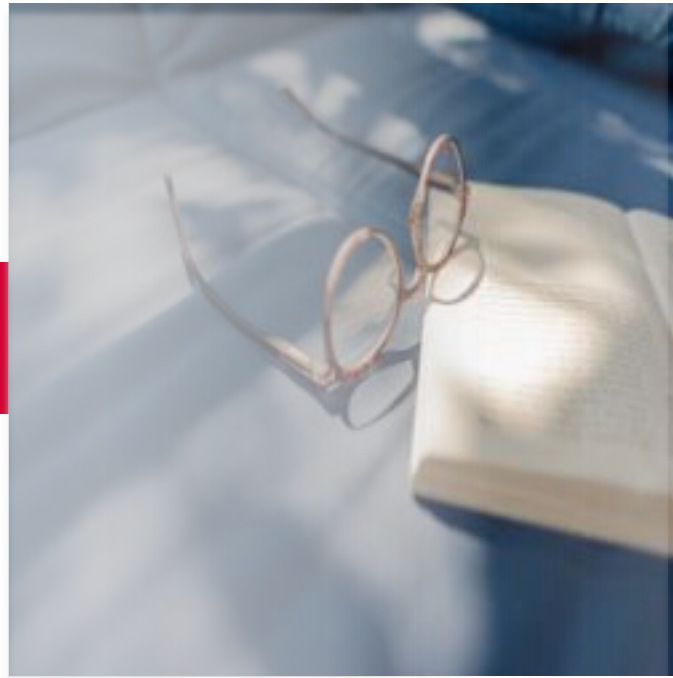


Sicherheits-organisation

- Festlegung des Gremiums
- Befugnisse des Gremiums
- Aufgaben der Key-Mitglieder
- Sitzungsintervale
- Kommunikation

infodas

Zusammenfassung und Fazit



Zusammenfassung

Erfolgsfaktor: Vorbereitung

Einen geeigneten Scope definieren, klare Abgrenzungen setzen und technische und organisatorische Schnittstellen beschreiben

Sicherheitsorganisation konzipieren, gründen und in Kraft setzen

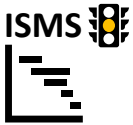
Durch Informationsveranstaltungen die Organisation auf allen Ebenen vorbereiten (Stakeholder-Management)

Frühzeitig Dokumentenhierarchien festlegen

infodas

Zusammenfassung

Erfolgsfaktor: Vorgehen



Aufbau ISMS mit bewährten PM-Methoden und Tools strukturieren, planen und steuern

Den Fokus auf die Prozesse legen, anstatt sich auf die Dokumentation zu konzentrieren

Zunächst eine Bewertung des IST-Standes vornehmen (Reifegradanalyse)

Sich dem Thema Schritt für Schritt annähern

infodas

Zusammenfassung

Erfolgsfaktor: Integration

So früh wie möglich das ISMS leben und sukzessive wachsen

Schaffung einer Parallelwelt vermeiden

ISMS mit Aufbau- und Ablauforganisation verzahnen

ISMS so gestalten, dass es nahtlos zur Unternehmenskultur passt

infodas

Zusammenfassung

Erfolgsfaktor: Synergie

Die Potenziale von funktionsübergreifenden Teams innerhalb der Organisation ausschöpfen:

- Risikomanagement
- Qualitätsmanagement
- Compliance-Management
- 1st-Level Support
- …

infodas

Zusammenfassung

Erfolgsfaktor: Messbarkeit

Frühzeitig messbare und quantifizierbare Ziele festlegen

Messbare Indikatoren, Kennzahlen und Erfassungsverfahren definieren

Regelmäßig den Fortschritt der Informationssicherheit verfolgen

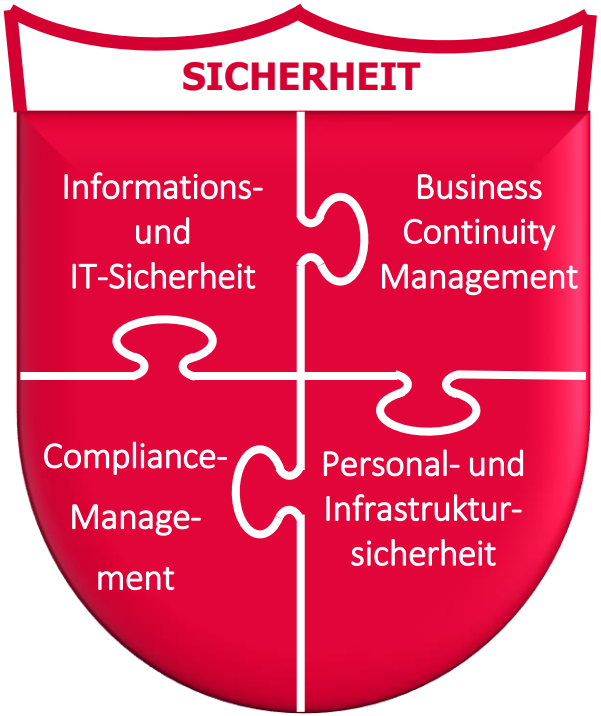
infodas

Stärkung des Unternehmens

infodas

Fazit

Ein organisationsfreundliches ISMS überzeugt nicht nur im Audit, sondern auch im Alltag



infodas

Vielen Dank für Ihre Aufmerksamkeit!

infodas