
DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

Agenda

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

Grundlagen & wichtige Fachbegriffe der Informationssicherheit

Schützenswerte Daten & Datensicherheit

Ausmaß potentieller Schäden

Agenda

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

Schwachstellen identifizieren

Mobile Geräte

Gefahren durch soziale Netzwerke

Agenda

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

Schadsoftware wie Viren, Würmer und Trojaner

Nötige Schritte zur Umsetzung eines ISMS

Ihr Referent - Jörg Deusinger

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

Jörg Deusinger

Geschäftsführer de-bit Computer-Service GmbH

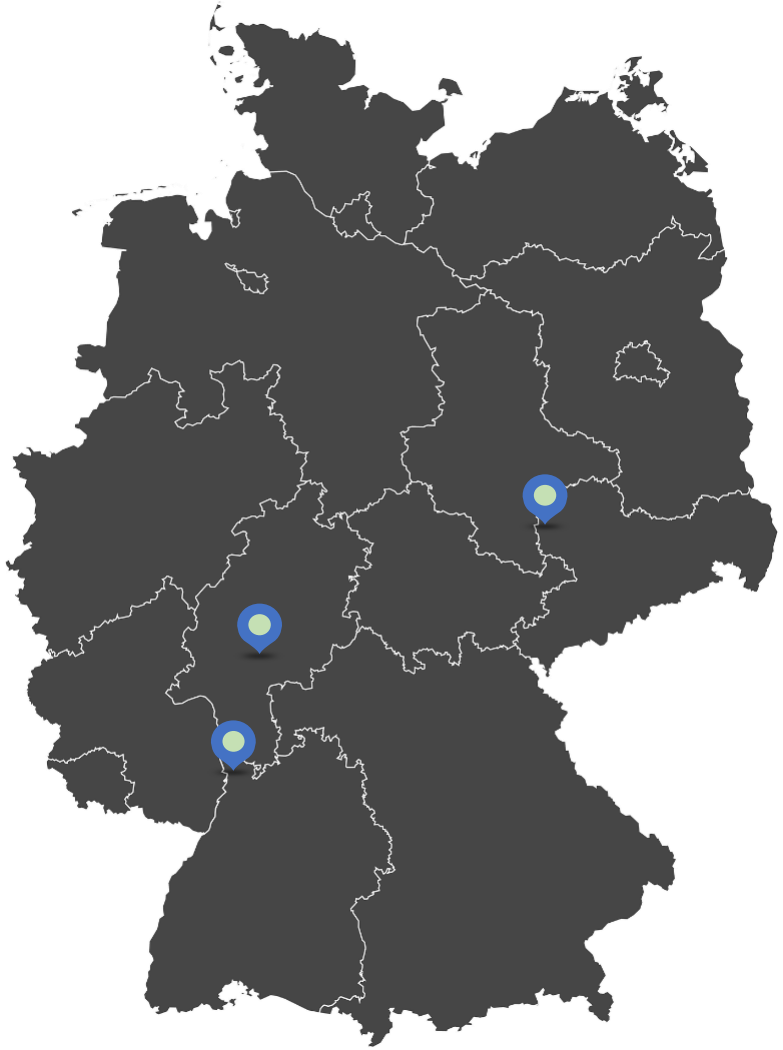
Principal Consultant Information Security & Data Protection
über 15 Jahre Berufserfahrung

- ISO 27001 – Auditteamleiter auf Basis von IT-Grundschutz (BSI)
- IS-Revisions- und IS-Beratungsexperte auf der Basis von IT-Grundschutz (BSI)
- Zertifizierter IT-Grundschutz-Berater (BSI)
- ISO/IEC 27001:2013 – Lead Auditor (NATIV)
- Zertifizierter Auditor „Secure CA Operation" für TR-03145 (BSI)
- Zertifizierter Auditor „Smart Meter Gateway Administration“ für BSI TR-03109-6 (BSI)
- Fachkundig geprüfter Datenschutzauditor (TÜV Rheinland)
- Fachkundig geprüfter Datenschutzbeauftragter nach dem „Ulmer Modell“
- Auditor auf Basis des IT-Sicherheitskataloges nach § 11 Abs. 1a EnWG (ENERGIE)
- Zusätzliche Prüfverfahrens-Kompetenz für § 8a (3) BSIG - branchenspezifische Sicherheitsstandards (B3S)
- Foundation Certificate in IT Service Management
- Systems Engineer Messaging on Windows Server

de-bit Computer-Service GmbH

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

- ✓ **Datenschutz, Audits, Zertifizierung** und **Informationssicherheit**
- ✓ **IT-Services, Managed Services, User-Help-Desk**
- ✓ Mehr als **60 Spezialisten**
- ✓ Standorte in **Gelnhausen**, **Mannheim** & **Leipzig**



Bundesamt für Sicherheit in der Informationstechnik
ISO 27001-Zertifikat
auf der Basis von IT-Grundschutz
Zertifikat Nummer:
BSI-IGZ-0356-2019
Gültig bis 03.06.2022

made in MAIN-KINZIG

IHK Ausbildungsbetrieb

de-bit Computer-Service GmbH

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

infaz
Institut für Auditierung und Zertifizierung

ZERTIFIKAT
DIN EN ISO 9001

ZERTIFIKAT · CERTIFICATE · CERTIFICAT

Institut für Auditierung
und Zertifizierung GmbH
bescheinigt dem Unternehmen

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

de-bit Computer Service GmbH
Seestraße 11
D-63751 Gelnhausen

für den Geltungsbereich:

Erbringung von Dienstleistungen in den Bereichen:
IT-Technik & IT-Sicherheit, IT-Service, Datenschutz,
Informationssicherheit, IT-Prozesse & Analysen,
Implementierung von Managementsystemen

die wirksame Anwendung eines Qualitätsmanagementsystems.

Durch das Audit, Bericht Nr.: A 004/2019, wurde der Nachweis erbracht,
dass die Forderungen der DIN EN ISO 9001:2015 erfüllt sind.

Dieses Zertifikat ist gültig bis: 15.03.2022
Zertifikat-Registrier-Nr.: 006/03/2019

Neuss, 16.03.2019
Geschäftsführung

Infaz - Institut für Auditierung und Zertifizierung GmbH • Nixhütter Weg 85 • D-41468 Neuss

infaz
Institut für Auditierung und Zertifizierung

ZERTIFIKAT
ISO/IEC 27001

ZERTIFIKAT · CERTIFICATE · CERTIFICAT

Institut für Auditierung
und Zertifizierung GmbH
bescheinigt dem Unternehmen

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

de-bit Computer Service GmbH
Seestraße 11, 63751 Gelnhausen

für den Geltungsbereich:

Bereitstellung von Einrichtungen, die für interne
und externe Kommunikation sowie zum Hosting und zur
Dienstleistungserbringung - auch vor Ort - erforderlich sind

die wirksame Anwendung eines Informationssicherheits-Managementsystems.

Durch das Audit, Bericht Nr.: A 014/2018, wurde der Nachweis erbracht,
dass die Forderungen der ISO/IEC 27001:2013 erfüllt sind.

Anwendbarkeitserklärung (SoA): 0050_SOA_01, Stand: 02.03.2015

Dieses Zertifikat ist gültig bis: 31.03.2021
Zertifikat-Registrier-Nr.: 012/06/2018

Neuss, 21.04.2018
Geschäftsführung

Infaz - Institut für Auditierung und Zertifizierung GmbH • Nixhütter Weg 85 • D-41468 Neuss

Bundesamt
für Sicherheit in der
Informationstechnik

Zertifikat
nach Technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik

BSI-IGZ-0356-2019

ISO 27001-Zertifikat auf der Basis von IT-Grundschutz

Bereitstellung IT-Systeme und Komponenten für die Erbringung
von IT-Dienstleistungen und Consulting

der de-bit Computer-Service GmbH

gültig bis: 3. Juni 2022*

ISO 27001-Zertifikat
auf der Basis von IT-Grundschutz
Zertifikat Nummer:
BSI-IGZ-0356-2019
Gültig bis 03.06.2022

Der Untersuchungsgegenstand umfasst die Infrastruktur, die IT-Systeme und die unterstützenden Prozesse der de-bit Computer-Service GmbH für die Erbringung von IT-Dienstleistungen für Geschäftskunden. Hierbei übernimmt die de-bit Computer-Service GmbH Dienstleistungen die Administration einzelner Systeme bis hin zur Administration der gesamten IT-Netzwerk- und Systemumgebung des Kunden sowie die Beratung der dortigen Administratoren im Bereich IT Administration. Hierzu gehören Server, zentrale Systeme, Netzwerke, Netzwerkkomponenten und Arbeitsplatzsysteme in den Räumlichkeiten der Kunden, sowie entsprechende Client-Systeme und Komponenten für den mobilen Einsatz. Die Dienstleistungen werden sowohl aus den eigenen Räumlichkeiten in Gelnhausen oder direkt beim Kunden vor Ort erbracht. Die hierfür benötigten IT-Systeme werden von der de-bit Computer-Service GmbH selbst betrieben. Für die verschiedenen Tätigkeiten sind redundante Interanbindungen von unterschiedlichen Providern beauftragt. Neben den Dienstleistungen hinsichtlich des IT-Services werden von der de-bit Computer-Service GmbH ebenfalls Beratungsleistungen im Bereich der Informationssicherheit und des Datenschutzes entsprechend des Leistungsspektrums angeboten.

Der oben aufgeführte Untersuchungsgegenstand wurde von Dr. Christian Scharff, zertifizierter Auditor für ISO 27001-Audits auf der Basis von IT-Grundschutz, in Übereinstimmung mit dem Zertifizierungsschema des Bundesamtes für Sicherheit in der Informationstechnik geprüft. Die im Auditbericht enthaltenen Schlussfolgerungen des Auditors sind im Einklang mit den erbrachten Nachweisen.

Die durch dieses Zertifikat bestätigte Anwendung von ISO 27001 auf der Basis von IT-Grundschutz umfasst die Maßnahmenziele und Maßnahmen aus Annex A von ISO/IEC 27001 und die damit verbundenen Ratschläge zur Umsetzung und Anleitungen für allgemein anerkannte Verfahren aus ISO/IEC 27002. Dieses Zertifikat ist keine generelle Empfehlung des Untersuchungsgegenstandes durch das Bundesamt für Sicherheit in der Informationstechnik. Eine Gewährleistung für den Untersuchungsgegenstand durch das Bundesamt für Sicherheit in der Informationstechnik ist weder enthalten noch zum Ausdruck gebracht.

Dieses Zertifikat gilt nur für den angegebenen Untersuchungsgegenstand und nur in Zusammenhang mit dem vollständigen Zertifizierungsreport.

Bonn, den 4. Juni 2019
Bundesamt für Sicherheit in der Informationstechnik
Im Auftrag

Bernd Kowalski
Abteilungspräsident

* Unter der Bedingung, dass die ab 4. Juni 2019 jährlich durchzuführenden Überwachungsaudits mit positivem Ergebnis abgeschlossen werden.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189, D-53175 Bonn · Postfach 20 03 63, D-53133 Bonn
Tel.: +49 (0)228 9582-0 · Fax: +49 (0)228 9582-5477 · Infoline: +49 (0)228 9582-111 · Internet: www.bsi.bund.de

Leistungsspektrum im Bereich Informationssicherheit

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

Implementierung eines ISMS nach DIN ISO/IEC 27001 ✓

Implementierung eines ISMS nach ISO 27001 auf Basis von IT-Grundschutz ✓

Betrieb einer CERT-Stelle ✓

Stellung externer Informationssicherheits- und IT-Sicherheitsbeauftragter ✓

Schwachstellenmanagement und Scan der IT-Infrastruktur ✓

Leistungsspektrum im Bereich Datenschutz

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

Externer Datenschutzbeauftragter

Unterstützung des betrieblichen Datenschutzbeauftragten

Gezielte Beratung in speziellen Themen

Leistungsspektrum im Bereich Audits

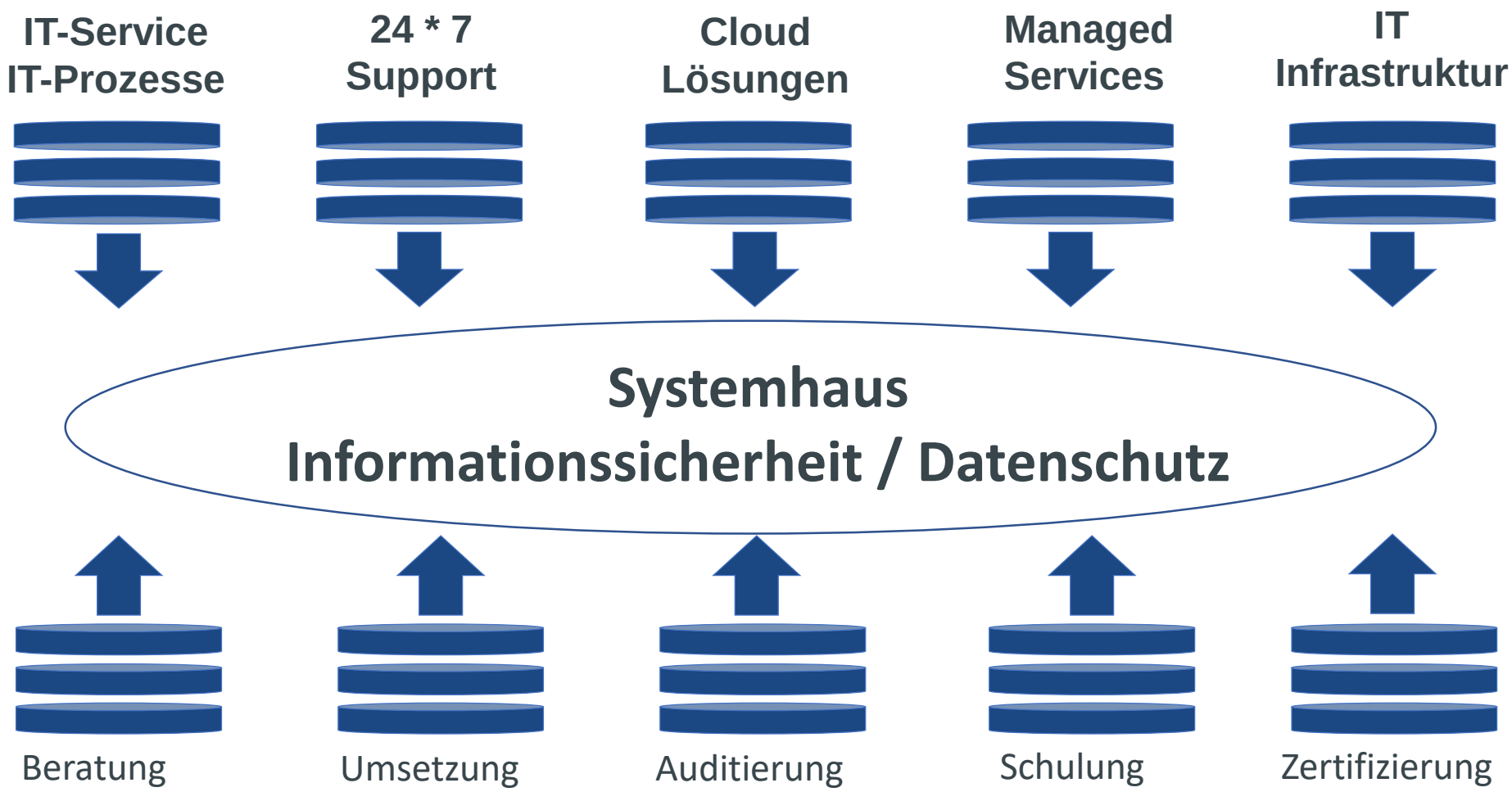
DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

Unser Team besitzt Zulassungen zur Auditierung für folgende Normen und Prüfgrundlagen

- ISO/IEC 27001 ✓
- ISO 27001 auf Basis von IT-Grundschutz ✓
- Datenschutzaudits (ohne Zertifizierung) ✓
- §8a BSIG (KRITIS) ✓
- IT-SICHERHEITSKATALOG GEM. §11 ABS. 1A ENWG ✓

Leistungsspektrum IT-Service – de-bit GmbH

Leistungsspektrum IT-Service – de-bit GmbH



Zertifizierungsstellen – Berufungen / Partnerschaften

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

Fachpartner der Kreiswerke Main-Kinzig GmbH im Bereich
„Zertifizierte IT-Dienstleistungen“

KITuS
Zertifizierte IT-Dienstleistungen
Kreiswerke Main-Kinzig

Bundesamt für Sicherheit in der Informationstechnik (BSI) aus Bonn

Bundesamt
für Sicherheit in der
Informationstechnik

Infaz, Institut für Auditierung und Zertifizierung
aus Neuss

infaz
Institut für Auditierung und Zertifizierung
INFORMATIONSSICHERHEITSMANAGEMENTSYSTEM
DIN ISO/IEC 27001 zertifiziert
Institut für Auditierung und Zertifizierung

Kiwa Deutschland GmbH
aus Hamburg

kiwa

Leistungsspektrum IT-Service – de-bit GmbH / KITuS

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

Die Kreiswerke Main-Kinzig GmbH und die de-bit Computer Service GmbH bietet dazu Full-Service Dienstleistungen im IT-Bereich an.

- Beratung bei Anschaffungen, Ausrüstung, strategischer Ausrichtung und Organisation der IT
- Durchführung von Projektstudien
  (bspw. IT-Audits, IT-Sachstandbewertungen, Management- empfehlungen, IT-Strategien)
- Durchführung und Begleitung von Projekten
- Zentralisierung/ Übernahme des IT-Betriebs von Servern (RZ) und Endgeräten (Clients)
- Aufbau Informationssicherheitsmanagement für die Organisation eines sicheren IT-Betriebs
- Beistellung von Informationssicherheits-Beauftragten, Datenschutz-Beauftragten, Zusammenschluss und Aufnahme in Arbeitskreisen mit anderen Betreibern
- Schwachstellenscans der IT-Umgebung (SECaaS)

IT-Betrieb aus dem Rechenzentrum für Server und Endgeräte

- Bereitstellung von kundenindividuellen Servern
- Betrieb von zentralen IT-Services für alle Benutzer
  (bspw. Outlook, Office,…)
- Bereitstellung von Arbeitsplatzcomputern (Clients)
- Inklusive aller Leistungen zum Betrieb der IT-Umgebung

Security as a Service (SECaaS)

- Dauerhafter, automatisierter Schwachstellenscan von IT-Umgebungen inkl. Reporting
- Beistellung von Informationssicherheits-Beauftragten und Datenschutz-Beauftragten
- Consulting und Sensibilisierungsmaßnahmen

Backup- und private Cloud-Dienste

- Organisation der Datensicherung und verschlüsselte Auslagerung der Daten in das Kreiswerke Rechenzentrum
- Bereitstellung von Datenspeicher/ Datenaustauschplattformen
  - Verfügbar im Internet über unseren gesicherten Cloud-Server
  - Zum Bereitstellen von Dokumenten für Externe oder für die Zusammen- arbeit mit anderen Dienstleistern

Telefonanlage aus dem Rechenzentrum

- Bereitstellung einer mandantenfähigen VoIP-Telefonanlage
  inkl. ausgesuchter Leistungsmerkmale der Telefonie
- Hard- und Softphones verfügbar
- Konzeptionierung der Telefonie-Umgebung

Grundlagen & wichtige Fachbegriffe der Informationssicherheit

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

Informationssicherheit

Informationssicherheit hat den Schutz von **Informationen** als Ziel. Dabei können Informationen sowohl auf Papier, in Rechnern oder auch in Köpfen gespeichert sein.

Die Schutzziele oder auch Grundwerte der Informationssicherheit sind mindestens *Vertraulichkeit*, *Integrität* und *Verfügbarkeit*.

Viele Anwender ziehen in ihre Betrachtungen weitere Grundwerte mit ein.

Informationssicherheitsmanagement (ISM)

Die **Planungs-, Lenkungs- und Kontrollaufgaben**, die erforderlich sind, um einen durchdachten und wirksamen Prozess zur Herstellung von Informationssicherheit aufzubauen und kontinuierlich umzusetzen, wird als Informationssicherheitsmanagement bezeichnet.

Dabei handelt es sich um einen kontinuierlichen Prozess, dessen Strategien und Konzepte ständig auf ihre Leistungsfähigkeit und Wirksamkeit zu überprüfen und bei Bedarf fortzuschreiben sind.

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

Informationssicherheitsmanagementsystem (ISMS)

Ein Informationssicherheitsmanagementsystem soll geordnete Prozesse und Verfahren zum Umgang mit den Problemstellungen der Informationssicherheit definieren und entsprechend bereitstellen.

Dabei gilt es ein angemessenes Informationssicherheitsniveau dauerhaft zu gewährleisten!

Das verfolgte Ziel eines ISMS ist es das Sicherheits- und Kontinuitätsniveau von Informationen nachhaltig und effektiv sicher, indem Unternehmensrichtlinien, Geschäftsprozesse, Mitarbeiter und IT-Strukturen einbezogen und risikoorientiert geschützt werden.

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

Informationssicherheitsbeauftragter (ISB)

Ein Informationssicherheitsbeauftragter ist für die operative Erfüllung der Aufgabe „Informationssicherheit“ sowie für alle Fragen rund um die Informationssicherheit zuständig.

Die Rolle des ISB MUSS von einer Person mit Fachkompetenz zur Informationssicherheit sowie zur Informationstechnik (IT) wahrgenommen werden.

Zur Wahrung der Unabhängigkeit MUSS der ISB direkt der obersten Leitung zugeordnet sein.

Grundlagen – Aufgaben eines ISB (Auszug)

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

- Den Sicherheitsprozess steuern und koordinieren
- Die Leitung bei der Erstellung der Sicherheitsleitlinie unterstützen
- Die Erstellung von Richtlinien, Konzepten und Verfahren koordinieren
- Realisierungspläne für Sicherheitsmaßnahmen anzufertigen sowie ihre Umsetzung initiieren und überprüfen
- Der Leitungsebene und anderen Sicherheitsverantwortlichen über den Status der Informationssicherheit berichten
- Sicherheitsrelevante Projekte koordinieren
- Sicherheitsrelevante Vorfälle untersuchen
- Sensibilisierungen und Schulungen zur Informationssicherheit zu initiieren und zu koordinieren

Grundlagen – Schutzziele der Informationssicherheit

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

- Die grundlegende Aufgabe der Informationssicherheit ist im Allgemeinen der Schutz von Informationen vor der anwachsenden Zahl der Gefahren und Bedrohungen.

- Augenmerk liegt auf denjenigen Informationen, die als schutzbedürftig eingestuft werden.

- **Sicherstellung der Informationssicherheit durch Erfüllung bzw. Aufrechterhaltung der Schutzziele.**

Grundlagen – Schutzziele der Informationssicherheit

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

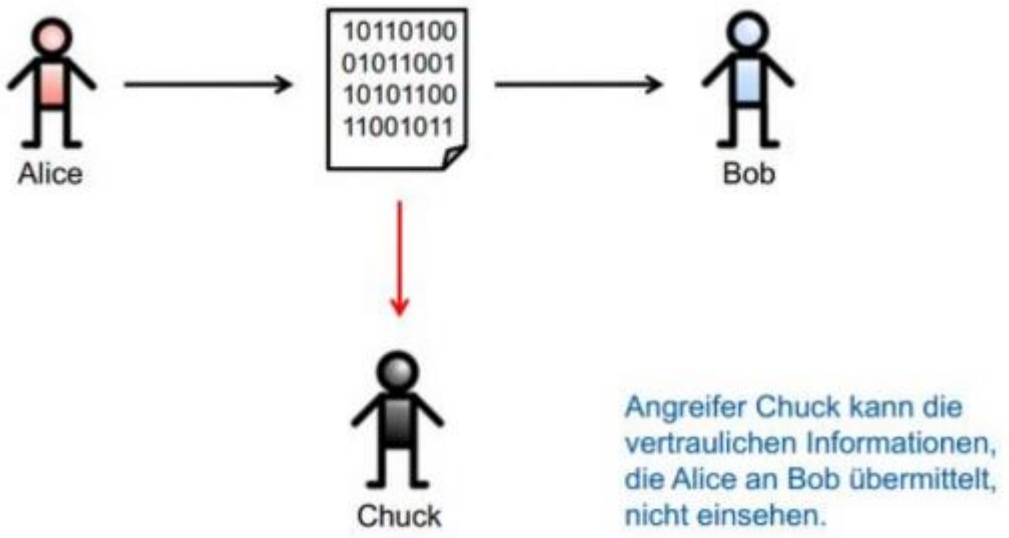
Klassische Schutzziele

Erweiterte Schutzziele

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

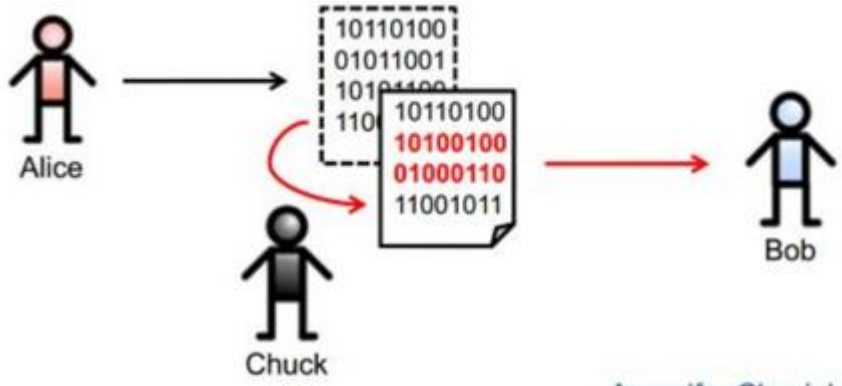
Vertraulichkeit:

- **Schutz von Informationen vor unberechtigter Offenlegung .**
- Vertraulichkeit bezeichnet die Eigenschaft, dass eine Information für unbefugte bzw. unautorisierte Personen oder Prozesse nicht zugänglich ist und von diesen auch nicht offengelegt werden kann.



Integrität:

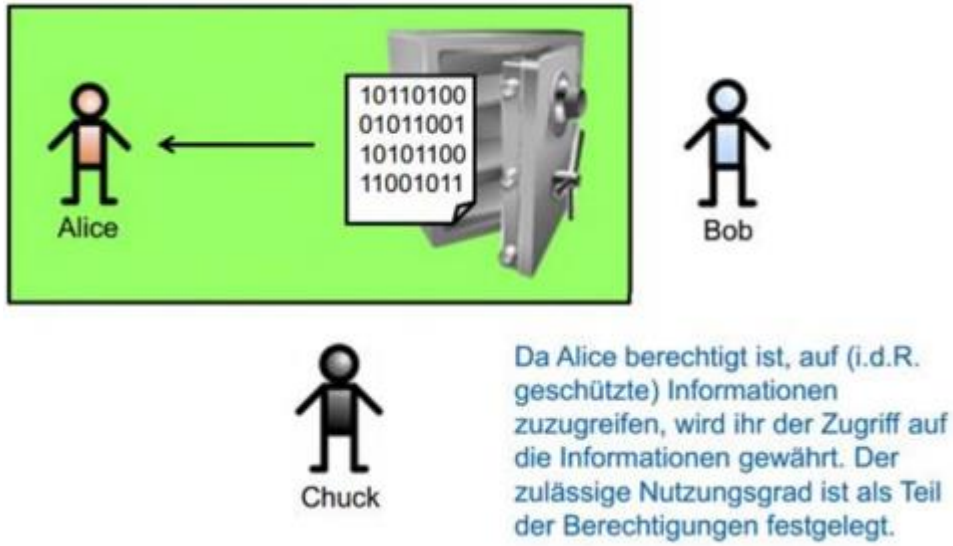
- **Schutz von Informationen vor Modifikation, Manipulation, Löschung, Umordnen, Duplikaten.**
- Mit der Integrität wird eine Eigenschaft bezeichnet, die Informationen und Werte im Hinblick auf die Richtigkeit und Vollständigkeit schützt und jede Veränderung angemessen erkennt.



Angreifer Chuck kann die Informationen, die Alice an Bob übermittelt, nicht (unbemerkt) manipulieren.

Verfügbarkeit:

- **Zugänglichkeit und Nutzbarkeit von Informationen für berechtigte Personen oder Services.**
- Verfügbarkeit bezeichnet die Eigenschaft einer Information oder eines Wertes für einen berechtigten Nutzer verfügbar und nutzbar zu sein, sobald der Nutzer dies verlangt.



Neben den klassischen Schutzzielen könne je nach Zielsetzung ergänzend zusätzliche bzw. erweiterte Schutzziel der Informationssicherheit hinzugezogen werden.

Authentizität:

- **Echtheit und Glaubwürdigkeit einer Person oder eines Dienstes.**
- Identitätsnachweis → der Kommunikationspartner ist der, für den er sich ausgibt.
- Authentizität der eigentlichen Daten → erhaltene Daten stammen auch tatsächlich von der authentisierten Instanz.

Grundlagen – Schutzziele der Informationssicherheit

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

Nichtabstreitbarkeit:

- Eintritt eines Ereignisses oder einer Aktion sowie der verursachende Nutzer zweifelsfrei belegbar.
- Ein Nutzer kann die Auslösung einer Aktion später nicht leugnen.

Zurechenbarkeit:

- Zuordenbarkeit eines Nutzers zu einer durchgeführten Aktion.
- Ausgeführte Aktionen können einem Nutzer zweifelsfrei zugeordnet werden.

Schützenswerte Daten & Datensicherheit

Schützenswerte Güter & Daten

Informationen
Ordner, Verträge, Vereinbarungen, Handbücher, Personalakten, usw.

Immaterielle Werte
Reputation, Image, usw.

Software
Anwendungen, Systemsoftware, usw.

Personal
Qualifikation, Fähigkeiten, Fertigkeiten, Erfahrungen, usw.

Physische Werte
Computer, Server, Router, Firewalls, Kommunikationsgeräte, Wechseldatenträger, usw.

Services
Klimaanlagen, Stromanlagen, Wasseranlagen, Telekommunikationsanlagen, usw.

Definition Datensicherheit / Informationssicherheit IT-Sicherheit

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

Unter dem Begriff „Datensicherheit“ versteht man den generellen Schutz aller Daten eines Unternehmens. Dabei handelt es sich sowohl um Daten mit Personenbezug, als auch um Daten, die keinen Bezug zu einer Person herstellen.

Weiterhin gibt es den Begriff der „Informationssicherheit“, der den Schutz von Informationen als Ziel hat. Dabei ist hier ebenfalls unerheblich, ob es sich um digitale oder analoge Informationen handelt und ob diese einen Personenbezug haben. Teilweise wird die Datensicherheit als ein Teil der Informationssicherheit angesehen, da Letzteres umfassender ist.

Auch die „IT-Sicherheit“ ist ein Teil der Informationssicherheit und bezieht sich auf elektronisch gespeicherte Informationen und IT-Systeme. Dabei wird unter IT-Sicherheit nicht nur der Schutz der technischen Verarbeitung von Informationen verstanden. Vielmehr fällt auch die Funktionssicherheit darunter, also das fehlerfreie Funktionieren und die Zuverlässigkeit der IT-Systeme.

Maßnahmen zur sicheren Datenverarbeitung

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

- EU-Datenschutzgrundverordnung (EU-DSGVO) inkl. BDSG neu
- IT-Sicherheitsgesetz: Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme
- KonTraG: Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
- GoBD: Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff durch die Finanzverwaltungen
- S-Ox: Sarbanes-Oxley Act
- COSO: Committee of Sponsoring Organizations of the Treadway Commission
- Basel III, Solvency II
- KWG: Kreditwesengesetz mit Bankenaufsichtliche Anforderungen an die IT (BAIT), Mindestanforderungen an die Compliance-Funktion (MaComp) und an das Risikomanagement (MaRisk (BA)

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

Weitere Spezialvorschriften für die Informationssicherheit

- Produkthaftungsgesetz beziehungsweise § 823 BGB (z.B. bei Softwarekauf)
- Teledienstgesetz (TDG)
- Telekommunikationsgesetz (TKG)
- Wassenar-Abkommen (europäische Kryptoregulierung) und zu berücksichtigende länderspezifische Gesetze, die Einschränkungen hinsichtlich der einsetzbaren Verschlüsselungstechnik vorschreiben
- Grundgesetz Artikel 10 und G10-Gesetz
- Urheberrechtsgesetz (UrhG)
- IT-bezogene Straftaten des StGB: § 202a (Ausspähen von Daten), §202b (Abfangen von Daten), §263a (Computerbetrug), §303a (Datenveränderung), und §303b (Computersabotage)

Maßnahmen zur sicheren Datenverarbeitung

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

- Das „neue“ Bundesdatenschutzgesetz verlangt diverse **Anforderungen an die Sicherheit der Datenverarbeitung.**

- Der Verantwortliche muss dafür Sorgen, dass die Daten unter Berücksichtigung des **Stands der Technik** geschützt werden.

- **Paragraph 64 (vergleichbar §9 BDSG alt - TOM)** des Bundesdatenschutzgesetzes nennt explizite Maßnahmen die erfüllt werden müssen um die Daten entsprechend zu sichern.

Maßnahmen zu sicheren Datenverarbeitung

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

Zugangskontrolle

Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte.

Speicherkontrolle

Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten.

§64 BDSG

Datenträgerkontrolle

Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern.

Benutzerkontrolle

Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte.

Maßnahmen zu sicheren Datenverarbeitung

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

Zugriffskontrolle

Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben.

Übertragungskontrolle

Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.

§64 BDSG

Eingabekontrolle

Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind.

Transportkontrolle

Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden.

Maßnahmen zu sicheren Datenverarbeitung

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

Wiederherstellbarkeit

Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.

Datenintegrität

Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.

§64
BDSG

Zuverlässigkeit

Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.

Auftragskontrolle

Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Maßnahmen zu sicheren Datenverarbeitung

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

Verfügbarkeitskontrolle

Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind.

§64
BDSG

Trennbarkeit

Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können.

5 Regeln für mehr Datensicherheit

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

Regel #1 Updates

Regelmäßiges und zeitnahes Einspielen von Updates

Zentrales Patchmanagement

Regel #2 Virenschutz

Nicht nur auf dem PC, auch Mobilgeräte berücksichtigen

Regel #3 Backup

Ein nicht vorhandenes oder nicht funktionierendes Backup kann fatale Folgen haben

Datensicherungs-konzept erarbeiten

Regel #4 Rechte-vergabe

Need-to-know-Prinzip

Rollenbasiertes Rechtekonzept einführen

Regel #5 Sensibili-sierung

Schulungskonzept entwickeln

Regelmäßige Sensibilisierung zu aktuellen IT-Sicherheitsthemen

Ausmaß potentieller Schäden

Ausmaß potentieller Schäden – Aktuelle Situation

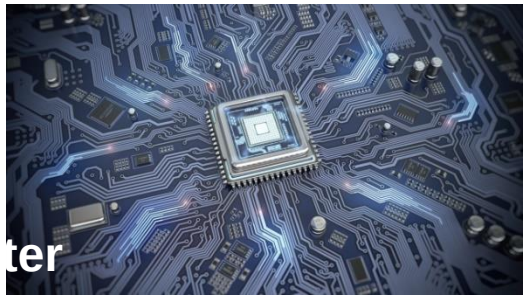
Studie Seagate & IDC:
„The Evolution of Data through 2025“:

Weltweit generiertes Datenvolumen:

2016: 16 Zettabyte
2025: 163 Zettabyte

Davon werden 2025
60% von Unternehmen generiert
(Vgl. 2015: knapp 30%)

➔ **eine Milliarde Terabytes**



Ausmaß potentieller Schäden – Aktuelle Situation

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

Cyber-Sicherheitslage gemäß BSI Lagebericht IT-Sicherheit 2019:

- 114 Mio. neue Schadprogrammvarianten
- Bis zu 110.000 Botinfektionen täglich in deutschen Systemen.
- Angriffsbandbreite bis zu 300 Gbit/s (2018 ca. 100 Gbit/s).
- Ein einzelnes Unternehmen erlitt einen Schaden von 40 Mio. Euro durch einen Ransomware-Angriff.
- **BSI registriert täglich 450.000 Attacken.**
  - **(Nur alleine 09-2019 (von 300.000 aus dem Vormonat))**

https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html

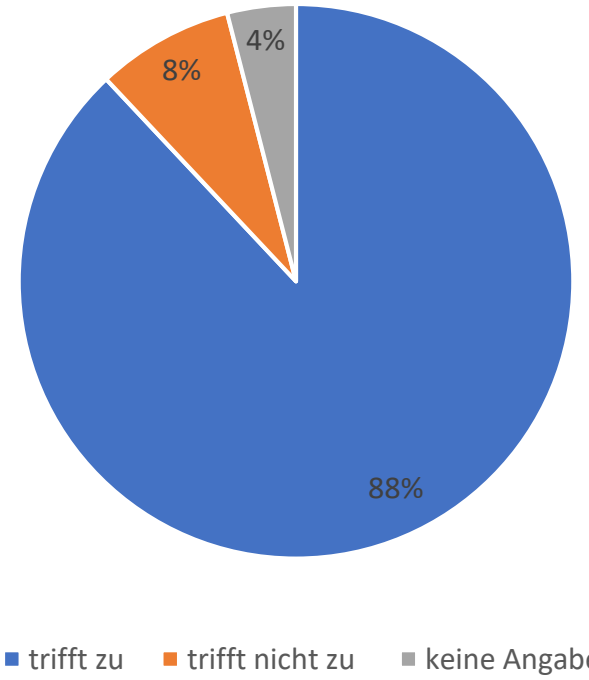
Ausmaß potentieller Schäden – Aktuelle Situation

- Fast neun von 10 Institutionen erwarten von der Digitalisierung eine Verschärfung der Bedrohungslage.

- 88% der Teilnehmenden erkennen, dass die Digitalisierung mit zusätzlichen Cyber-Risiken einhergeht und dass neben den sichtbaren Chancen auch die unsichtbaren Gefahren wachsen.

- 8% gehen davon aus, dass keine zusätzlichen Gefährdungen entstehen.

Im Zuge der Digitalisierung wächst die Angriffsfläche für Bedrohungen

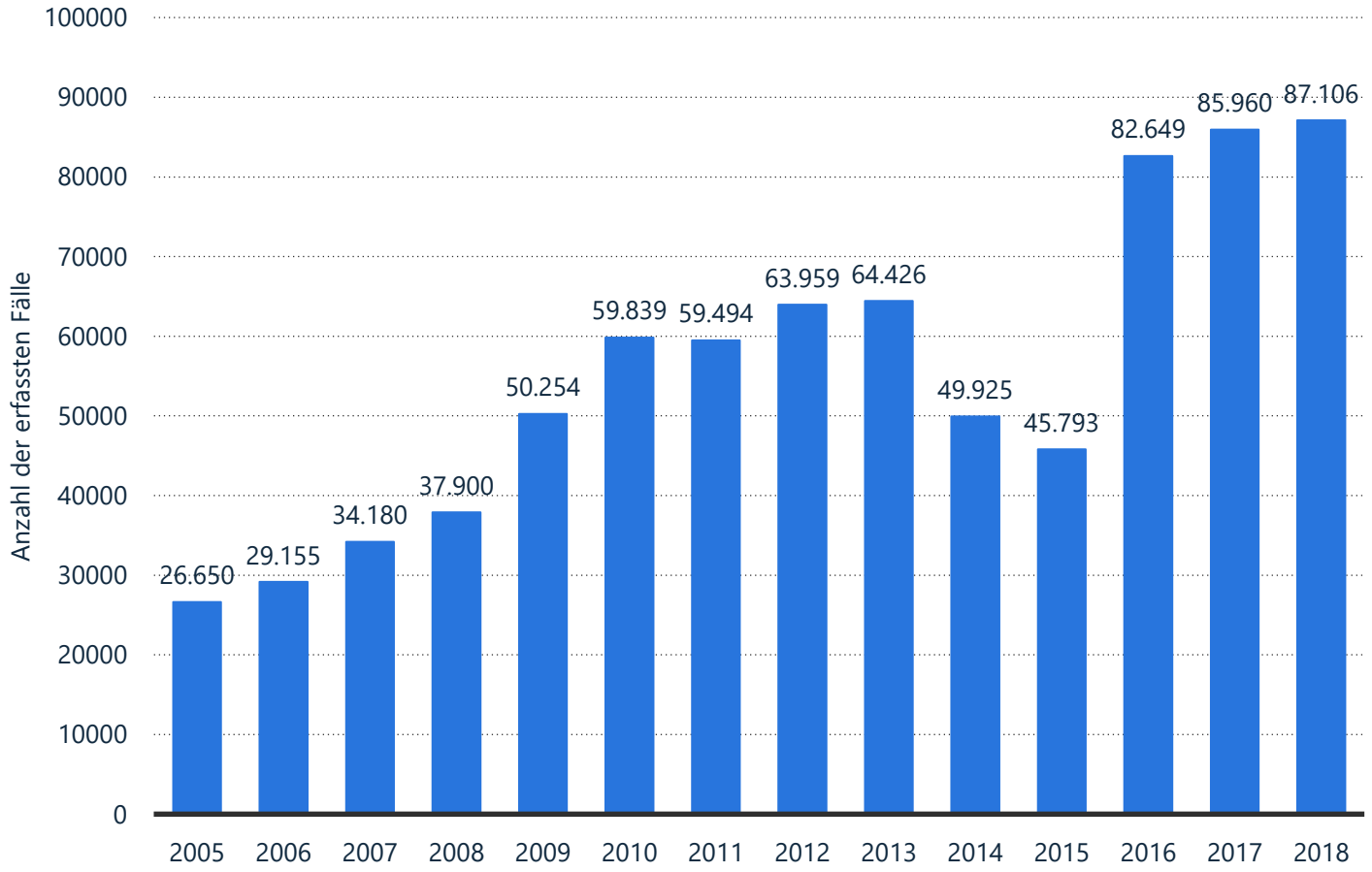


Quelle: Allianz für Cyber-Sicherheit | Cyber-Sicherheits-Umfrage 2018

Ausmaß potentieller Schäden – Aktuelle Situation

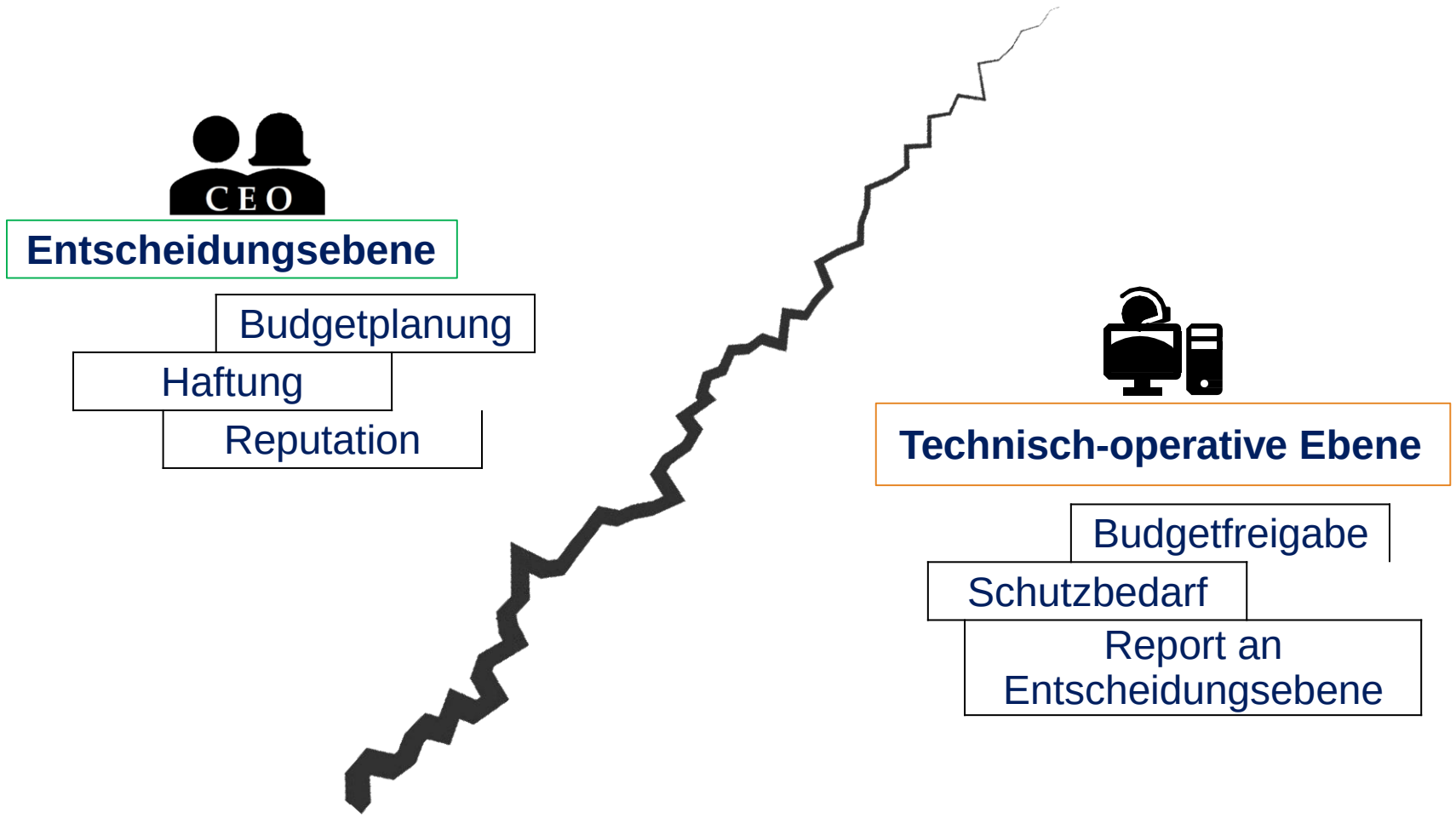
DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

Polizeilich erfasste Fälle von Cyberkriminalität in Deutschland bis 2018



Quelle: Statista - Bundeskriminalamt

Ausmaß potentieller Schäden – Aktuelle Situation



Ausmaß potentieller Schäden – Aktuelle Situation

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

- Der Grad der Vernetzung sowie die IT-Abhängigkeit von Unternehmen und damit das Schadenspotenzial nimmt immer weiter zu .
- Eine vollständige Vermeidung oder Verhinderung von Angriffen ist in der Praxis jedoch nicht möglich.
- Aus diesem Grund gilt es das potentielle Schadensausmaß auf ein akzeptables Maß zu reduzieren.
- Die technologischen Entwicklungen unserer Zeit sorgen für eine große Dynamik:
  - Qualität von Cyber-Angriffen nimmt stetig zu.

Um den heutigen Gefahren angemessen entgegenzuwirken,
gilt es die Informationssicherheit von Beginn an mit zu berücksichtigen.

Ausmaß potentieller Schäden – Schadensszenarien

Der Schaden, der von einer Verletzung der Grundwerte ausgehen kann, kann sich auf verschiedene Schadensszenarien beziehen …

- Verstöße gegen Gesetze, Vorschriften oder Verträge,
- Beeinträchtigungen des informationellen Selbstbestimmungsrechts,
- Beeinträchtigungen der persönlichen Unversehrtheit,
- Beeinträchtigungen der Aufgabenerfüllung,
- negative Innen- oder Außenwirkung oder
- finanzielle Auswirkungen.

Beispiel: Justus-Liebig-Universität Gießen (JLU)

- Am 8. Dezember 2019 wurde ein Hacker-Angriff entdeckt und die Admins der Universität fuhren alle Server runter.
- Eingesetzte Schadsoftware war wahrscheinlich Emotet in Kombination mit der Ransomware Ryuk.
- Erst am 6. Januar 2020 konnte die Lehrplattform Stud.IP wieder online gehen.
- Zu diesem Zeitpunkt war aber immer noch kein normaler Lehrbetrieb möglich und die Reparaturarbeiten noch nicht komplett abgeschlossen.

Fazit: Schadsoftware kann eine Universität wochenlang größtenteils in den Offline-Modus versetzen!

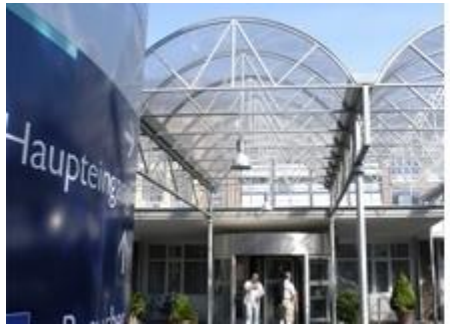
Beispiel: Stadt Frankfurt

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

- Ein Stadt-Mitarbeiter erhält im Dezember 2019 eine sehr gut getarnte E-Mail mit der Schadsoftware Emotet.
- Die Sicherheitssysteme haben Alarm geschlagen, dennoch wurden sicherheitshalber alle Systeme heruntergefahren und der Vorfall untersucht.
- Die Stadt Frankfurt war einen Tag nur telefonisch zu erreichen.
- Die meisten Dienstleistungen für die Bürger konnten ohne Computer nicht erbracht werden.

Beispiel: Lukaskrankenhaus Neuss

- Ein Computervirus legte 2016 das städtische Lukaskrankenhaus in Neuss lahm.
- Alle IT-Systeme der 540-Betten-Klinik mussten heruntergefahren werden.
- Es konnte noch vereinzelt ausgedruckt werden. Ansonsten lief nur das Faxgerät und Befunde wurden über Boten übermittelt.
- Circa 15 Prozent der Operationen konnten nicht stattfinden.



Rheinland Klinikum
Neuss Lukaskrankenhaus

Schwachstellen identifizieren

Schwachstellen identifizieren - Definition

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

Bedrohung

Eine Bedrohung ist ein Umstand, der die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen beeinträchtigen kann, wodurch dem Benutzer der Informationen ein Schaden entstehen kann.

Beispiele für Bedrohungen sind höhere Gewalt, menschliche Fehlhandlungen, technisches Versagen oder vorsätzliche Handlungen.

Eine Bedrohung wird erst durch eine vorhandene Schwachstelle zur Gefährdung für ein Objekt.

Beispielhafte Bedrohung: Verschlüsselungstrojaner

Schwachstellen identifizieren - Definition

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

Schwachstelle

Eine Schwachstelle ist ein sicherheitsrelevanter Fehler eines IT-Systems, oder organisatorische Fehler in Institutionen.

Ursachen können in der Konzeption, den verwendeten Algorithmen, der Implementation, der Konfiguration, dem Betrieb sowie der Organisation liegen.

Eine Schwachstelle kann dazu führen, dass eine Bedrohung wirksam wird und ein System geschädigt wird.

Erst durch eine Schwachstelle wird ein System anfällig für Bedrohungen.

Beispielhafte Schwachstelle: Kein aktueller Virenschutz

Schwachstellen identifizieren - Definition

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

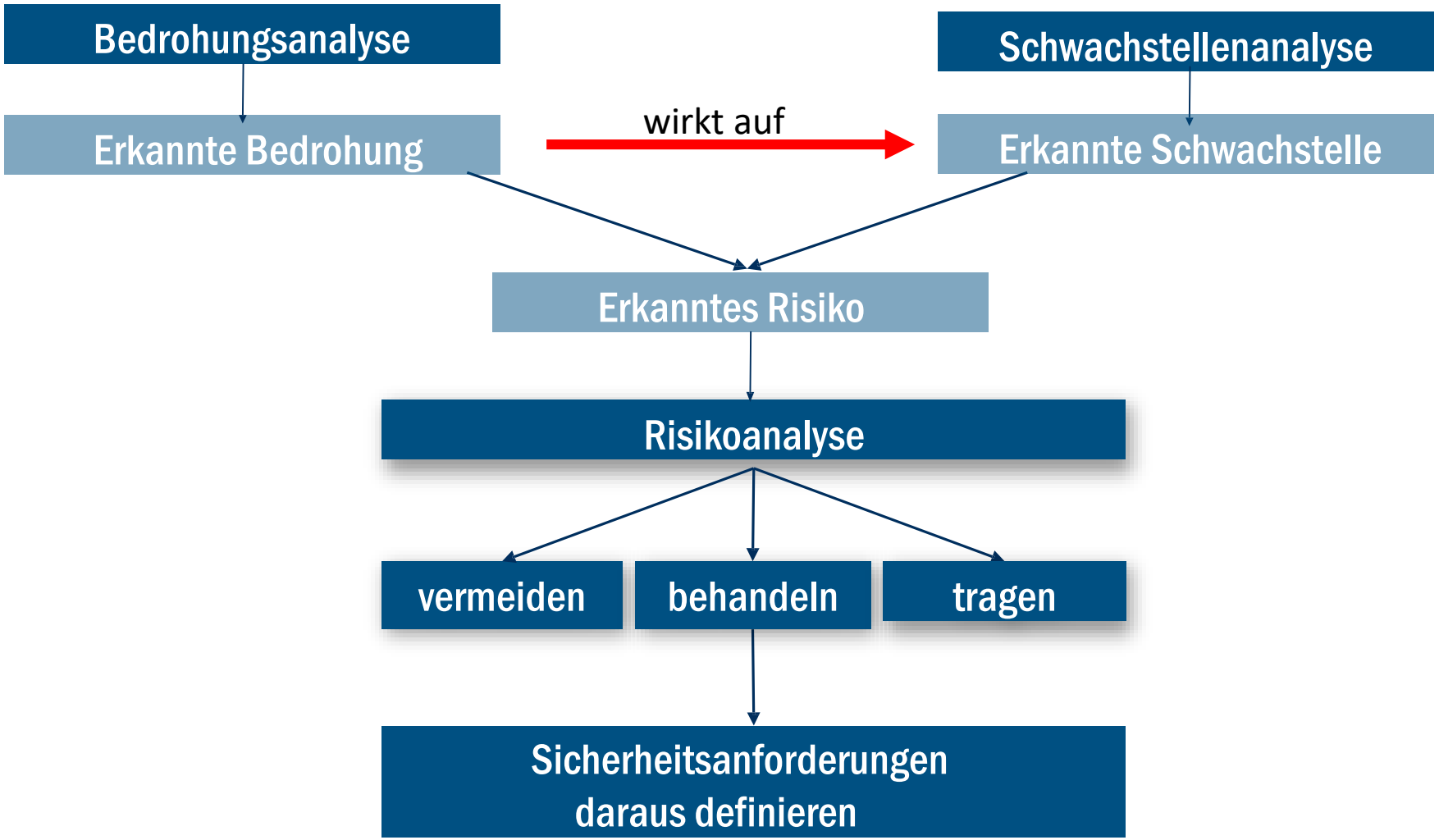
Risiko

Von einem Risiko spricht man, wenn eine Bedrohung (Verschlüsselungstrojaner) eine Schwachstelle (kein Virenschutz) ausnutzt.

Nur dann entsteht ein Risiko, nämlich **Verschlüsselung der Dateien.**

Die schwere des Risikos errechnet sich aus der Häufigkeit, mit der ein Schaden auftritt und dem Ausmaß dieses Schadens.

Schwachstellen identifizieren - Definition



Schwachstellen identifizieren - Beispiele

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

Typische Schwachstellen (Auszüge):

- Ungepachte Systeme
- Fehlende organisatorische Reglungen
- Unzureichende Systemabsicherung
- Menschliche Fehlhandlung
- Keine Kennzahlen (KPI - Key Performance Indicator)

Da die eingesetzten IT-Komponenten immer komplexer werden, grundsätzlich angreifbar sind und Schwachstellen enthalten können, ist es essenziell auf entdeckte Schwachstellen und Angriffe planvoll, systematisch und zeitnah zu reagieren.

Schwachstellen identifizieren – Methoden

Um Informationssicherheitsrisiken zu minimieren und für Informationssicherheit zu sorgen, sind sowohl technische als auch organisatorische Maßnahmen zu ergreifen.

Prozess-/Risiko-/Schwachstellenanalyse

1. Identifizierung der kritischen Geschäftsprozesse und zugehörigen Assets.
2. Bestimmung der relevanten Schwachstellen.
3. Einschätzung der Eintrittswahrscheinlichkeit, zur Ausnutzung einer Schwachstelle.
4. Einschätzung des potentiellen Schadensausmaß.

Schwachstellen identifizieren – Methoden

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

Einholen von Schwachstellenmeldungen

- Durch Anschluss an Cert-Stellen Informationen über aktuelle Schwachstellenmeldungen erhalten.

- Geeignete Kanäle (z.B.)
  - Bundesamt für Sicherheit in der Informationstechnik (BSI)
  - Hersteller
  - CERT-Stellen (DFN-CERT, Bürger-CERT, CERT-Bund …)

Schwachstellen identifizieren – Methoden

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

Technischer Schwachstellen-Scan:

- Widerstandsfähigkeit der internen IT-Umgebung gegenüber externen Angreifern prüfen.
- Netzwerke und Geräte werden auf Schwachstellen untersucht.
- Ergebnis der Analyse ist die Identifizierung potenzielle Einfallstore.

Beim technischen Schwachstellen-Scan (bsp. Greenbone) werden die Schwachstellen lediglich identifiziert.

Geöffnete Tür wird gefunden, es wird aber nicht hindurchgegangen.

Schwachstellen identifizieren – Methoden

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

Penetrationstest:

- Umfassenden Sicherheitstest einzelner Rechner oder Netzwerke jeglicher Größe.
- Prüfung der Sicherheit mit Mitteln und Methoden, die ein Angreifer (Hacker) anwenden würde.
- Ermittelt die Empfindlichkeit des zu testenden Systems gegen derartige Angriffe.

Beim Penetrationstest werden die Schwachstellen im Gegensatz zum Schwachstellenscan nicht nur identifiziert sondern auch ausgenutzt.

Geöffnete Tür wird gefunden, und wird versucht hindurch zu gehen.

Schwachstellen identifizieren – Methoden

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

Security Audit auf Basis der ISO 27001 (Intern/Extern):

- Prüfung technischer und organisatorischer Vorgaben bspw.:
  - Clean-Desk
  - Zutrittskontrolle
  - Zugriffskontrolle
  - Besuchermanagement
  - Netzwerkmanagement
  - Physische Sicherheit
  - Lieferantensteuerung
  - Betriebssicherheit
  - Kommunikationssicherheit

Ziel: Identifizierung möglicher Risiken und Festlegung geeigneter Maßnahmen.

Mobile Geräte

Mobile Geräte - Einleitung

Viele Aktivitäten im Geschäftsleben laufen über mobile Geräte wie

- **Laptops**
- **Smartphones**
- **Tablets**

Die mobilen Geräte ermöglichen uns an jedem Ort der Welt zu arbeiten und beispielsweise schnell auf E-Mails zu reagieren.

Das geschäftliche E-Mail-Konto ruft heutzutage nahezu jeder mit einem Smartphone ab.

Mobile Geräte - Gefahren

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

Mobile Geräte sind im Vergleich zu einem stationären PC-Arbeitsplatz zusätzlichen Gefahren ausgesetzt:

- Mobile Geräte können leicht gestohlen werden oder verloren gehen.
- Im mobilen Einsatz können Angreifer oder Fremde möglicherweise vertrauliche Informationen vom Bildschirm ablesen oder bei Gesprächen mithören.
- In offenen bzw. fremden WLANs droht die Gefahr, dass ein Angreifer den Datenverkehr „mithören“ oder manipulieren kann. Dies ist vor allem bei unverschlüsseltem Datenverkehr kritisch.
- Smartphones und Tablets bieten durch App-Downloads eine zusätzliche Quelle für Gefährdungen.
- Kameras und Mikrofone können zusätzliche Angriffspunkte für Spionage sein.
- Cloud-Nutzung kann für datenschutzrechtliche Probleme sorgen.

Schutzmaßnahme - Verschlüsslung

Die Festplatten mobiler Geräte sollten verschlüsselt sein

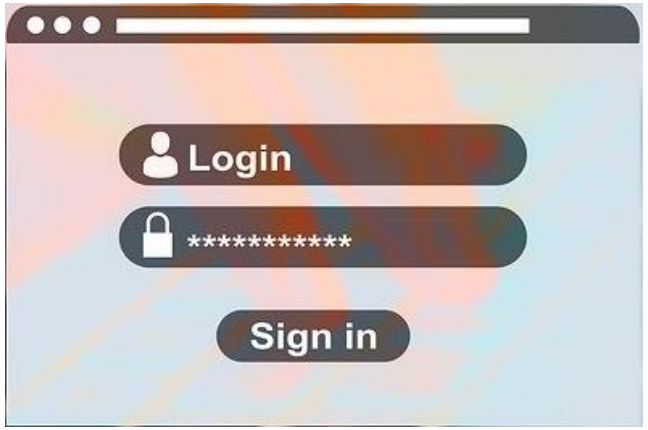
(z.B. mittels BitLocker bei Windows-Geräten)

- Die Verschlüsslung von Festplatten ist eine sehr gute Absicherung für den Fall, wenn ein mobiles Gerät in die Hände von Unbefugten gelangt ist (Diebstahl oder Verlust).
- Dank der Verschlüsslung kann die Festplatte durch den Unbefugten nicht einfach ausgelesen werden.

Im Optimalfall werden Daten zudem zentral auf einem gut gesicherten Server gehalten und nicht auf dem mobilen Gerät

Schutzmaßnahme - Authentifizierung / Passwörter

Eine starke Authentifizierung ist auch bei mobilen Geräten essenziell



- Es müssen starke Passwörter (mind. 10 Zeichen, Groß- und Kleinbuchstaben, Zahlen, Sonderzeichen) verwendet werden.
- Biometrische Authentifizierungsmethoden (Fingerabdruck / Iris) sollten wenn möglich genutzt werden.
- Zwei-Faktor-Authentisierung (2FA) sollte wenn möglich genutzt werden (z.B. Sicherheits-Token, Kurzzeitkennwortgenerator, Einmalpasswort per SMS/E-Mail).
- Für verschiedene Geräte sollten unterschiedliche Passwörter genutzt werden.

Schutzmaßnahme - Achtsam- und Aufmerksamkeit

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

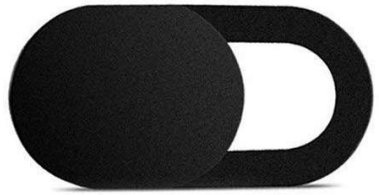
Achtsam- und Aufmerksamkeit ist elementar für die Sicherheit mobiler Geräte

- Mobile Geräte sollten nicht unbeobachtet oder offen liegen gelassen werden (z.B. im Auto).
- Verschlussmöglichkeiten (z.B. Safe, Schrank) sollten genutzt werden.
- Mobile Geräte sollten bei Nichtnutzung immer gesperrt sein.
- Es ist immer sinnvoll die Umgebung zu beobachten (Neugierige Blicke oder Zuhörer bei Gesprächen).
- Lieber einmal mehr nachschauen, ob man das mobile Gerät bei sich hat oder es sicher gelagert bzw. gesperrt ist.

Schutzmaßnahme - Schutzabdeckungen

Schutzabdeckungen bieten zusätzlichen Schutz für mobile Geräte

- Blickschutzfolien schützen vor unerwünschten Blicken aus diversen Blickwinkeln.
- Schutzabdeckungen für Kameralinsen verhindern Spionage über die Kamera von mobilen Geräten.
- Bei Laptops ist zusätzlich auch die hardwareseitige Deaktivierung von Kamera und Mikrofon eine gute Option zur Verhinderung von Spionage.



Bring Your Own Device (BYOD)

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

Bring Your Own Device (BYOD) ist die Bezeichnung dafür, private mobile Endgeräte wie Laptops, Tablets oder Smartphones in die Netzwerke von Organisationen zu integrieren

- Private Geräte können ein Sicherheitsrisiko darstellen: Daten werden auf nicht oder teilweise kontrollierbaren fremden Geräten verarbeitet.
- Private Geräte, welche sich im internen Netzwerk bewegen, können stören oder ausspionieren.
- BYOD läuft der Strategie zur Vereinheitlichung der IT-Infrastruktur entgegen.
- Komplexität und Betriebsaufwand steigen durch BYOD.
- BYOD kann aus Datenschutzsicht problematisch sein.
- Strikte Trennung von privaten und beruflichen Daten muss gewährleistet sein und dies macht BYOD oft zu einem Problem.

BYOD sollte untersagt oder sehr streng geregelt sein.

Schutzmaßnahme - Mobile-Device-Management (MDM)

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

Mobile-Device-Management (MDM) steht für die zentralisierte Verwaltung von mobilen Geräten durch Administratoren mit Hilfe von Software und Hardware

- Zentrales Management verschiedenster Mobilgeräte
- u.a. Übersicht der IMEI-Nummern, Seriennummern, Zuordnung der Geräte zu Mitarbeitern
- Trennung von Unternehmens- und Privatdaten (DSGVO-konforme Trennung möglich)
- Reduzierter Kosten- und Administrationsaufwand
- Sicherheitsstandards der Organisation können gewahrt werden
- Zentrale Verwaltung von Zugangsberechtigungen ins Firmennetzwerk (z.B. WLAN und VPN)

Gefahren durch soziale Netzwerke

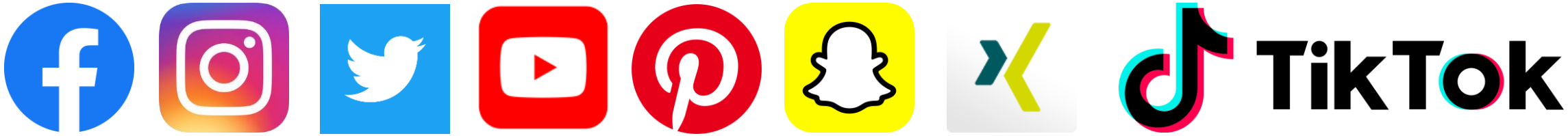
Soziale Netzwerke - Allgemeines

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

Soziale Netzwerke…

- erfreuen sich weltweit einer sehr großen Nutzeranzahl (3,48 Milliarden Stand Januar 2019, Statista)
- sprechen alle Altersgruppen an
- werden durch Nutzer oft mehrmals am Tag genutzt
- können über Smartphone-Apps auch unterwegs jederzeit verwendet werden
- sind ohne direkte Bezahlung von Geld nutzbar

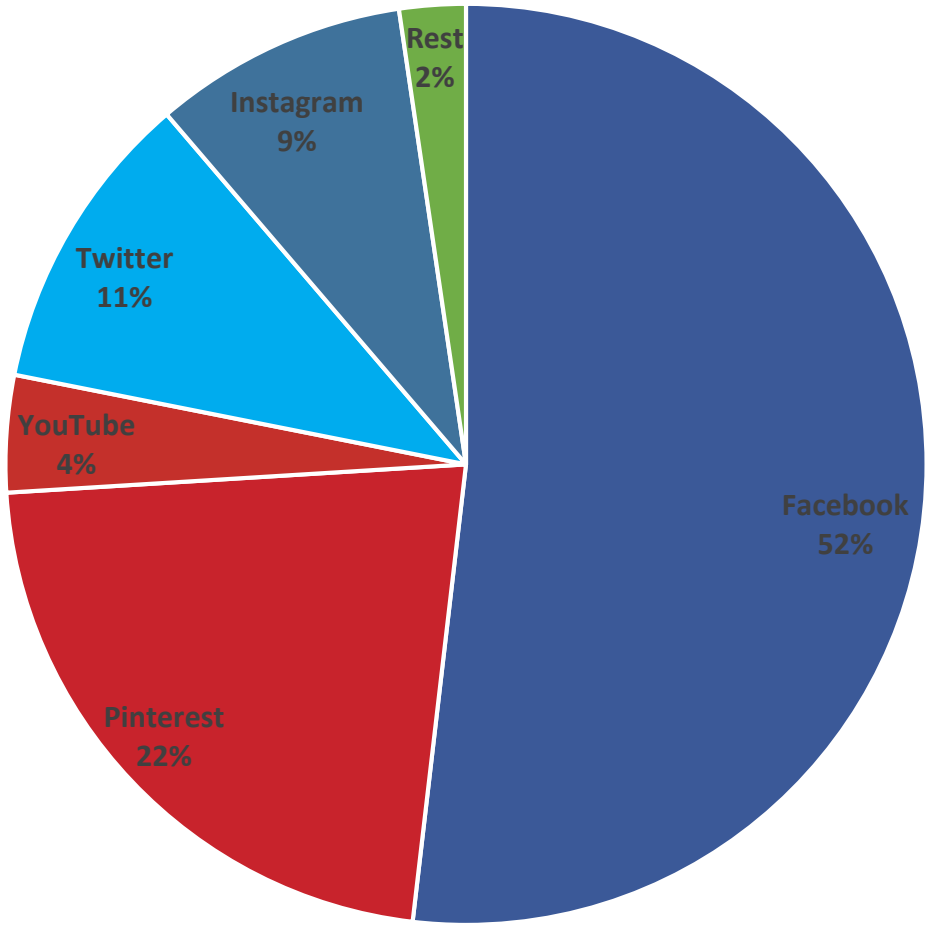
Beliebte Netzwerke in Deutschland (Auszug):



Soziale Netzwerke - Marktanteile in Deutschland

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

Marktanteile von sozialen Netzwerken in Deutschland (Januar 2020, Statista)



Soziale Netzwerke - Kennzahlen aus Deutschland

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

- durchschnittliche tägliche Verweildauer: **64 Minuten**
- Anteil der 16- bis 24-Jährigen: **89%**
- Anteil der Nutzer mit hohem Bildungsstand: **52%**
- Anzahl der mobilen Nutzer: **30 Millionen**
- regelmäßige mobile Nutzung: **34,9%**

Statistiken aus diversen Untersuchungen von Statista

Soziale Netzwerke - Problematiken

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

Betreiber von sozialen Netzwerken sitzen meistens in Drittländern (z.B. USA), haben ein schlechteres Datenschutzniveau und kommen Ihren rechtlichen Verantwortungen meist nur sehr zögerlich und widerwillig hinterher

- Oftmals leichtfertiger Umgang mit persönlichen Daten.
- Umsetzung von europäischen Standards oft erst kurz vor oder nach Geldstrafen bzw. nach großem Druck durch die Öffentlichkeit und drohendem Imageverlust.
- Nutzertracking und Werbung wird lockerer gesehen.

Soziale Netzwerke - Problematiken

Soziale Netzwerke haben immer das Ziel Umsatz zu erzielen

- Nutzer bezahlen nicht mit Geld, sondern mit Ihren Daten (Stammdaten und persönliche Daten, Fotos/Videos, Likes, Interessen, Nutzungsverhalten).
- Nutzer erhalten interessensbezogene und perfekt zugeschnittene Werbung.
- Potentielle Weitergabe von Daten an Dritte.

Die Nutzung eines sozialen Netzwerks ist also nicht wirklich kostenlos:

Nutzer zahlen mit den eigenen Daten!

Soziale Netzwerke - Problematiken

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

Die Oberhand über die Daten von Nutzern behält zumeist das soziale Netzwerk

- Selbst nach Löschung von Daten oder Profilen wissen Nutzer nicht, ob das soziale Netzwerk noch eine Datensicherung hat.
- Vieles spricht für eine dauerhafte Speicherung im Hintergrund, denn oftmals kann man bei sozialen Netzwerken sein Profil nur deaktivieren statt löschen und später nach Wunsch wieder reaktivieren.
- In Drittländern wie den USA haben auch Regierungsorganisationen (z.B. FBI oder NSA) leichten Zugriff auf Nutzerdaten.

Drittanbieter-Apps (vor allem Facebook) können für Datenskandale sorgen

- Über sogenannte Programmierschnittstellen (APIs) können auch Dritte Daten sammeln (z.B. Umfrageapps auf Facebook).

„Zentral für „eines der größten Datenlecks in der Geschichte von Facebook“ ist die App eines Drittanbieters, mit der Facebook-Nutzer einen Persönlichkeitstest machen konnten. Die Anwendung sammelte allerdings nicht nur Informationen über die etwa 270.000 Menschen, die sie bewusst genutzt haben, sondern auch über deren Facebook-Kontakte.

Nachdem anfänglich von rund 50 Millionen Betroffenen die Rede war, musste Facebook inzwischen eingestehen, dass wahrscheinlich die Daten von 87 Millionen Nutzern abgezogen wurden.“

Soziale Netzwerke - Gefahren

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

Kontrollverlust über die eigenen Daten („Einmal im Netz, immer im Netz“)

- Nutzerdaten sind teilweise dauerhaft auf den Servern von sozialen Netzwerken gespeichert.
- Die eigenen Daten können durch andere Nutzer vervielfältigt und abgespeichert werden.
- Öffentliche Profile können durch Suchmaschinen aufgefunden, ausgelesen und vervielfältigt werden → vollkommen automatisch.

Man muss sich bewusst sein:

Was einmal ins Internet gestellt wird, könnte für immer im Internet bleiben

Soziale Netzwerke - Gefahren

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

Betrug mit den eigenen Daten

- Social Engineering / Social Hacking
  - Soziale Manipulation durch Nutzung von auf sozialen Profilen preisgegebenen Daten.
  - Beispiel: Erlangen von sensiblen Daten oder Auslösen von Aktionen durch die Kenntnis von privaten Daten.
  - Ein Angreifer hat die Möglichkeit mit den preisgegebenen Daten zu arbeiten und andere Personen zu manipulieren.

- Fake-Profile mit den eigenen Daten, Bildern und Videos
  - Cybermobbing
  - Ein Angreifer hat die Möglichkeit sich als das betroffene Opfer auszugeben.

Soziale Netzwerke - Gefahren

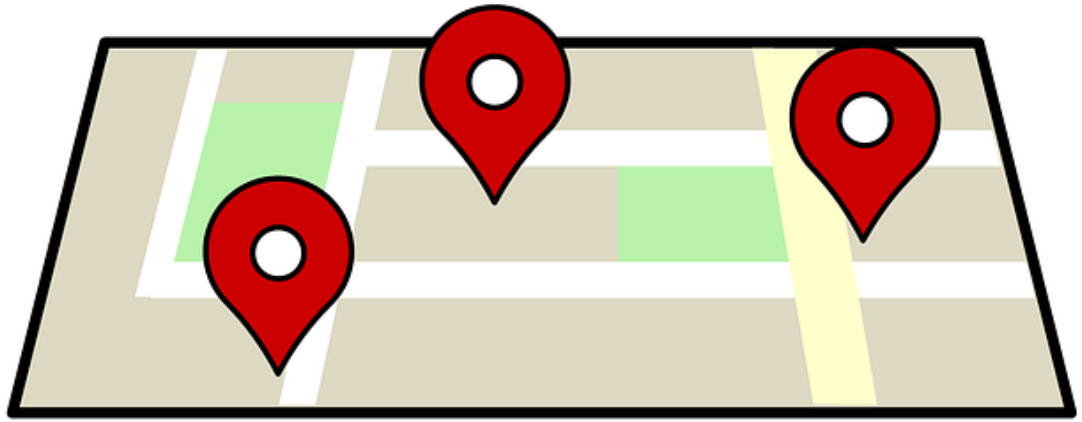
DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

Unerwünschtes Tracking auf Websites über Like-Buttons und anderen sozialen Plugins

- Websites, können Plugins von sozialen Netzwerken eingebaut haben (z.B. Like-Buttons oder Timeline-Feeds) → Ist ein Nutzer beim sozialen Netzwerk eingeloggt, weiß das soziale Netzwerk auf welchen Websites man unterwegs war.
- Dadurch ist eine noch bessere Optimierung von Werbeanzeigen möglich.

Tracking des Standortes und daraus entstehende Bewegungsprofile

- Gerade bei der mobilen Nutzung von sozialen Netzwerken und einer permanenten Standort-Freigaben können Bewegungsprofile von Nutzern erstellt werden.
- Das soziale Netzwerk weiß somit genau wo Sie sich aufhalten und kann Werbemaßnahmen optimieren oder die Daten im schlimmsten Fall weitergeben.



DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

Unerwünschte Werbung

- Werbung versteckt zwischen normalen Beiträgen / Posts.
- Perfekt abgestimmte Werbung nach Interessen oder Produkten, die man kürzlich auf anderen Websites gesucht hat.
- Werbetreibende können nach Alter, Geschlecht, Land, Wohnort, Likes und vielen weiteren Merkmalen die Werbeanzeigen perfekt abstimmen.

Soziale Netzwerke - Neu im Geschäft: TikTok

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

TikTok ist ein derzeit sehr angesagtes chinesisches Videoportal für die Lippensynchronisation von Musikvideos und anderen kurzen Videos

TikTok

- Sehr junge Nutzerzielgruppe, oftmals Teenager
- Videos sind ohne Anmeldung zu sehen (Kommentare erst nach Anmeldung)
- Nach Anmeldung Kommentar- und Kontaktmöglichkeit
- Zensur politischer, religiöser und unternehmenskritischer Themen sowie Blockierung von homosexuellen Inhalten und deren Befürwortung
- Datenschutz und Jugendschutz stark verbesserungswürdig
- Sexismus und Cyber-Mobbing sind an der Tagesordnung

Soziale Netzwerke - Tipps

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

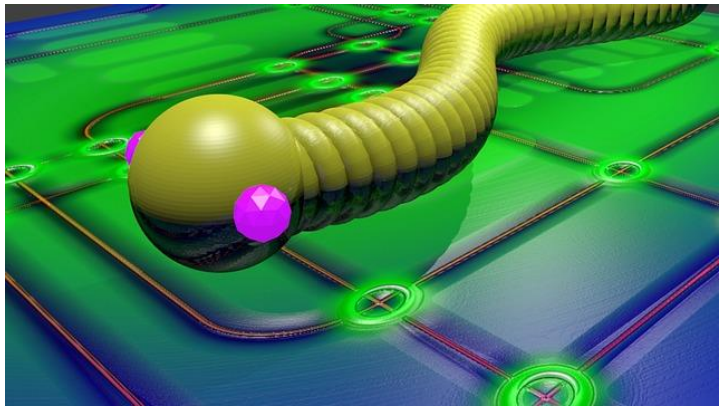
- ✓ Geben Sie so wenig wie möglich Daten an und laden Sie so wenig wie möglich Fotos und Videos hoch.
- ✓ Nutzen Sie immer die bestmöglichen Datenschutzeinstellungen der jeweiligen Plattform und lassen Sie nur engste Kontakte auf Ihre Daten zugreifen.
- ✓ Nutzen Sie bessere Alternativen, wenn vorhanden → z.B. Threema statt WhatsApp.
- ✓ Deaktivieren Sie Standort-Freigaben in Apps und Browser.
- ✓ Ein Abmelden bzw. Ausloggen bei der jeweiligen Plattform verhindert das Tracking beim surfen auf anderen Websites.

Schadsoftware wie Viren, Würmer und Trojaner

Schadsoftware - Einleitung

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

Als Schadsoftware oder Malware bezeichnet man Computerprogramme, die entwickelt wurden, um unerwünschte und meist schädliche Funktionen auszuführen



Computervirus

- Schreibt Kopien von sich selbst in Programme, Dokumente oder Datenträger.

Computerwurm

- Verbreitet sich direkt über Netze wie das Internet und versucht, in andere Computer einzudringen.

Trojanisches Pferd / Trojaner

- Werden verbreitet um einen sogenannten Backdoor zu schaffen, um Zugriff auf einen infizierten Computer zu erlangen und diesen z.B. als Spamverteiler oder für Denial-of-Service-Angriffe zu missbrauchen.

Schadsoftware - Einleitung

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

Ransomware

- Blockiert den Zugriff auf das Betriebssystem bzw. verschlüsselt potenziell wichtige Dateien und fordert den Benutzer zur Zahlung von Lösegeld auf.

Spyware und Adware

- Forschen den Computer und das Nutzerverhalten aus und senden die Daten an den Hersteller oder andere Quellen, um diese entweder zu verkaufen oder um gezielt Werbung zu platzieren.

Scareware

- Ist darauf angelegt, den Benutzer zu verunsichern (z.B. angeblicher Virenbefall) und ihn dazu zu verleiten, schädliche Software zu installieren oder für ein unnützes Produkt zu bezahlen.

Keylogger

- Programme die dazu verwendet werden, die Eingaben (z.B. Benutzernamen und Passwörter) des Benutzers an der Tastatur eines Computers zu protokollieren und einem Dritten bereitzustellen.

Schadsoftware - Beispiel: Ransomware „WannaCry“

- Verschlüsselt Benutzerdateien eines Computers.
- Für die Entschlüsselung muss der Nutzer eine vorgegebene Geldsumme per Bitcoin überweisen.
- Nach abgelaufener Frist droht das Programm mit Datenverlust.
- Des Weiteren versucht das Schadprogramm weitere Windows-Rechner zu infizieren.

Schadsoftware - Bedrohungslage

Remshalden im Rems-Murr-Kreis

Computer

21.10.2019 - 16:38 Uhr

Ein aggressives Computervirus be
dpa/Oliver Berg

Die Remshaldener Verv
Schadsoftware gelangt
System – was Bürger je

Stand: 10.09.2019 16:54 Uhr - Lesezeit: ca.3 Min.

Trojaner: Neustadt bleibt bis Freitag offline

Bei der Schadsoftware handelt es sich na
Angaben der Stadt um einen Emotet-Troj
(Themenbild)

Trojaner befallen worden. "Das w
können normale Virenprogramm
Was das Ziel der Attacke war, dazu wollten sich die Stadt und das
Landeskriminalamt Niedersachsen mit Verweis auf die laufenden Ermittlungen
nicht äußern.

…t schlägt wieder zu

r Trojaner befällt in

Trojaner-Attacken auf Universitäten, Behörden und Krankenhäuser

Emotet hat Deutschland weiterhin im Griff

11.02.20 | Autor: Susanne Ehneß

Emotet hat in den letzten Monaten immer wieder Stadtverwaltungen, Krankenhäuser und Universitäten lahmgelegt. Der Trojaner zählt laut BSI aktuell zu den gefährlichsten Schadprogrammen.

Das Kammergericht Berlin, die Universität Gießen, das Klinikum Fürth sowie die Städte Frankfurt und Bad Homburg – sie alle wurden Opfer der Schadsoftware Emotet. Der Trojaner wurde erstmals 2014 identifiziert und ist nach wie vor aktiv.

…e Opfer.

Schadsoftware - Schutz durch Antivirensoftware

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

Antivirensoftware ist nur eine Grundabsicherung gegen Schadsoftware

- Die tägliche Flut neuester unterschiedlichster Varianten von Schadsoftware macht es den Herstellern von Antivirensoftware schwer hinterherzukommen.

- Antivirensoftware bietet meistens nur Schutz gegen altbekannte Schadsoftware.

Ein Antivirensoftware bietet also in der Regel keinen Schutz gegen neue Schadsoftware!

Schadsoftware - Schutz durch Sensibilisierung

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

Ein sensibilisierter und aufmerksamer Beschäftigter ist das wirksamste Mittel gegen Schadsoftware

Im Optimalfall erkennt der sensibilisierte Beschäftigte…

- betrügerische E-Mails und Websites
- manipulierte Links
- ungewohntes Verhalten von den täglich benutzten Systemen
- unverschlüsselte Websites
- gefährliche Dateiendungen

Schadsoftware - Sonstige mögliche Schutzmaßnahmen

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

- Über Windows Gruppenrichtlinien können gewisse potentielle Gefährdungen (z.B. Excel- und Word-Makros) blockiert bzw. deaktiviert werden.
- Benutzer sollten nicht mit einem administrativen Account unterwegs sein.
- Blockieren von gefährlichen Dateiendungen bei Dateianhängen in E-Mails.
- Blockieren von aktiven Inhalten auf Websites.
- Richtlinien und Dienstanweisungen zur Informationssicherheit für Beschäftigte.

Ein Informationssicherheitsbeauftragter (ISB) …

… übernimmt die Steuerung und Überwachung des Informationssicherheitsprozesses und die Sensibilisierung von Beschäftigten.

Nötige Schritte zur Umsetzung eines ISMS

Vorteile eines ISMS

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

Risikomanagement

- Gezielte Risikosteuerung
- Transparenz über die Risikosituation
- Erhöhung des Unternehmenswertes durch eine Verringerung von risikobedingten Schwankungen

Kosten Senkend

- Optimierte Abstimmung zwischen Fachbereichen und IT
- Steigerung der Produktivität durch Effizienz
- Prozessoptimierung

Cyber-Abwehr

- Systematische Steigerung des IT-Sicherheitsniveaus auf allen Ebenen
- Vorbereitung auf die Abwehr von Cyber-Angriffen u. sonstigen Notfällen
- Sicherer Betrieb des Kerngeschäfts

Compliance

- Imagegewinn und Wettbewerbsvorteil
- Regelmäßige Überprüfung durch unabhängige Dritte
- Vorbereitung auf künftige regulatorische Anforderungen

ISO 27001 vs. BSI IT-Grundschutz

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

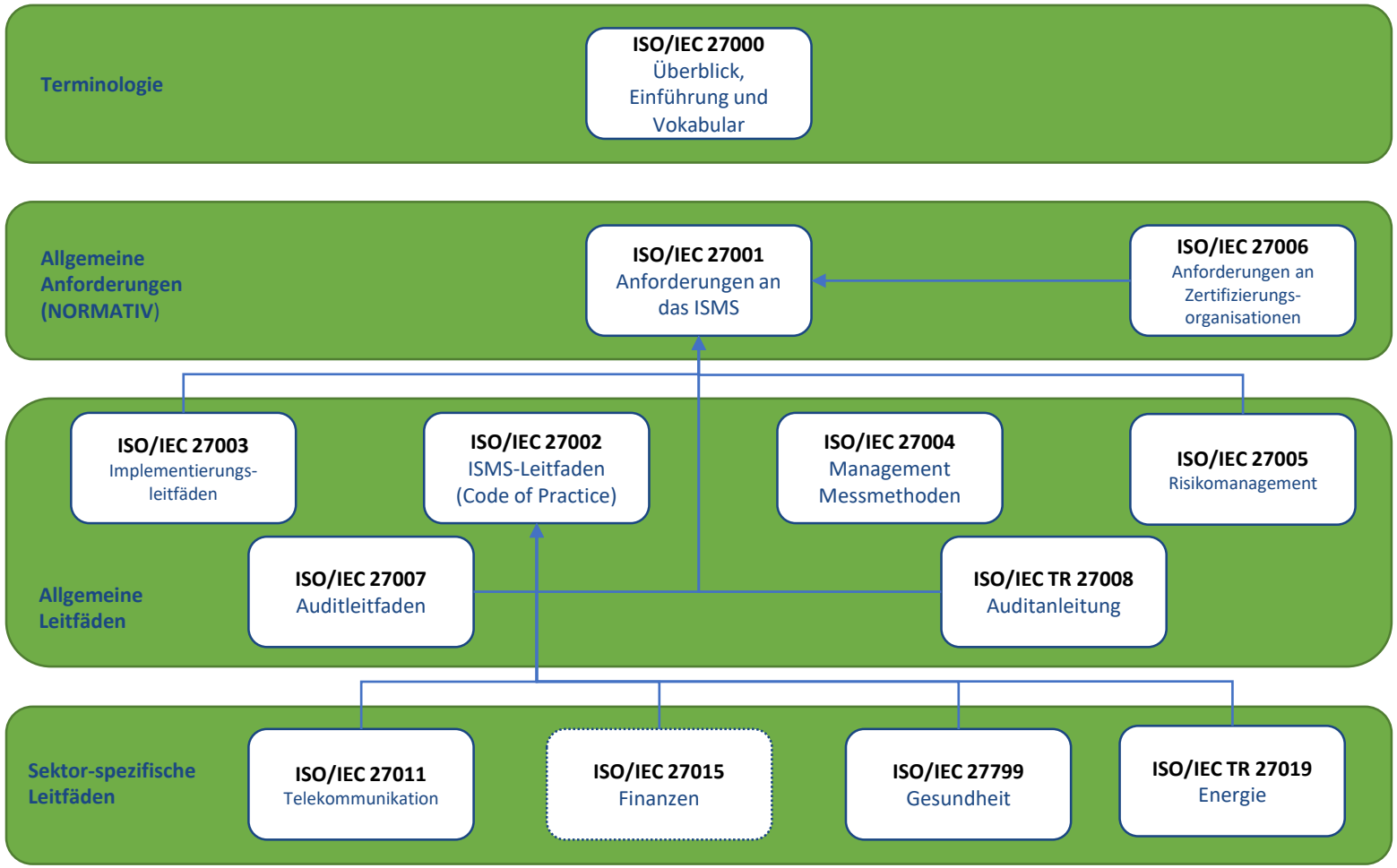
- Es gibt verschiedene Möglichkeiten ein ISMS aufzubauen und zertifizieren zu lassen.
- Die meist genutzten Grundlagen sind

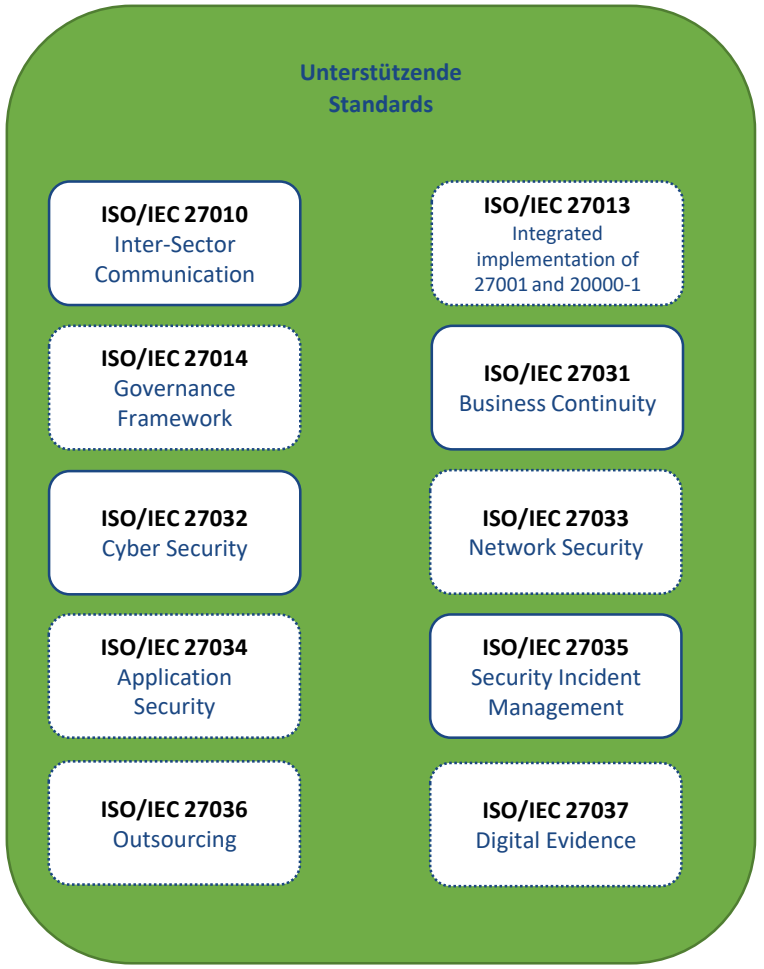
➢ISO 27001 auf Basis von IT-Grundschutz (nationaler Standard) – BSI.

➢ISO 27001 nativ (internationaler Standard)
in Deutschland zuständig „DAkkS - Deutsche Akkreditierungsstelle“.

ISO 27001

Normenübersicht (2700X)





BSI Standard 200 - X

BSI-Standard 200-1:	Managementsysteme für Informationssicherheit (ISMS)
BSI-Standard 200-2:	IT-Grundschutz-Methodik
BSI-Standard 200-3:	Risikomanagement
BSI-Standard 100-4:	Notfallmanagement (wird derzeit überarbeitet)

BSI Standard 200 - X

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

IT-Grundschutz-Kompendium (aktuell Februar 2020)

Das IT-Grundschutz-Kompendium enthält Prozess- und Systembausteine aus den folgenden Bereichen

- **ISMS**: Management von Informationssicherheit,
- **ORP**: Organisation und Personal,
- **CON**: Konzepte und Vorgehensweisen (z.B. Kryptokonzept, Softwareentwicklung),
- **OPS**: Betrieb (z. B. Schutz vor Schadprogrammen, Cloud-Computing) und
- **DER**: Detektion und Reaktion (Behandlung von Sicherheitsvorfällen, Notfallmanagement),
- **INF**: Infrastruktur (z. B. Gebäude, Rechenzentrum),
- **SYS**: IT-Systemen (z. B. Servern, Clients),
- **NET**: Netzen und Kommunikation (z. B. Netzarchitektur und -design),
- **APP**: Anwendungen (z. B. E-Mail und Browser) und
- **IND**: Industrieller IT (z. B. Betriebs- und Steuerungstechnik sowie Leitstand).

ISO 27001 vs. BSI IT-Grundschutz

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

ISO/IEC 27001	ISO 27001 auf Basis IT-Grundschutz
internationale Norm mit Flexibilität in der Umsetzung	detaillierte Vorgaben, strikt geführte Umsetzung
Geringerer Aufwand, vor allem für kleine und mittlere Unternehmen	Deutlich höherer Aufwand für Vorbereitung und Zertifizierung
International anerkannt	Höhere nationale Relevanz

Nötige Schritte zur Umsetzung eines ISMS (ISO/IEC 27001 nativ)

Mit einer erfolgreichen Zertifizierung ist der Prozess nicht abgeschlossen
– Nach der Zertifizierung ist vor der Zertifizierung

Schritt 1 - Definition des Geltungsbereich

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

- Ein ISMS kann **Unternehmensweit** aufgebaut werden oder nur **Teilbereiche** abdecken.
- Zunächst müssen die **Grenzen und Schnittstellen** des ISMS klar definiert werden.
- Dabei müssen die
  - **infrastrukturellen,**
  - **organisatorischen,**
  - **personellen und**
  - **technischen Komponenten** berücksichtigt werden.

Schritt 2 - Bestandsaufnahme und Bewertung

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

- Auf Basis des definierten Geltungsbereiches findet eine **umfangreiche Bestandsaufnahme** der IT-Infrastruktur sowie der vorhandenen Regularien, Verfahren und Dokumentation statt.

- Die Durchführung erfolgt anhand von **Interviews und Prüfungen**. Bei Bedarf findet eine **Begehung** der relevanten Gebäude und Räume statt, die sich im Geltungsbereich befinden.

- Es werden sowohl **technische Aspekte** wie auch **organisatorische Maßnahmen** erfasst um einen aussagekräftigen SOLL /IST Vergleich anfertigen zu können.

Schritt 3 - Managementstruktur definieren

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

- Ziel in Schritt 3 ist es die **übergreifenden Vorgaben** festzulegen und die entsprechenden Dokumente zu erstellen

- Die benötigten Dokumente sind beispielsweise:
  - Dokumentenlenkung
  - Richtlinie zum Risikomanagement
  - Richtlinie für interne Audits
  - Richtlinie für Korrektur- und Vorbeugemaßnahmen
  - ggf. weitere

Schritt 4 - Erstellung der Anwendbarkeitserklärung

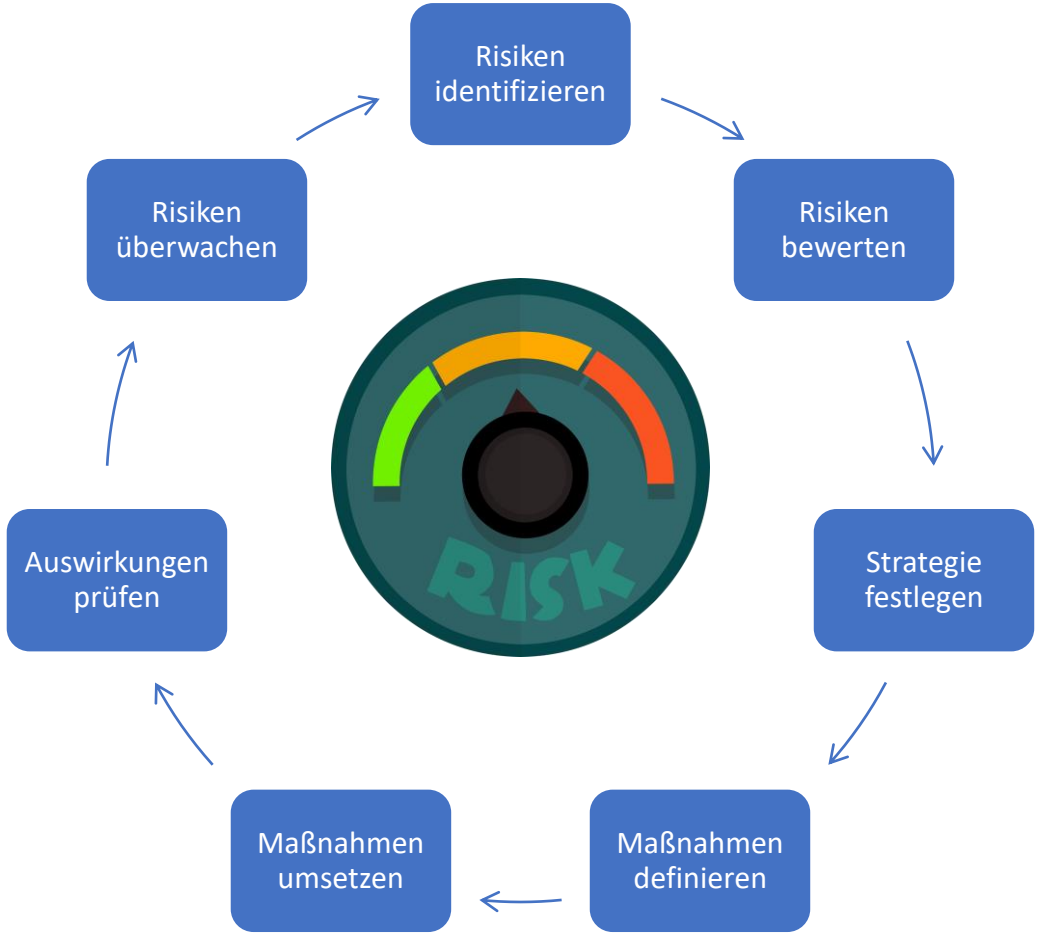
- Die Anwendbarkeitserklärung enthält alle 114 Maßnahmen aus dem Anhang A der DIN ISO/IEC 27001.

- Es gilt nun zu beurteilen welche Maßnahmen angewendet bzw. nicht angewendet werden.

- Ziel ist es die Maßnahmen anzuwenden um Risiken zu minimieren.

Schritt 5 - Risikomanagement

- Es gibt **verschiedene Herangehensweisen** ein Risikomanagement zu implementieren.
- Wichtig ist es eine Herangehensweise zu wählen, die **für Ihre Organisation passend** ist.
- Grundlegend haben beinhalten alle Herangehensweisen die **gleichen Schritte**, die sich in der Umsetzung aber unterscheiden.



Schritt 6 - Erstellung der Dokumentation

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

- Die Dokumentation der technischen und operativen Aspekte der DIN EN ISO/IEC 27001 ist i.d.R. die **quantitativ aufwändigste Aufgabe** innerhalb des gesamten Projektverlaufes

- Eine ordentliche Dokumentation sollte mindestens folgende Themen abdecken:
  - Patchmanagement
  - Backupmanagement
  - Konzept gegen Schadprogramme
  - Richtlinien Internetnutzung, Arbeitsplatz (Clean Desk)
  - Protokollierungsmanagement
  - Schulungs- und Sensibilisierungskonzept
  - Passwortrichtlinie
  - Zugangs- Zugriffs- und Zutrittskontrolle
  - Rollen- und Berechtigungskonzept
  - Notfallmanagement

Schritt 7 - Internes Audit

- Ein internes Audit **muss mindestens 1 mal jährlich** durchgeführt werden.

- Es ist ratsam das interne Audit durch einen **externen Auditor** durchführen zu lassen, da dieser einen anderen Blick auf das ISMS hat als ein Interner Mitarbeiter.

- Es muss ein **Auditprogramm** erstellt werden der alle Themen der jeweiligen Prüfgrundlage in einem 3-Jahreszyklus abdeckt.

Schritt 8 - Zertifizierungsaudit

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

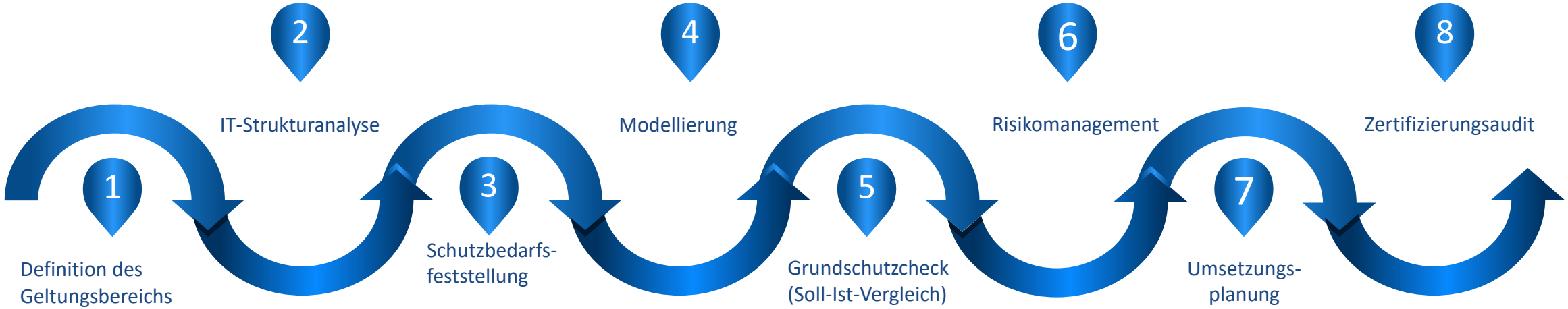
- Beim Zertifizierungsaudit beantragt der Antragsteller die Durchführung des Audits bei einer unabhängigen Zertifizierungsstelle. Die Zertifizierungsstelle bestimmt das Auditteam.

- Das Auditteam führt zunächst die Bereitschaftsbewertung beim Antragsteller durch (Stufe 1). Dabei wird geprüft ob der Antragsteller bereit für das Stufe 2 Audit ist.

- Beim Stufe 2 Audit wird das ISMS vollumfänglich geprüft. Dies kann je nach Größe des Informationsverbundes mehrere Tage dauern.

- Bei einer erfolgreichen Prüfung stellt die Zertifizierungsstelle dem Antragssteller ein entsprechendes Zertifikat aus.

Nötige Schritte zur Umsetzung eines ISMS (ISO/IEC 27001 auf Basis IT-Grundschutz)



Mit einer erfolgreichen Zertifizierung ist der Prozess nicht abgeschlossen
– Nach der Zertifizierung ist vor der Zertifizierung

Schritt 1: Definition des Geltungsbereichs

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

- Der Geltungsbereich oder auch Anwendungsbereich umfasst die Gesamtheit von
  - infrastrukturellen,
  - organisatorischen,
  - personellen und
  - technischen Komponenten,

  die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen.

- Kann die gesamte Institution umfassen aber auch aus Teilbereichen bestehen.

Schritt 2: IT-Strukturanalyse

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

- Die Strukturanalyse dient der Vorerhebung von Informationen, die für die weitere Vorgehensweise nach IT-Grundschutz benötigt werden.

- Erfassung der Bestandteile des Geltungsbereich
  - Geschäftsprozesse und Informationen
  - Anwendungen
  - IT-Systeme
  - Räume, Gebäude, Standorte
  - Kommunikationsverbindungen

Ziel dabei ist es das Zusammenspiel der Geschäftsprozesse, der Anwendungen und der vorliegenden Informationstechnik zu analysieren und zu dokumentieren.

Schritt 3: Schutzbedarfsfeststellung

- Ermittlung welcher Schutz für die Geschäftsprozesse, die dabei verarbeiteten Informationen und die eingesetzte Informationstechnik hinreichend und angemessen ist.

- Betrachtung des erwartete Schadens, der bei einer Beeinträchtigung von Vertraulichkeit, Integrität oder Verfügbarkeit entstehen könnte.

- Einteilung in die drei Schutzbedarfskategorien
  - Normal: Die Schadensauswirkungen sind begrenzt und überschaubar.
  - Hoch: Die Schadensauswirkungen können beträchtlich sein.
  - Sehr hoch: Die Schadensauswirkungen können ein existentiell bedrohliches Ausmaß erreichen.

Schritt 4: Modellierung

- Auswahl derjenigen IT-Grundschutzbausteine, die für die Sicherheit des betrachteten Geltungsbereiches benötigt werden und relevant sind.

- Zuordnung der im Zuge der Strukturanalyse erfassten Zielobjekte zu den entsprechenden IT-Grundschutz-Bausteine der einzelnen Schichten.
  - Im Idealfall werden alle Zielobjekte angemessen durch IT-Grundschutz-Bausteine abgebildet.
  - Zielobjekte, für die es keinen hinreichend passenden Baustein gibt, muss explizit eine Risikoanalyse durchgeführt werden.

- Nicht jeder Baustein ist relevant.
  - Hinreichende, aussagekräftige Begründung bei Nichtanwendung erforderlich.

- Ergebnisse werden dokumentiert.

Schritt 5: Grundschutzcheck (Soll-Ist-Vergleich)

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

- Organisationinstrument, mit dessen Hilfe ein Überblick über das vorhandene Sicherheitsniveau aufgezeigt werden kann.

- Ermittlung des Umsetzungsgrades der Sicherheitsanforderungen des IT-Grundschutz-Kompendiums:
  - Ja
  - Teilweise
  - Nein
  - Entbehrlich

- Die Identifizierung von noch nicht oder nur teilweise erfüllten Anforderungen zeigt dabei Verbesserungsmöglichkeiten auf.

Schritt 6: Risikomanagement

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

- Die Risikoanalyse hat die Aufgabe, relevante Gefährdungen für den Informationsverbund zu identifizieren und die daraus möglicherweise resultierenden Risiken abzuschätzen.
- Muss explizit durchgeführt werden, wenn der betrachtete Informationsverbund Zielobjekte enthält, die:
  - einen hohen oder sehr hohen Schutzbedarf in mindestens einem der drei Grundwerte Vertraulichkeit, Integrität oder Verfügbarkeit haben oder,
  - mit den existierenden Bausteinen des IT-Grundschutzes nicht hinreichend abgebildet (modelliert) werden können,
  - in Einsatzszenarien (Umgebung, Anwendung) betrieben werden, die im Rahmen des IT-Grundschutzes nicht vorgesehen sind.

Das Ziel ist es, die Risiken durch angemessene Gegenmaßnahmen auf ein akzeptables Maß zu reduzieren, die Restrisiken transparent zu machen und dadurch das

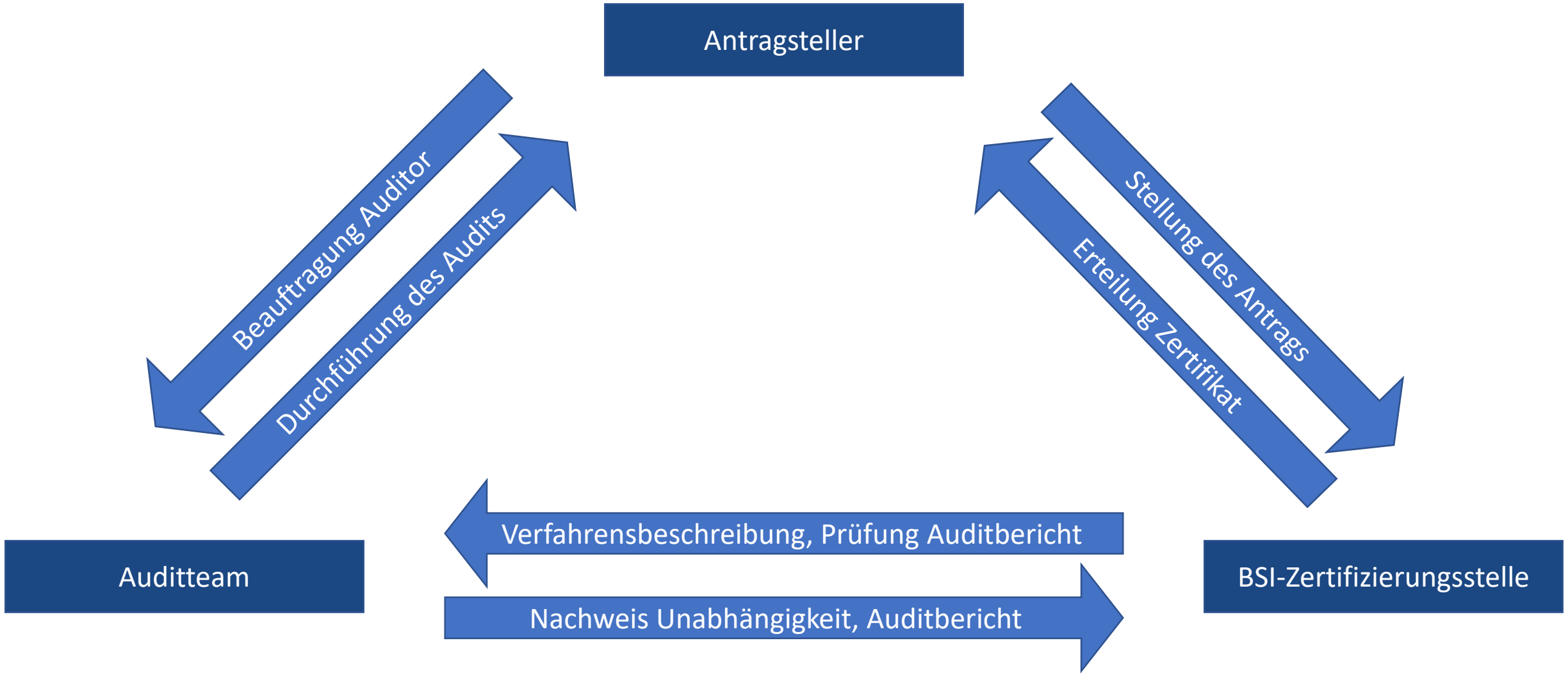
Schritt 7: Umsetzungsplanung

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

- In der Regel decken der IT-Grundschutz-Check und ggf. zusätzliche Risikoanalysen Defizite auf:
  - Lücken in den vorhandenen organisatorischen Regelungen
  - Mangelnde Kontrolle der geltenden Regeln
  - fehlende Sicherheitstechnik
  - unzureichender baulicher Schutz

- Im Zuge der Umsetzungsplanung geht es darum diese Lücken und Defizite effizient zu beseitigen:
  - Maßnahmen konsolidieren
  - Kosten und Aufwände bestimmen
  - Umsetzungsreihenfolge festlegen
  - Verantwortlichkeiten regeln

Schritt 8: Zertifizierungsaudit



Schritt 8: Zertifizierungsaudit

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT

Phase 1: Dokumentenprüfung

- Prüfung der Referenzdokumente
  - A.0 IT-Sicherheitsrichtlinien
  - A.1 IT-Strukturanalyse
  - A.2 Schutzbedarfsfeststellung
  - A.3 Modellierung des Informationsverbund
  - A.4 Ergebnis des IT-Grundschutz-Checks
  - A.5 Risikoanalyse
  - A.6 Risikobehandlungsplan (Realisierungsplan)

Phase 2: Umsetzungsprüfung

- Prüfung der Umsetzung durch den Auditor
  - Fokus auf Vollständigkeit, Korrektheit, und Wirksamkeit der in den Referenzdokumenten beschriebenen Maßnahmen sowie deren Konformität zu den Anforderungen von ISO 27001 und IT-Grundschutz

Fragen

Vielen Dank für Ihre Aufmerksamkeit

DEBIT
IHR IT-SYSTEMHAUS MIT SICHERHEIT