DTS

DTS
Information Security

Information Security

Informationssicherheit ist die Voraussetzung für eine erfolgreiche Digitalisierung. Unterschiedliche Vorgaben, Best Practices, Normen oder Zertifizierungen liefern hierfür ein solides fachliches Fundament und ein umfangreiches Arbeitswerkzeug. Dabei handelt es sich um Methoden, Anleitungen, Empfehlungen und Hilfestellungen zur Selbsthilfe für Behörden, Unternehmen und Institutionen, die sich mit der Absicherung ihrer Daten, Systeme und Informationen befassen wollen. Zentral ist dabei, einen ganzheitlichen Ansatz zur Informationssicherheit zu verfolgen: Neben technischen Aspekten werden infrastrukturelle, organisatorische und personelle Themen betrachtet. Dies ermöglicht ein systematisches Vorgehen, um notwendige Sicherheitsmaßnahmen zu identifizieren und umzusetzen. So definiert der BSI die Information Security.

Gerade die benannte Ganzheitlichkeit steht für uns in allen Bereichen an erster Stelle, d. h. beginnend mit der Strategie und den entsprechenden Richtlinien über die daraus resultierenden Prozesse bis hin zu Workshops und IT-Security Lösungen. Somit ist sichergestellt, dass das gesamte Zusammenspiel funktioniert. Unsere Experten stehen Ihnen mit umfangreichen Beratungs- und Dienstleistungen zur Verfügung. Wir erstellen mit Ihnen maßgeschneiderte Lösungen und unterstützen Sie in jedem erdenklichen Aspekt der Information Security.

- Aufbau, Implementierung & Aufrechthaltung eines Informationssicherheitsmanagementsystems (ISMS)
- Vorbereitung auf Zertifizierungen & Anforderungen resultierend aus der Informationssicherheit
  - Consulting für: ISO 27001/27002, ISO 27019 & IT-SiKat, TISAX®, BSI Grundschutz auf Basis ISO27001, KRITIS, EU-DSGVO
- Systemaudits/First Audits/Internal Audits
- Notfallmanagement
- Risikomanagement/Risk Assessment
  - BSI 200-3, ISO27005
- Krisenkommunikation/Krisenbewältigung
- Individuelle Schulungs- & Sensibilisierungskonzepte

Unsere Vorteile:

Pragmatischer Lösungsansatz
Wir passen Ihre Prozesse und Maßnahmen so an, dass diese in Ihrem Unternehmen ressourcensparend integriert und gelebt werden können.

Geringerer Kostenaufwand
Durch unseren pragmatischen Ansatz sparen wir Projektkosten und Aufwand.

Erfahrung im Bereich Informationssicherheit
Durch die unterschiedlichsten Projekte in allen möglichen Branchen bringen wir übergreifende Erfahrungen und Expertise mit.

Reports & Handlungsempfehlungen
Sie erhalten von uns auf Wunsch ausführliche Berichte zu allen Etappen und Prozessen, inkl. entsprechender Handlungsempfehlungen, angepasst auf Ihre Unternehmensstruktur.

Informationssicherheitsmanagementsystem (ISMS)

Nicht erst seit der Digitalisierung zählen Informationen mit zu den höchsten Gütern eines Unternehmens und erfordern einen umfangreichen Schutz. Betriebsgeheimnisse, Produktionsverfahren, Kundeninformationen – Sie vor Missbrauch, Verlust oder Diebstahl zu bewahren ist unabdingbar. Dabei umfasst die Informationssicherheit sowohl digitale als auch analoge Daten. Mithilfe einer nachhaltigen Strategie wird sichergestellt, dass die Schutzziele der Informationssicherheit erreicht werden bzw. erhalten bleiben.

- Integrität der Systeme, der Daten und von notwendigen Veränderungen
- Vertraulichkeit der Daten
- Verfügbarkeit der Systeme und Daten
- Authentizität von Informationen und Quellen
- Verbindlichkeit für Prozesse, Handlungen, Systembestandteile
- Belastbarkeit der IT-Systeme

Der Service

Um zu einem bedarfsgerechten Sicherheitsniveau für alle Geschäftsprozesse, Informationen und der IT-Systeme einer Institution zu kommen, ist mehr als das Anschaffen von Virenschutz, Firewalls oder die Datensicherung notwendig. Ein ganzheitliches Konzept ist wichtig. Dazu gehört vor allem ein funktionierendes und in die Institution integriertes Sicherheitsmanagement. Informationssicherheitsmanagement ist jener Teil des allgemeinen Risikomanagements, der die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen, Geschäftsprozessen, Anwendungen und IT-Systemen gewährleisten soll. 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. Informationssicherheit ist nicht nur eine Frage der Technik, sondern hängt in erheblichem Maße von den organisatorischen und personellen Rahmenbedingungen ab.

Immer mehr Geschäftsprozesse werden über Informations- und Kommunikationstechnik miteinander verknüpft. Dies geht einher mit einer steigenden Komplexität der technischen Systeme und mit einer hohen Abhängigkeit vom korrekten Funktionieren der Technik. Daher ist ein geplantes und organisiertes Vorgehen aller Beteiligten notwendig, um ein angemessenes und ausreichendes Sicherheitsniveau durchzusetzen und aufrechtzuerhalten. Eine Verankerung dieses Prozesses in allen Geschäftsbereichen kann nur gewährleistet werden, wenn dieser zur Aufgabe der obersten Leitungs- bzw. Managementebene wird. Die oberste Managementebene ist verantwortlich für das zielgerichtete und ordnungsgemäße Funktionieren einer Institution und damit auch für die Gewährleistung der Informationssicherheit nach innen und außen. Daher muss diese den Sicherheitsprozess initiieren, steuern und kontrollieren. Dazu gehören strategische Leitaussagen zur Informationssicherheit, konzeptionelle Vorgaben und organisatorische Rahmenbedingungen sowie ausreichende Ressourcen, um Informationssicherheit innerhalb aller Geschäftsprozesse erreichen zu können.
(Quelle: BSI Bund 200-2 Grundschutz Standard)

Was leistet DTS?

Damit die wichtigsten Geschäftsprozesse eines Unternehmens nachhaltig störungsfrei ablaufen, bedarf es einer Sicherheitsstrategie, die über sämtliche Bereiche eines Unternehmens oder eine Behörde hinweg etabliert wird.
Die Integration eines ISMS kann sich in der Praxis als durchaus aufwendig erweisen. Hierbei ist es essenziell, dass das Sicherheitskonzept in bestehende Organisationsstrukturen und betriebliche Abläufe integriert wird und die Geschäftsprozesse einer Institution nicht grundlegend verändert werden. Dabei entstehen folgende Herausforderungen, die es zu berücksichtigen gilt:

- Aufbau und Definition der Aufgabenbereiche eines ISMS
- Festlegung des Geltungsbereichs
- Etablierung der notwendigen Sicherheitsorganisation und des Sicherheitsprozesses
- Entwicklung einer angemessenen Sicherheitsstrategie und Sicherheitszielen
- Integration der Informationssicherheitsstrategie in die bestehende Unternehmensstrategie

- Auswahl geeigneter Sicherheitsmaßnahmen
- Erhalt sowie kontinuierliche Verbesserung des einmal erreichten Sicherheitsniveaus
- Klare Abgrenzung zum Datenschutz und der IT-Sicherheit
- Aufbau einer geeigneten Sicherheitsorganisation

Wir unterstützen Sie bei der gesamten Konzeption und Umsetzung eines ISMS nach der ISO 27001 oder ähnlichen angelehnten Standards. Als Grundlage der Umsetzung eines ISMS wird der PDCA-Zyklus verwendet. Dabei unterteilt sich die Einführung eines ISMS in die Planungsphase, Umsetzungsphase, Überprüfungs- und Überarbeitungsphase sowie Verbesserungsphase mit entsprechender Neugestaltung. In dem gesamten Projekt wird die Projektleitung von Hr. Sven Meier, seit 2012 ausgebildeter und zertifizierter IT-Sicherheitsbeauftragter (ISO, BSI Grundschutz, TISAX, etc.), übernommen. Dieser trägt die Verantwortung für das Projekt und die eingesetzten Ressourcen. Während der Projektphase werden entsprechende Kennzahlen definiert, die die Wirksamkeit eines ISMS bemessen und auswerten können.

Vorbereitung auf Zertifizierung zur Informationssicherheit

Wir bereiten Sie auf alle wichtigen Zertifizierungen der Informationssicherheit vor, beraten Sie in allen notwendigen Aspekten und erarbeiten gemeinsam Konzepte und Strategien.

- ISO 27001 & 27002 Consulting
- ISO 27019 & IT-SiKat Consulting
- TISAX® Consulting
- BSI Grundschutz
- KRITIS Consulting
- EU-DSGVO Consulting / ISO 27018

Der Service

ISO 27001 & 27002 Consulting

Verschiedene Gesetze verpflichten dazu, die Informationstechnik zurechenbar und ganzheitlich zu betrachten und einen rechtsverbindlichen Nachweis der Schutzmaßnahmen zu erbringen. Zudem ist die Informationssicherheit ein stetig wachsender Erfolgs- sowie Vertrauensfaktor für Unternehmen und Institutionen. Die internationale Norm ISO/IEC 27001 stellt bei der Darstellung eines verlässlichen Informationssicherheitsmanagementsystems eines der bekannten und anerkanntesten Frameworks im internationalen Umfeld dar.

Jede Umsetzung der ISO/IEC 27001 steht und fällt mit einem an der Geschäftsstrategie einer Institution ausgerichteten Scoping. Die Kür ist es sowohl wirtschaftliche als auch funktionale Aspekte dabei in einem idealen Verhältnis unter einen Hut zu bringen. Im Rahmen einer GAP-Analyse definieren wir die notwendigen Maßnahmen zur Erfüllung der Anforderungen.

Im Projekt stellen wir frühzeitig fest, welche Maßnahmen zwingend direkt umgesetzt werden müssen und wo eine spätere Umsetzung genügt. Unsere Ergebnisse zeigen Ihnen konkrete Verbesserungspotentiale. Auf Grundlage eines verlässlichen Projektplanes, der alle Aufwände und zeitlichen Vorgaben darstellt, können Sie selbst entscheiden, wo wir Sie unterstützen dürfen.

(Quelle: www.hisolutions.com/security-consulting/informationssicherheit/iso-27001)

ISO 27019 & IT-SiKat Consulting – Norm zur Informationssicherheit für die Energieversorgung

Mit der internationalen Norm zur Informationssicherheit für die Energieversorgungsindustrie wird die Leitlinie für ein Informationssicherheitsmanagementsystem (ISMS) dargelegt, welches die Sicherstellung des funktionsfähigen und zuverlässigen Betriebs der Leit- und Automatisierungstechnik verfolgt. Hierbei werden Systeme und Netzwerke zur Steuerung, Regelung und Überwachung von Gewinnung, Erzeugung, Übertragung, Speicherung und Verteilung von elektrischer Energie, Gas, Öl und Wärme miteinbezogen. Unter dem Begriff der Prozessleittechnik fallen u. a. die Kommunikationstechnik sowie Steuerungs-, Automatisierungs-, Schutz-, Sicherheits- und Messsysteme. Eine ganzheitliche Betrachtung, welche die dazugehörigen IT- und OT-Systeme einschließt, ist unerlässlich, um eine zuverlässige Energieversorgung zu gewährleisten. Ferner sind sämtliche Prozesse und Systeme zu betrachten, die innerhalb einer Organisation angewandt werden. Die aktualisierte Norm fordert bspw. dass die Betreiber kritischer Infrastruktur im Energiesektor ein gleichwertiges Sicherheitsniveau von relevanten Dienstleistern einfordern und dies dokumentieren. Der Ablauf ist analog zu einer Zertifizierung nach ISO 27001.

Vorteile einer Zertifizierung nach ISO 27001 oder 27019:

- International akkreditierter Nachweis über die Wirksamkeit des Sicherheitskonzepts
- Stärkere Rechtssicherheit in sicherheitskritischen Belangen
- Systematische Realisierung der Schutzziele der Informationssicherheit
- Erhaltung und kontinuierliche Steigerung des Sicherheitsniveaus
- Integration geeigneter Maßnahmen zur Abwehr von Bedrohungen aller Art
- Stärkung des Sicherheitsbewusstseins der Mitarbeiter

TISAX® Consulting
Ablauf einer TISAX Zertifizierung:

- Definition des Geltungsbereichs und des Assessment-Levels
- Kick-Off, Dokumentenprüfung und Self-Assessment
- Vor-Ort-Assessment oder Remote-Assessment mit Zwischenbericht
- Planung, Freigabe, Umsetzung und anschließende Bewertung von Korrekturmaßnahmen
- Audit zur Wirksamkeitsprüfung
- Einstellung des Abschlussberichts in der TISAX®-Onlineplattform und Erteilung der Prüflabels

Vorteile für ein Unternehmen:

- Vertrauen aller Stakeholder gewinnen
- Erfüllung der Bedürfnisse und Anforderungen für Lieferanten und Kunden
- Erfüllung der hohen Sicherheitsanforderungen in der Automobilindustrie
- Internationale Anerkennung des Sicherheitsniveaus durch die Automobilindustrie
- Vermeidung von Mehrfachzertifizierungen und -bewertungen
- Zeit- und Kostenersparnis aufgrund höherer Effizienz
- Erhöhte Transparenz entlang der gesamten Lieferkette
- Verankerung der Informationssicherheit im Unternehmen
- Kontinuierliche Erhaltung des einmal erreichten Informationssicherheitsniveaus
- Wettbewerbsvorteil durch Abgrenzung zu Marktbegleitern

BSI Grundschutz auf Basis des ISO27001 Consulting

Die IT-Grundschutz-Methodik wird im BSI Standard 200-2 definiert und beinhaltet eine praxisnahe Beschreibung zum Aufbau und Betrieb eines ISMS. Die wichtigsten Themen hierbei sind:

- Aufgaben des ISMS
- Aufbau Organisationsstruktur für IS
- Auswahl der Sicherheitsanforderungen & Umsetzung des Sicherheitskonzepts
- Kontinuierliche Verbesserung und Aufrechterhaltung der IS
- Auswahl der Vorgehensweise bzw. des Absicherungsniveaus auf Basis der Ersterfassung, damit der IT-Grundschutz an die Anforderungen von Organisationen unterschiedlicher Größe, Branche und Funktion dem Schutzbedarf entsprechend angepasst werden können.
- Ziel: Kosteneffektives und Zielführendes ISMS, Aufwandsreduktion
    - Basis
        - Einstieg in Sicherheitsprozess
        - Initiierung eines ISMS
        - Schnellstmögliche Reduktion der Risiken

        - Anschließende Detailanalyse der eigentlichen Sicherheitsanforderungen
    - Standard
        - Umfassende und tiefgehende Methodik
        - Vom BSI bevorzugte Vorgehensweise
        - ISO 27001 kompatibel
    - Kern
        - Vertiefte Absicherung von besonders wichtigen Geschäftsprozessen und Assets
        - Auch als Einstieg in den Sicherheitsprozess möglich, um besonders gefährdete Geschäftsbereiche abzusichern

KRITIS Consulting
Das 2021 verabschiedete IT-Sicherheitsgesetz festigt allen voran die Rolle des BSI als zentrale Behörde für Informationssicherheit und Digitalisierung. Als Cyber-Sicherheitsbehörde Deutschlands erhält es u. a. weitreichende Befugnisse und Kompetenzen bei der Erkennung von Sicherheitslücken oder bei der Untersagung des Einsatzes kritischer Komponenten in sicherheitskritischen Bereichen. Zentraler Bestandteil des überarbeiteten Gesetzes ist die Veränderung im Hinblick auf die Sicherheit von Betreibern kritischer Infrastrukturen und deren Systeme. Die KRITIS-Regulierung wurde durch das IT-Sicherheitsgesetz 2.0 erheblich ausgeweitet. Folgende Neuerungen sind im Zuge dessen in Kraft getreten:

- Eine Angriffserkennung ist verpflichtend für Betreiber kritischer Infrastrukturen zu implementieren. In der Praxis kann dieser Anforderung durch ein SIEM und ein SOC nachgegangen werden.
- KRITIS-Betreiber und UNBÖFI sind in einem Störungsfall dazu verpflichtet, dem BSI auf Nachfrage sämtliche Daten zur Verfügung zu stellen, die zur Bewältigung der Störung notwendig sind.
- Dem Innenministerium muss der Einsatz von kritischen Komponenten durch KRITIS-Betreiber bestimmter Sektoren angezeigt werden. Kritische Komponenten sind IT-Produkte in KRITIS-Anlagen, von deren Funktionalität der Betrieb der Anlage maßgeblich abhängt und ein Ausfall einer solchen Komponente erheblichen Einfluss auf die Funktion der Anlage hätte.
- Unmittelbar nach Feststellung als KRITIS-Betreiber müssen sich diese beim BSI registrieren und eine Kontaktstelle benennen.
- Vergrößerung des Geltungsbereichs der KRITIS-Sektoren wurde um den Siedlungsabfallentsorgungssektor erweitert und Schwellenwerten für Betreiber kritischer Infrastruktur wurden erheblich gesenkt sowie neue KRITIS-Anlagen hinzugefügt.

Unsere passgenaue ISMS KRITIS Konzeption mit Ihnen bzw. für Sie erfolgt in den folgenden Phasen:

- Phase 1: Workshop/Coaching zur Definition der Grundstrukturen
- Phase 2: Aufbau und Integration eines Informationssicherheitsmanagementsystems
- Phase 3: Implementierung der definierten Maßnahmen zur Informationssicherheit an den Standorten
- Phase 4: Begleitung des Audits zur Überprüfung nach §8a KRITIS Verordnung

EU-DSGVO Consulting / ISO 27018 als international zertifizierter Cloud-Standard
Für Anbieter von Cloud-Diensten werden durch die Norm datenschutzrechtliche Anforderungen festgelegt, welche die Verarbeitung von personenbezogenen Daten behandeln. Die Zertifizierung nach ISO 27018 stellt für viele ein entscheidendes Kriterium für die Auswahl des Cloud-Dienstleisters dar. Die Vorteile dieser Zertifizierung sind demnach:

- Wettbewerbsvorteil durch Abgrenzung zu Marktbegleitern
- Stärkung des Vertrauens potenzieller Kunden in das eigene Unternehmen
- Hohe Konformität zur DSGVO und zur EU-Datenschutzrichtlinie

Systemaudits / First Audits / Internal Audits

Wie weit ist Ihr Unternehmen im Zertifizierungsprozess zur Informationssicherheit? Egal ob ISO 27001, BSI Grundschutz, TISAX® oder anderweitige Vorgaben zur Informationssicherheit – Um die Normkonformität Ihres Informationssicherheitsmanagementsystems oder Teilen davon zu überprüfen, führen wir Systemaudits anhand Ihrer definierten Anforderungen durch. Hierzu betrachten und bewerten wir die Dokumentation, machen aber auch entsprechende Begutachtungen der Räumlichkeiten vor Ort.

- Systemaudits
- First Audits
- Internal Audits
- ISO 27001, BSI Grundschutz, TISAX® etc.

Der Service

Das Vorgehensmodell stellt sich in den folgenden Phasen dar:

Phase 1:

- Vorbereitungs-Kickoff
- Bestimmung der notwendigen Ansprechpartner
- Abstimmung von Interview-Terminen
- Sichtung der Kundendokumentation mit dem Ziel ein Verständnis der Regelungen zu bekommen

Phase 2:

- Durchführung des Systemaudits vor Ort beim Kunden
- Auditierung der gelebten Praxis in den Prozessen
- Auditierung der Vorgabe- und Nachweisdokumentation
- Auditierung der physischen und räumlichen Gegebenheit vor Ort beim Kunden inkl. Gebäude und Infrastruktur
- Identifikation von GAPs (Maßnahmenlücken)

Phase 3:

- Erstellung eines ausführlichen Auditberichts mir Handlungsempfehlungen (Referenzmaßnahmenziele)
- Besprechung und Präsentation der Ergebnisse auf Wunsch auch vor dem Management

Phase 4:

- Erstellung eines Maßnahmenplans auf Basis der Feststellungen
- Erarbeitung eines Projektplans zur Umsetzung der nicht erfüllten Referenzmaßnahmen
- Unterstützung bei der Abarbeitung der Maßnahmen bis zum erfolgreichen Abschluss

Notfallmanagement

Unser Konzept beinhaltet Methoden und Maßnahmen für die Integration eines Notfallmanagements in der Organisation bzw. Institution der Mediengruppe Oberfranken. Die angebotenen Dienstleistungen basieren auf dem aktuellen Standard 200-4 des BSI. Die einzelnen Tätigkeiten lassen sich aber auch nach anderen Standards definieren.

- Ganzheitliche Notfallmanagement-Konzeptionierung
- Anforderungsaufnahme, Voranalyse & Soll-Ist-Vergleich
- Leitlinie mit Definition aller Hauptprozesse
- Aufbau konkreter Notfallpläne
- Überprüfung, Auswertung & Optimierung der Notfallpläne

Der Service

Die angebotenen Dienstleistungen umfassen:

- Phase 1: Initialisierung & Voranalyse & BIA – Kickoff Konzeption-Workshop
    - Anforderungsaufnahme der Motivation des BCM
    - Anforderungsaufnahme des abzusichernden Zeitraums des BCM
    - Anforderungsaufnahme für die Bestimmung der Kritikalitäten/MTPD/RTO/RPO
    - Anforderungsaufnahme der vorhandenen Ressourcen
    - Anforderungsaufnahme der Systeme
    - Anforderungsaufnahme der genutzten kritischen Systeme
    - Anforderungsaufnahme der Kommunikationsarchitektur
    - Möglichkeiten der Strukturierung und Aufbau reaktiver Notfalldokumentation
    - Übernahme der Ergebnisse aus dem Risikomanagement und Gefährdungsdefinitionen
    - Bestimmung der inhaltlichen Ziele und des Geltungsbereichs
    - Sichtung aktueller Informations- und Dokumentationsquellen
    - Abgrenzung/ Erweiterung zu Betriebshandbüchern und Richtlinien
    - Aufnahme der Organisationsstruktur intern und extern
    - Voranalyse der BIA
    - Business Impact Analyse
    - Soll-Ist-Vergleich
    - GFP

- Phase 2: Erstellung BCM-Pläne für Hauptprozesse – Die Erstellung einer Dokumentenvorlage zur Definition einer Leitlinie
    - Motivation für den Aufbau des BCMS
    - Definition des abzusichernden Zeitraums
    - Geltungsbereich des BCM
    - Definierung der Gesamtverantwortung

    - Definierung der Verantwortlichkeiten im BCM
    - Definition des BCM und der Eskalationsstufen „Störung“, „Notfall“, „Krise“
    - Definition der Netzwerkkommunikation
    - Definition der Kryptographie
    - Zentrale Rollen im BCMS
    - Verfügbare Ressourcen

- Phase 3: Erstellung für IT-Notfallpläne – Eine Richtlinie zum Aufbau einer besonderen Aufbauorganisation (BAO)
    - Aufbau eines Notfall- /Krisenstabs
    - Aufbau des Kernteams
    - Aufbau der situativen Erweiterung (optional)
    - Aufbau der Stabsassistenz
    - Aufbau des Notfallbewältigungsteams
    - Definition/ Erstellung des Meldewegs
    - Vorgaben der Methoden und Regeln für die Stabsarbeit
    - Vorgaben für die Kommunikation während einer Notfallbewältigung
    - Definieren der Kriterien für die Deeskalation
    - Definieren der Kriterien für die Auflösung der BAO
    - Analyse der Bewältigung
    - Erstellung oder Erweiterung von Notfallplänen
    - Aufrechterhaltung und Kontrolle des Notfallmanagements

- Phase 4: Test & Übung – Die definierten und umgesetzten Maßnahmen werden nach erfolgreicher Integration mit den Verantwortlichen der Mediengruppe Oberfranken getestet.
    - Überprüfung des BCMS

- Phase 5: Optimierung
    - Unterstützung bei dem Optimierungsprozess

Risikomanagement/Risk Assessment

Wir ermöglichen Ihnen ein vollumfassendes Risikomanagement und/oder Risk Assessment nach BSI Standard 200-3 und ISO 27005.

- BSI Standard 200-3
- ISO 27005
- Risikoanalyse, -bewertung, -behandlung & -überwachung

Der Service

BSI Standard 200-3

Das Verfahren zur Risikoanalyse stellt eine anerkannte und bewährte Möglichkeit dar, ein vorher definiertes Informationssicherheitsniveau aufwandsreduziert zu erreichen. Auf Basis elementarer Gefährdungen, welche im IT-Grundschutz-Kompendium charakterisiert werden, wird bereits bei der Entwicklung der IT-Grundschutz-Bausteine eine Risikobewertung für Bereiche mit normalem Schutzbedarf miteinbezogen. Der Vorteil dieser Methode besteht darin, dass Anwender des IT-Grundschutzes für die meisten Informationssysteme keine separate Bedrohungs- und Schwachstellenanalyse durchführen müssen, da diese im Vorfeld durch das BSI durchgeführt wurde.

Sollte der betrachtete Informationsverbund jedoch Zielobjekte enthalten, die einen hohen Schutzbedarf aufweisen, mit den vorhandenen Bausteinen des IT-Grundschutzes nicht vollständig modelliert werden können oder in Umgebungen betrieben werden, welche nicht durch den IT-Grundschutz abgedeckt werden können, ist eine Risikoanalyse zwingend erforderlich.

ISO 27005

- Definition der Rahmenbedingungen
  - Betrachtungsbereich abgrenzen
  - Organisation für das Risikomanagement etablieren
  - Methodenfestlegung
  - Kriterien zur Bewertung, Akzeptanz und den Auswirkungen festlegen
- Identifizierung von Risiken
  - Erfassung aller Unternehmenswerte. Hierunter fallen Informationen, Geschäftsprozesse, Personal, Organisationen und IT-Komponenten
  - Feststellung aller relevanten Bedrohungen und vorhandenen Schwachstellen
  - Identifizierung bestehender und bereits geplanter Sicherheitsmaßnahmen
  - Ermittlung potenzieller Konsequenzen, die bei Eintritt relevanter Bedrohungen entstehen könnten
- Analyse von Risiken
  - Bewertung des Schadenausmaßes bei Verletzung einer der Schutzziele der Informationssicherheit (Vertraulichkeit, Integrität oder Verfügbarkeit)
  - Bestimmung der Eintrittswahrscheinlichkeit einer Bedrohung
  - Mit der Kombination aus Schadenausmaß und Eintrittswahrscheinlichkeit lässt sich das Risikoniveau ermitteln
- Bewertung von Risiken
  - Die Priorisierung der Risiken auf Grundlage des Risikoniveaus sowie der Bewertungs- und Akzeptanzkriterien bildet die Entscheidungsbasis für die anschließende Risikobehandlung

- Behandlung von Risiken
    - Durch die Erstellung eines Risikobehandlungsplans auf Grundlage des erstellten Risikobilds kann entschieden werden, wie die identifizierten Risiken behandelt werden. In Anbetracht der wirtschaftlichen Folgen der Risiken im Verhältnis zu den Implementierungskosten angemessener Vorkehrungen werden dann die Entscheidungen zur Behandlung der Risiken getroffen. In der Regel fallen die Möglichkeiten zur Risikobehandlung in eine der folgenden vier Kategorien
    - Entscheidung, ob ein Risiko
        - mit Hilfe geeigneter Sicherheitsmaßnahmen reduziert wird
        - aufgrund Erfüllung der Akzeptanzkriterien für Restrisiken unbehandelt bleibt
        - durch Verzicht auf bestimmte Prozesse bzw. Aktivitäten vermieden wird
        - mittels geeigneter Übertragung an Dritte (bspw. Versicherung) geteilt wird
- Akzeptanz von Risiken
    - Die Leitung einer Organisation entscheidet auf Grundlage des Risikobehandlungsplans über die darin enthaltenen Handlungsempfehlungen zwecks Implementierung der Maßnahmen unter Berücksichtigung des Ressourceneinsatzes. Risiken, gegen die keine Maßnahmen ergriffen werden, müssen akzeptiert werden.
- Kommunikation von Risiken
    - Um die Aktualität der Ergebnisse und angewandten Methoden sicherzustellen, bedarf es einer stetigen Kommunikation bezüglich der Informationen über Risiken zwischen dem Risikomanagement und den Entscheidungsträgern. Es ist empfehlenswert ggf. weitere relevante Mitarbeiter hinzuzuziehen und einen ständigen Austausch mit diesen zu pflegen.
- Überwachung und Überprüfung von Risiken
    - Sämtliche Einflüsse auf das Risikomanagement müssen jederzeit auf Veränderungen untersucht werden. Da das geschäftliche und technologische Umfeld stets einem Änderungsprozess unterworfen ist, wirken sich diese Änderungen auf die Bedrohungen und Schwachstellen einer Institution aus. Auch sollte der Ansatz für das Risikomanagement in regelmäßigen Abständen auf Angemessenheit überprüft werden.

Krisenkommunikation

In der IT-Branche ist es einzigartig, dass wir Ihnen eine ganzheitliche Konzeption zur Krisenkommunikation, beginnend mit einem Konzeptions-Kick-Off bis hin zur Definierung und Aktualisierung der Krisenmanagementstrukturen anbieten.

- Konzept zur Krisenkommunikation, inkl. Kick-Off
- Vorbereitung der Krisenkommunikation
- Definierung & Anpassung der Kommunikationsstrukturen
- Entwicklung eines Krisenkommunikationsplans
- Aktualisierung der Krisenmanagementstrukturen

Der Service

- Konzeptions-Kick-Off
    - Anforderungsaufnahme der Unternehmensstrukturen, des etablierten Notfall- & Krisenmanagements, der Kommunikationsarchitektur
    - Sichtung der Dokumentationsquellen
- (1) Vorbereitung der Krisenkommunikation
    - Definition der grundlegenden und organisatorischen Rahmenbedingungen für die Krisenkommunikation
    - Entwicklung/Umsetzung/Prüfung des Krisenkommunikationszyklus
    - Evaluierung/Prüfung/Aktualisierung der Kommunikations- bzw. Informationsflüsse
- (2) Definierung/ Aktualisierung von Kommunikationsstrukturen innerhalb des Krisenstabs
    - Definierung/Evaluierung der zielgruppengerechten Kommunikation
    - Festlegung der Kommunikationsstrukturen innerhalb/außerhalb der Organisation
    - Definieren der Presseaufgaben
- (3) Entwicklung eines Krisenkommunikationsplans
    - Vorbereitende Maßnahmen zum Kommunikationsplan & Entwicklung eines Maßnahmenplans
- (4) Definierung und Aktualisierung der Krisenmanagementstrukturen
    - Festlegung der Zuständigkeiten, Kompetenzen und Rollen des Krisenstabs
    - Definition der Kommunikationswege
    - Prüfung des Lagezentrums und der Ausstattung
    - Richtlinien zur Öffentlichkeitsarbeit
    - Dokumentationsvorlage für die Protokollierung

Individuelle Schulungs- & Sensibilisierungskonzepte

Awareness-Kampagnen und eine e-Learning Plattform sind nicht immer ausreichend, um den Bedürfnissen und die Erreichbarkeit der Benutzer/Mitarbeiter gerecht zu werden. Wir bieten individuelle Schulungskonzept an, die auf Ihre Anforderungen maßgeschneidert sind und wir Ihnen dieses entsprechend den Anforderungen erstellen und bei Ihnen auf Wunsch in Ihrem Schulungssystem implementieren, als Schulungsvideo zur Verfügung stellen oder als Präsenzveranstaltung abhalten.

- Schulungs- und Sensibilisierungskonzepte
- kundenindividuell
- Implementierung in bestehende Schulungssysteme
- Schulungsvideos
- Schulung vor Ort

DTS Systeme GmbH
+49 5221 1013-000

DTS Systeme Münster GmbH
+49 251 6060-0

dts.de
info@dts.de