Aufgabe: Umsetzung Datenschutz und IT-Sicherheit

UNSERE GESCHÄFTSBEZIEHUNG ZUR TEC4NET BESTEHT SEIT DEM JAHR 2007.
ICH SCHÄTZE DIE ZUVERLÄSSIGKEIT UND DAS GROSSE PERSÖNLICHE ENGAGEMENT DER MITARBEITER.

Hendrik van den Berg, Geschäftsführer der Neos Ventures GmbH

UNSERE DIENSTLEISTUNGEN

Um IT-Systeme und sensible Bereiche vor Störungen oder böswilliger Manipulation wirkungsvoll zu schützen, reicht eine Abschottung nach außen alleine nicht aus. IT-Sicherheit muss vielmehr, als ein zentrales Thema in Ihrem Unternehmen verstanden werden und im Denken und Handeln aller Mitarbeiter verankert sein.

Damit diese Anforderungen wirkungsvoll umgesetzt werden können, führen wir gemeinsam mit Ihnen eine Risikoanalyse durch, erarbeiten eine IT-Security-Policy und entwickeln effektive technische und organisatorische Maßnahmen zur Sicherstellung des nötigen Sicherheitsniveaus gemäß der nötigen Compliance- oder Security-Standards.

Wir Implementieren diese Ergebnisse im Rahmen eines Informations-Sicherheits-Management-Systems (ISMS) mit kontinuierlichen Verbesserungsprozess (KVP) in Ihrem Unternehmen und begleiten Sie durch das anstehende Zertifizierungsaudit.

Wir bieten:

- → **EINFÜHRUNG (ISMS)**
- → **PROZESSDESIGN**
- → **DOKUMENTATION**
- → **AUDITIERUNG (ISO 19011)**
- → **ISO/IEC 27001**
- → **PCI-DSS**
- → **BSI IT-GRUNDSCHUTZ**

Rufen Sie uns an wir beraten Sie gerne.

IHR STARKER IT-PARTNER

tec4net GmbH
Lohenstraße 13
82166 Gräfelfing

T +49 89 54 04 36 30
F +49 89 54 04 36 31
info@tec4net.com

www.tec4net.com

tec4net

CONSULTING | IT-SECURITY | DATENSCHUTZ

IT-Security für Unternehmen

Die regelkonforme Umsetzung bis zur Zertifizierung

www.tec4net.com

IT-SECURITY

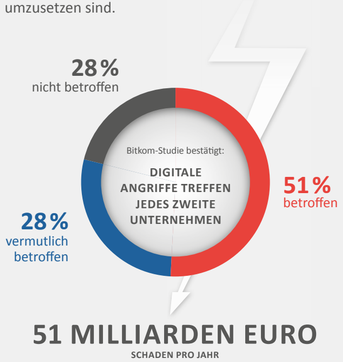
Sicherheit mit System

Die Absicherung komplexer Netzwerke und IT-Systeme ist für Unternehmen nicht nur lebensnotwendig sondern gerade wenn es um sensible Daten geht gesetzlich vorgeschrieben.

In der modernen Wissens- und Informationsgesellschaft sind Unternehmen bei der Verarbeitung von geschäftsrelevanten Daten auf IT-Systeme angewiesen. Die Informationstechnik erleichtert hierbei viele Prozesse bringt aber auch Risiken mit sich, da elektronisch verarbeitete Daten einer ständigen Bedrohung ausgesetzt sind.

Neben den zunehmenden Angriffen aus dem Internet, gilt es auch die Daten vor Verlust durch Diebstahl, äußere Einwirkungen oder menschliches Fehlverhalten zu sichern.

Zur Umsetzung wirkungsvoller Maßnahmen wurden verschiedene Sicherheitsstandards und Normen entwickelt, die von Unternehmen im Rahmen eines Informationssicherheits-Managementsystems (ISMS) umzusetzen sind.

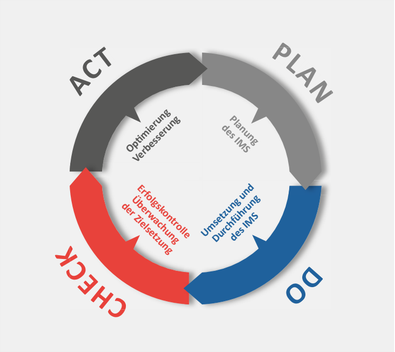


Durch die Implementierung eines Informationssicherheits-Managementsystems (ISMS) unterstützen wir Unternehmen dabei, Risiken die im Zusammenhang mit der Datenverarbeitung stehen zu identifizieren, zu Analysieren und auf systematische Weise abzustellen.

Nach erfolgreicher Implementierung begleiten wir Sie gerne durch das Zertifizierungsaudit, in welchem die Regelkonforme Umsetzung und Wirksamkeit des ISMS geprüft und bestätigt wird.

Vorteile einer Zertifizierung:

- → SENKUNG DER PROZESSKOSTEN
- → SENKUNG DER FINANZIERUNGSKOSTEN
- → SENKUNG DER VERSICHERUNGSBEITRÄGE
- → SENKUNG VON GESCHÄFTS- UND HAFTUNGSRISIKEN
- → STEIGERUNG DER WETTBEWERBSFÄHIGKEIT
- → IMAGEVERBESSERUNG BEI KUNDEN UND GESCHÄFTSPARTNERN



ISO/IEC 27001

Die internationale Norm ISO/IEC 27001 beschreibt die nötigen Anforderungen zur Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufenden Verbesserung eines dokumentierten Informationssicherheits-Managementsystems.

Darüber hinaus beinhaltet die Norm Anforderungen für die Beurteilung und Behandlung von Informationssicherheitsrisiken entsprechend den individuellen Bedürfnissen von Unternehmen. Die Norm spezifiziert Anforderungen zur Implementierung von geeigneten Sicherheitsmechanismen, welche an die Gegebenheiten der einzelnen Unternehmen adaptiert werden.

Säulen der Sicherheit:

- → PHYSIKALISCHE SICHERHEIT
- → PERSONELLE SICHERHEIT
- → SICHERHEIT DES IT-BETRIEBS
- → ZUTRITTS- UND ZUGANGSSCHUTZ
- → SICHERHEIT BEI DER ENTWICKLUNG
- → SICHERHEITSVORFÄLLE
- → VORGEHEN IM NOTFALL
- → COMPLIANCE

Ein nach ISO/IEC 27001 organisiertes ISMS ist vollständig kompatibel zu anderen Managementsystemen wie ISO/IEC 9001 Qualitätsmanagement (QM) oder ISO/IEC 20000-1 IT Service Management (ITSM).

Die Norm betrachtet drei wesentlichen Merkmale einer Information:

- **VERFÜGBARKEIT**
  Daten sind bei Bedarf verfügbar
- **VERTRAULICHKEIT**
  Zugriff nur für Berechtigte
- **INTEGRITÄT**
  Daten sind komplett und vertrauenswürdig

Diese Merkmale sind ebenfalls grundlegender Inhalt externen Anforderungen wie KontraG, Basel II, SOX oder die der Wirtschaftsprüfer.

Die Norm wird als Informationssicherheits-Managementsystems (ISMS) umgesetzt und gibt die Durchführung regelmäßiger Audits vor. Die wirkungsvolle Implementierung kann im Rahmen eines Audit nachgewiesen und anschließend durch ein Zertifikat bestätigt werden.

Wir bieten:

- → EINFÜHRUNG
- → RISIKOANALYSE
- → PROZESSDESIGN
- → DOKUMENTATION
- → AUDITIERUNG

PCI-DSS

Der Payment Card Industry Data Security Standard, ist ein Regelwerk im Zahlungsverkehr, das sich auf die Abwicklung von Kreditkartentransaktionen bezieht und von allen wichtigen Kreditkartenorganisationen unterstützt wird.

PCI basiert auf dem Visa-Account-Information-Security-Programm (AIS und dessen Schwesterprogramm CISP), dem MasterCard-Site-Data-Protection-Programm (SDP), der American Express Security Operating Policy (DSOP), der Discover Information Security and Compliance (DISC) und den JCB-Sicherheitsregeln.

Der Standard wird als Informationssicherheits-Managementsystem (ISMS) umgesetzt und gibt neben regelmäßigen Sicherheitsscans auch Audits vor. Der Nachweis der regelkonformen Umsetzung des Standards erfolgt durch wiederkehrende Zertifizierungsaudits, auf deren Grundlage das jeweils begrenzt gültige Zertifikat ausgestellt wird.

Wir bieten:

- → EINFÜHRUNG
- → RISIKOANALYSE
- → PROZESSDESIGN
- → DOKUMENTATION
- → AUDITIERUNG

BSI IT-GRUNDSCHUTZ

IT-Grundschutz bezeichnet eine vom Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelte Vorgehensweise zur Identifizierung und Umsetzen von Sicherheitsmaßnahmen in der Informationstechnik (IT) von Behörden oder Unternehmen.

Das Ziel des Grundschutzes ist das Erreichen eines mittleren, angemessenen und ausreichenden Schutzniveaus für IT-Systeme. Zum Erreichen des Ziels empfehlen die IT-Grundschutz-Kataloge technische Sicherheitsmaßnahmen und infrastrukturelle, organisatorische und personelle Schutzmaßnahmen.

Die empfohlenen Maßnahmen können als Informationssicherheits-Managementsystems (ISMS) umgesetzt werden. Die erfolgreiche Umsetzung kann anschließend im Rahmen eines Audit nachgewiesen und als ISO/IEC 27001-Zertifikat auf Basis des IT-Grundschutz bestätigt werden.

Wir bieten:

- → EINFÜHRUNG
- → RISIKOANALYSE
- → PROZESSDESIGN
- → DOKUMENTATION
- → AUDITIERUNG