Akademie für Informationssicherheit

der
HEGO Informationstechnologie GmbH

Seminarkatalog

Januar 2019 – Dezember 2019

Stand: 13.03.2019

Aufbau der Unterlage

Die HEGO Akademie bietet Seminare und Workshops in Bezug auf Informationssicherheit an. Hierzu gehören technische, organisatorische wie rechtliche Betrachtungen.

Die Seminare sind nach unterschiedlichen Zielen organisiert:

A Anwenderschulungen

C Corporate Social Responsibility

Q Qualifizierungsmaßnahme Digitalisierung und Sicherheit 2020

T Technisch orientierte Seminare zur Optimierung im Umgang mit technischen Lösungen

W Workshops

Inhaltsverzeichnis

Über uns

Die HEGO Informationstechnologie GmbH ist ein in 1997 gegründetes IT-Systemhaus mit Sitz in Wermelskirchen.

Das Unternehmen gliedert sich in zwei Bereiche: Das klassische HEGO Systemhaus, sowie die HEGO Akademie.

Ursprünglich als Dienstleistung des Systemhauses mit Einweisungen und Schulung der eingesetzten Produkte geplant, hat sich dieser Bereich so stark entwickelt, dass das Systemhaus diesen eigenen Zweig als Akademie im Jahr 2016 geplant und umgesetzt hat. In der Akademie werden heute Seminare zur allgemeinen IT-Weiterbildung angeboten, insbesondere in Bezug auf IT-Sicherheitsfragen.

Insgesamt bietet die Akademie der HEGO Informationstechnologie GmbH einen vollständigen Weiterbildungsrahmen für alle Hierarchien, von der Unternehmensleitung bis zur IT-Administration, denn zunehmend ist die Funktionsverfügbarkeit für ein Unternehmen lebensnotwendig. Mit diesem Konzept greifen die Sicherheitsaspekte für alle Beteiligten in allen Unternehmensprozessen.

Das Akademie-Konzept konzentriert sich deshalb auf

- Notwendige Umsetzungen von Gesetzesseite
- Konzepte zur Umsetzung
- Prävention gegen Angriffe jeder Art, von innen und außen
- Selbsthilfe im Notfall

Bei der Lösung dieser Aufgaben helfen wir Ihnen gerne!

Ihre Akademie der
HEGO Informationstechnologie GmbH

„A“

Anwenderschulungen

Organisatorische Maßnahmen umzusetzen ist die eine Sache, sie durchzusetzen die andere. Ohne für das Verständnis anstehender organisatorischer Maßnahmen geworben zu haben ist die Umsetzung schwierig, wenn nicht sogar unmöglich.

Und selbst wenn die Akzeptanz für anstehende Maßnahmen da ist, so ist doch auch dafür zu sorgen, dass die Anwender die Maßnahmen richtig umsetzen können.

Diese Thematik wird in einigen unserer Moduln angesprochen, und in einem Modul als gesondertes Thema „Compliance“ behandelt. Während sie dort Thema für die Umsetzung durch die Führungsebene ist, wird sie in diesem Kapitel hier für den Anwender „begreifbar“ gemacht.

Mit praktischen Beispielen versehen wird dem Anwender bewusst, auf was er zu achten hat, und wie er mit den organisatorischen Maßnahmen im Alltag umzugehen hat.

Der Gesetzgeber schreibt bezüglich der EU-Datenschutzgrundverordnung nachweisliche, regelmäßige Anwenderschulungen vor.

A01 – Der Umgang mit personenbezogenen Daten

Die EU-Datenschutzgrundverordnung ist seit dem 25.5.2018 in Kraft getreten, und die Verantwortung für die Einhaltung liegt bei der Unternehmensleitung. Doch die Verarbeitung personenbezogener Daten erfolgt im Alltag durch diejenigen Personen, die diese Daten verarbeiten.

Der Gesetzgeber schreibt, um sicherzustellen, dass die notwendige Wissensgrundlage vorhanden ist, regelmäßige Datenschutzschulungen der Anwender vor.

Zielgruppe	**Anwender**
Ziel	Lernen Sie die Grundsätze des neuen Datenschutzrechts, und auf was Sie im Alltag achten sollten um Verstöße zu vermeiden
Voraussetzung	Keine
Dozent	eine zertifizierte Fachkraft für Datenschutz
Dauer	4 Stunden
Verpflegung	keine

Inhalte

Dem Anwender wird zunächst erklärt, was personenbezogene Daten im Sinne der DSGVO sind. Dies ist für den Anwender u.U. nicht so schnell einsichtig, da die DSGVO auch technisch bedingte Daten als personenbezogen definiert. Im Anschluss werden die maßgeblichen Grundsätze der DSGVO erläutert, so dass der Anwender weiß, warum es die DSGVO gibt, und was der Gedanke des Datenschutzes grundsätzlich ist.
Nach einer kurzen Pause geht es in die Umsetzung: Wie ist bei der Verarbeitung personenbezogener Daten zu verfahren, worauf muss geachtet werden? Da personenbezogene Daten jedoch nicht nur auf die Speicherung in der Datenverarbeitung bezogen betrachtet werden dürfen, werden im Anschluss Hinweise zum Umgang mit Daten auf Papier, der Umgang mit Passwörtern sowie allerlei alltägliche Situationen besprochen.
Nach dem Seminar ist der Anwender auf die Notwendigkeit der Einhaltung datenschutzrechtlichen Handelns sensibilisiert, und das Risiko eines datenschutzrechtlichen Verstoßes ist wesentlich geringer.

Agenda

- Was sind personenbezogene Daten?
- Grundsätze der EU-Datenschutzgrundverordnung (DSGVO)
- Der Umgang mit personenbezogenen Daten
- Datenschutz am Arbeitsplatz
- Möglichkeit betriebsinterner Verhaltensregeln (Compliance)
- Zusammenfassung

HEGO
Informationstechnologie GmbH
Telegrafenstraße 8
D-42929 Wermelskirchen
T: +49 (0) 21 96 8 82 97 - 0
F: +49 (0) 21 96 8 82 97 - 23
info@hego-it.com
www.hego-it.com

„C“

Corporate Social Responsibility

Unter "Corporate Social Responsibility" oder kurz CSR ist die gesellschaftliche Verantwortung von Unternehmen als Teil des nachhaltigen Wirtschaftens zu verstehen. Gemeint ist die Verantwortung, die Unternehmen über die gesetzlichen Anforderungen hinaus freiwillig übernehmen.

Ziel ist die eine Strategie, welche darauf abzielt, in das Kerngeschäft soziale und ökologische Unternehmensverantwortung sowie nachhaltig ausgerichtetes Wirtschaften mit ökonomischem Erfolg einzubetten.
Bei CSR betrachten wir, wie die Gewinne erwirtschaftet werden, und begnügen uns nicht mit der Darstellung der Aktivitäten in den Bereichen Stiften, Spenden, Sponsern oder weiterer so genannter guter Taten.
Die Europäische Kommission hat die soziale Verantwortung der Unternehmen (Corporate Social Responsibility = CSR) definiert „als ein Konzept, das den Unternehmen als Grundlage dient, auf freiwilliger Basis soziale Belange und Umweltbelange in ihre Unternehmenstätigkeit und in die Wechselbeziehungen mit den Stakeholdern zu integrieren“.
Neben der EU-Leitlinie gibt es auch eine unverbindliche Norm für CSR. Die DIN ISO 26000 – Leitfaden zur gesellschaftlichen Verantwortung von Organisationen:
Diese Norm stellt einen Referenzrahmen für gesellschaftliche Verantwortung dar und hat mit den Kernthemen Organisationsführung, Menschenrechte, Arbeitspraktiken, Umwelt, faire Betriebs- und Geschäftspraktiken, Konsumentenanliegen sowie Einbindung und Entwicklung der Gemeinschaft einen umfassenden inhaltlichen Anspruch. Die Norm ist im Gegensatz zu Normen des Qualitäts- und Umweltmanagements nicht zertifizierbar und dient eher als Orientierungshilfe beim Aufbau eines Nachhaltigkeitsmanagements.
CSR fordert und fördert freiwillige Maßnahmen und eine Orientierung des Kerngeschäfts an sozialen, ökologischen und ethischen Indikatoren, welche deutlich über gesetzliche Vorgaben hinausgehen. Diese sollen in der Unternehmensführung und -tätigkeit sowie in den Wechselbeziehungen mit Stakeholdern im Inland, als auch im Ausland Berücksichtigung finden.

CSR – Corporate Social Responsibility

In dem im Oktober 2011 beschlossenen „Deutschen Nachhaltigkeitskodex (DNK)“ finden Unternehmen Hinweise und 20 Anforderungen für nachhaltiges Wirtschaften in Unternehmen aller Größen und Rechtsformen, mit denen sie ihre Leistungen messen und darstellen können. Durch den „Deutschen Nachhaltigkeitskodex“ soll erreicht werden, dass durch mehr Transparenz über Nachhaltigkeitsleistungen eine Vergleichbarkeit möglich ist. Grundlagen stellen die Kriterien der Global Reporting Initiative (GRI) und den ESG-Indikatoren der Europäischen Finanzprofi-Organisation EFFAS.

Zielgruppe	**Unternehmensführung**
Ziel	Lernen Sie, welche Vorteile Ihr Unternehmen mit Einführung von CSR hat
Voraussetzung	keine
Dozent	Christian Gollmer, Unternehmensberater
Dauer	1 Tag
Verpflegung	Mittagessen, Pausensnacks, Kaffee, Kaltgetränke inkl.

Inhalte

Nachhaltigkeit ist mehr als Umweltschutz und Energiesparen – es geht um neue Konzepte und Strategien für ihren langfristigen wirtschaftlichen Erfolg. Nachhaltiges Unternehmertum wird künftig immer öfter über Erfolg und Akzeptanz eines Unternehmens auf dem Markt und bei den Kunden entscheiden. Vernünftig und vorausschauend wirtschaften, mit dem Blick auf das Wohl der Beschäftigten, mit Verantwortung für Gesellschaft und Umwelt, das lohnt sich. Wer verantwortungsbewusst handelt, der lernt, unnötige Risiken zu vermeiden, Marktentwicklungen frühzeitig zu erkennen und sich langfristig für den Wettbewerb zu rüsten. All das legt die Basis für einen stabilen und dauerhaften Unternehmenserfolg.

CSR, die Strategie zur gesellschaftlichen Verantwortungsübernahme von Unternehmen, ist der wesentliche Treiber für die Entwicklung zukunftsfähiger Lösungen als Antwort auf die globalen Herausforderungen von Markt, Umwelt und Gesellschaft

In diesem Seminar werden die aktuellen Instrumente, die Inhalte und Arbeitsweisen von CSR vermittelt, damit Sie am Ende wissen, wie Sie CSR in Ihrem Bereich umsetzen können.

Agenda CSR

- Grundlagen von CSR
- Umsetzung von CSR im Unternehmen bzw. in der Non-Profit-Organisation
- Grundlagen des Nachhaltigkeitsberichtes
- Grundlagen der CSR-Strategie
- Fallbeispiele aus der Praxis

HEGO
Informationstechnologie GmbH
Telegrafenstraße 8
D-42929 Wermelskirchen
T: +49 (0) 21 96 8 82 97 - 0
F: +49 (0) 21 96 8 82 97 - 23
info@hego-it.com
www.hego-it.com

„Q“

Qualifizierungsoffensive „Digitalisierung und Sicherheit 2020“

Die Teilnehmer der Qualifizierungsoffensive werden in die Lage versetzt, die Notwendigkeit der Erfüllung kommender geschäftlicher Anforderungen bezüglich Datensicherheit, Datenschutz, sowie gesetzliche Neuerungen zu erfassen und für das eigene Unternehmen zu bewerten. Darüber hinaus sind sie in der Lage zu bewerten, welche Risiken bzgl. der Datensicherheit existieren, welche Maßnahmen möglich sind, und welche Chancen diese Maßnahmen bieten.

Nach dieser Qualifizierungsmaßnahme entscheidet der Unternehmer, inwieweit er den Weg zur Einführung eines Information Security Management Systems gehen will.

Parallel zu dieser Qualifizierungsmaßnahme können auf Wunsch jederzeit technische Maßnahmen zur Bewertung der eigenen Situation zur Datensicherheit durchgeführt werden, durch die die Qualifizierungsmaßnahme einen echten Bezug zur eigenen Situation erfahren kann.

Nach Kenntnis über ein Information Security Management Systems ist der Teilnehmer in der Lage zu beurteilen, welche Vorteile ein ISMS für das Unternehmen hat und welche Schritte er umsetzen möchte, falls er ein solches System in absehbarer Zeit nicht komplett umsetzen möchte. So kann er entscheiden, einzelne Schritte nach den Vorgaben, die für eine spätere Zertifizierung nötig sind, bereits jetzt umzusetzen.

Natürlich kann sich der Teilnehmer auch entscheiden alle Schritte bis zu einer möglichen Zertifizierung bereits zu gehen um anschließend eine ISO-Zertifizierung anzustreben. Die notwendigen Maßnahmen begleitet die HEGO Informationstechnologie GmbH mit ihren vom TÜV Rheinland zertifizierten IT-Sicherheitsbeauftragten, IT-Sicherheitsmanagern und IT-Sicherheitsauditoren.

In jedem Fall, auch bei Umsetzung der kleinsten Maßnahme, wird die Datensicherheit des Unternehmens verbessert werden, und das Unternehmen für die digitale Zukunft besser gerüstet sein. Die Dokumentation durchgeführter Maßnahmen wird das Unternehmen in die Lage versetzen, nachzuweisen, dass Maßnahmen zur Kontinuität des Unternehmens durchgeführt wurden, und somit die Bedingungen der unternehmerischen Sorgfaltspflicht erfüllen.

Q01 - Anforderungen an Unternehmer

Das erste Seminar unserer Qualifikationsmaßnahme wendet sich an die Unternehmensleitung, und beinhaltet die gesetzlichen und geschäftlichen Anforderungen, deren Erfüllung zur Digitalisierung der Geschäftsprozesse notwendig sind.

Zielgruppe	**Unternehmensführung, strategische IT-Leitung**
Ziel	Überblick über die Anforderungen zum Einstieg ins „Digitale Zeitalter“ – Risiken, Maßnahmen, gesetzliche Anforderungen
Voraussetzung	keine
Dozent	Ralf Gogolin
Dauer	1 Tag
Verpflegung	Mittagessen, Pausensnacks, Kaffee, Kaltgetränke inkl.

Inhalte

Schon heute sind Unternehmen von der Zuverlässigkeit Ihrer IT-Prozesse in hohem Maße abhängig. Der Ausfall eines IT-Prozesses kann ein Unternehmen zum vorübergehenden oder sogar endgültigen Stillstand zwingen.

Wie lange hält das Unternehmen durch, wenn IT-Prozesse ausfallen?

Welche IT-Prozesse sind in Ihrem Unternehmen existenziell wichtige Prozesse?

Wie erkennen Sie diese Prozesse, und worauf müssen Sie achten?

Die Politik hat darauf mit dem IT-Sicherheitsgesetz reagiert, aber nur wenige kennen es, und nur sehr wenige wissen, ob sie davon betroffen sind. Darüber hinaus hat die europäische Gesetzgebung mit der EU-Datenschutzgrundverordnung für eine Vereinheitlichung des Schutzes personenbezogener Daten eine neue, starke Grundlage geschaffen. Beide Gesetze greifen ineinander, und werden in den kommenden Jahren für alle Unternehmen ein zu erfüllender Standard sein.

Die Unternehmensführung ist für den reibungslosen Betrieb verantwortlich. Hier gilt es etablierte Methoden unter Berücksichtigung der neuen IT-Gesetze anzuwenden.

Dieses Seminar ist das Einstiegsseminar einer Reihe von sechs Seminaren. In diesem ersten Modul erhält die Unternehmensführung das notwendige Überblickwissen über die kommenden Anforderungen und die Möglichkeiten, diesen Anforderungen zu entsprechen.

Agenda Q01

- Beispiele aus Statistik und Praxis mit Diskussion
- Folgen mangelnder Sorgfalt:
    - Zugriff auf sensible Systeme
    - Cyber-Kriminalität am Beispiel Ransomware
- Das Umfeld der Informationssicherheit
    - Compliance
    - Gesetze und Normen heute
    - Awareness
    - Dokumentation
    - Datenschutz
    - Risiko- und Notfallmanagement
    - Was ist notwendig, was nicht?
- Einblick in neue Gesetze und Folgen der Nichtbeachtung
    - IT-Sicherheitsgesetz (IT-SIG / BSI-G)
    - EU Datenschutz-Grundverordnung (EU-DSGVO)
    - Zusammenhang zur gesetzlichen Sorgfaltspflicht
- Von der Einführung etablierter Methoden bis zur Zertifizierung
    - EC Council Penetration-Test
    - Quickcheck VdS, ISIS, ITQ13 u.a.
    - BSI Grundschutz
    - ISO 27001
    - Einführung eines ISMS

Q02 - Technische und organisatorische Umsetzungsmöglichkeiten

In der zweiten Qualifizierungsmaßnahme werden die IT-Verantwortlichen auf die Durchführung der notwendigen organisatorischen und technischen Maßnahmen vorbereitet. Sie lernen in diesem Modul die gesetzlichen und geschäftlichen Notwendigkeiten in angemessenem Umfang, insbesondere jedoch organisatorische und technische Umsetzungskonzepte und –möglichkeiten kennen.

Zielgruppe	**IT-Leitung / IT-Verantwortliche**
Ziel	Überblick über technische und organisatorische Möglichkeiten zur sicheren Umsetzung im Digitalisierungsprozess
Voraussetzung	Workshop W001 „Angriffsszenarien – Identifikation – Prävention“ oder vergleichbare Kenntnisse
Dozent	Jörg Hermanns
Dauer	1 Tag
Verpflegung	Mittagessen, Pausensnacks, Kaffee, Kaltgetränke inkl.

Inhalte

Schon heute sind Unternehmen von der Zuverlässigkeit Ihrer IT-Prozesse in hohem Maße abhängig. Der Ausfall eines IT-Prozesses kann ein Unternehmen zum vorübergehenden oder sogar endgültigen Stillstand zwingen.

Welche IT-Prozesse sind in Ihrem Unternehmen existenziell wichtige Prozesse?

Wie schützen Sie Ihre Systemumgebung gegen Ausfall, Manipulation oder Schadsoftware?

Wie können Sie die Sicherheit ihrer IT Systeme gewährleisten ohne den laufenden Betrieb zu sehr einzuschränken?

Gibt es für die Erfüllung der gesetzlichen Anforderungen Software auf dem Markt? Welche Software ist in welchem Umfeld notwendig oder ratsam, welcher Aufwand ist angemessen?

Welchen Nutzen bringt die Einführung eines ISMS auf Basis von bewährten Methoden und Vorgehensweisen?

Dieses Seminar ist das zweite Seminar in einer Reihe von sechs Seminaren. In diesem Modul erhält die IT Leitung das notwendige Überblickwissen über die kommenden Anforderungen an die IT Sicherheit sowie technische und organisatorische Konzepte und Möglichkeiten um diesen Anforderungen zu entsprechen.

Agenda Q02

- Beispiele aus der Praxis: Folgen mangelnder Sorgfalt:
- Technische und organisatorische Maßnahm der Informationssicherheit
- Compliance – Mit welchen Maßnahmen kann verhindert werden, dass
  - Schadsoftware unbemerkt den Weg in das interne Netzwerk findet
  - unbefugt Unternehmensdaten, bewusst oder unbewusst, das Unternehmen verlassen
  - Anwendungen über einen nicht befugten Kanal Daten austauschen
  - Schadsoftware wie Ransomware das gesamte Unternehmen befällt
- Awareness - Wie kann erreicht werden, dass Mitarbeiter
  - Schadsoftware in Mails erkennen
  - auf dem laufenden Stand aktueller Mailbedrohungen sind
- Ausfallsicherheit - Wie kann verhindert werden, dass das Unternehmen
  - bei Brand oder Stromausfall über eine kritische Dauer handlungsunfähig wird
  - wegen Internetausfall nur noch eingeschränkt handlungsfähig ist
  - Unternehmensdaten verloren gehen
  - In einem Notfall handlungsunfähig wird
- Prävention - Wie können Sie erreichen, dass
  - Ihre Anwendungen nicht manipulierbar sind
  - Schadsoftware vor Erreichen Ihres Postfachs ausgeschaltet wird
- Etablierte Methoden - vom Einstieg bis zur Zertifizierung
  - BSI, ISO27001
  - ISIS, VdS, ITQ13
  - Einführung eines Information Security Management Systems

Q03 - Informationssicherheit nach Recht und Gesetz

Unternehmenswichtige Daten müssen heute in nahezu allen Branchen jederzeit verfügbar sein, personenbezogene Daten müssen gemäß der Datenschutzgrundverordnung spätestens zum 25. Mai 2018 geschützt werden, wobei betroffenen Personen im Hinblick auf personenbezogene Daten eine Vielzahl an Rechten zusteht, bis hin zur Löschung ihrer Daten. Was ist also im Umgang mit Daten zu beachten? Was ändert sich durch die neue Datenschutzgrundverordnung der EU?
Die Akademie der HEGO Informationstechnologie GmbH gibt in Zusammenarbeit mit Herrn Rechtsanwalt Dr. Matthias Rudolph (FREY Rechtsanwälte) hierauf fundierte Antworten.

Zielgruppe	**IT-Leitung / IT-Verantwortliche**
Ziel	Überblick über die rechtlichen und organisatorischen Aspekte der Informationssicherheit
Voraussetzung	keine
Dozent	Ralf Gogolin / Dr. Matthias Rudolph, Frey Rechtsanwälte, Köln
Dauer	1 Tag
Verpflegung	Mittagessen, Pausensnacks, Kaffee, Kaltgetränke inkl.

Inhalte

Informationssicherheit bezieht sich darauf, unternehmensspezifische Daten und damit auch das Wissen, also das höchste Gut eines Unternehmens, gesichert verfügbar zu haben. Mit zunehmender Intensität wird die Daten- und Informationssicherheit sowohl vom Gesetzgeber als auch von den Kunden gefordert. Doch auch ohne „Druck von außen“, sollte die Daten- und Informationssicherheit jedem Unternehmen ebenso wichtig sein, wie der jeweilige Wert der Information selbst und der hierauf bezogene gesetzliche Schutz.

Unternehmen, die diese Anforderungen nicht beachten, laufen Gefahr gegen zahlreiche Gesetze zu verstoßen, Versicherungsschutz zu gefährden oder Kundenanforderungen nicht mehr gerecht zu werden.

Was ist zu beachten? Welche Konsequenzen drohen? Und wie können Unternehmen diesen Anforderungen genügen?

Agenda Q03

Dieses Seminar befasst sich mit dem Umgang mit personenbezogenen Daten aus rechtlicher sowie technischer Sicht.

- **Recht und Gesetz – Umgang mit personenbezogenen Daten**
  - **Einführung**
    Was sind „personenbezogene Daten“?
    Wer ist geschützt / wer ist verpflichtet?
  - **Die EU-Datenschutzgrundverordnung**
    Überblick: Was ist neu? Was bleibt erhalten?
    Die wichtigsten Pflichten eines Unternehmens als für den Datenschutz Verantwortlicher
  - **Datenschutzrechtliche Erlaubnistatbestände**
    Gesetzliche Erlaubnis
    Die Einwilligung und ihre Anforderungen
    Das Gebot der Datenvermeidung und der Datensparsamkeit
    Die Auftragsdatenverarbeitung
    Datenschutz in der betrieblichen Praxis und seine Anforderungen
    Anforderungen an die Datensicherheit
    Interoperabilität und Datenportabilität
    Der betriebliche Datenschutzbeauftragte und seine Aufgaben
  - **Compliance**
    Sind gesonderte Compliance-Regelungen im Unternehmen sinnvoll?
- **Best Practice**
  - **Mobilität von Daten: Die technische Umsetzung**
    Der Empfang und Versand von personenbezogenen Mails auf „mobile devices“: Was muss der Unternehmer berücksichtigen, um den Datenschutz einzuhalten?
    Welche Konsequenzen könnte der Verlust des mobilen Gerätes beinhalten?
    Was passiert mit den Daten, wenn der Mitarbeiter aus dem Arbeitsverhältnis ausscheidet?
  - **„Technische und Organisatorische Maßnahmen (TOMs)“**
    Welche TOMs kommen in der Praxis in Betracht? Wie werden sie praktisch umgesetzt? Was ist zu beachten?
  - **Kritische Infrastrukturen im Spiegel des IT-Sicherheitsgesetzes**
    Mindestanforderungen an die Datensicherheit kraft Gesetzes: „state of the art“;
    Wer ist von diesem Gesetz betroffen, wer nicht?
    Rechtsfolgen bei Nichtbeachtung: Was kann passieren, wenn ich den Anforderungen des Rechts nicht genüge?

Q04 - Compliance und Verarbeitungsverzeichnis

Nichts ist geregelt, wenn Regeln fehlen!

Über die Notwendigkeit von Compliance ist seit Jahren redlich gestritten worden – heute ist Compliance unternehmerische Notwendigkeit!

Compliance regelt das Verständnis der gesetzlichen und regulatorischen Verpflichtungen. Es stellt ein unternehmensweit verfügbares Nachschlagewerk dar, das beispielsweise auf die für das Unternehmen maßgeblichen Gesetze und Normen hinweist, aber auch und insbesondere die für die Organisation relevanten Auszüge dessen.

Zielgruppe	**IT-Leitung / IT-Verantwortliche**
Ziel	Überblick über die Anforderungen an ein internes Compliance-Handbuch
Voraussetzung	keine
Dozent	Ralf Gogolin / Dr. Matthias Rudolph, Frey Rechtsanwälte, Köln
Dauer	1 Tag
Verpflegung	Mittagessen, Pausensnacks, Kaffee, Kaltgetränke inkl.

Inhalte

Für die Mitarbeiter, Lieferanten und Kunden eines Unternehmens ist wichtig nachlesen zu können, wie die Anforderungen aus Gesetzgebung, Branchennormen, Verordnungen etc. umgesetzt werden. Die Compliance ist damit ein Spiegel der Wertvorstellungen eines Unternehmens.

Sanktionen bei Nichterfüllung sind Grundlage des sogenannten KVP, des Kontinuierlichen Verbesserungsprozesses. Etablierte Methoden zum Action Tracking, zur Durchführung von Compliance-Audits, sowie das Handling mit Alerts sind wichtiges und immer notwendigeres Werkzeug an Führungspositionen, die in einigen Ländern bereits längere Zeit vorgeschrieben sind, und nun EU-weiter Standard werden.

Eine Compliance fördert das bessere Verständnis der rechtlichen und regulatorischen Verpflichtungen im Unternehmen. Es reduziert Compliance-Risiken und die damit verbundenen Strafen, und ermöglicht dem Management, sich auf das Kerngeschäft zu konzentrieren.

Der Schwerpunkt in diesem Seminar betrachtet die Notwendigkeit, und konzentriert sich insbesondere auf den Umgang mit personenbezogenen Daten bei Einführung der DSGVO.

Agenda Q04

Dieses Seminar rund um das Thema „Compliance“ widmet sich der Zielsetzung Unternehmensrichtlinien zu erstellen, und dem Aufbau eines solchen Dokumentes. Insbesondere wird auf die umzusetzenden Regeln im Umgang mit personenbezogenen Daten eingegangen, um Risiken von Gesetzes- und Rechtsverstößen vorzubeugen.

Der Umgang mit einem Compliance-Handbuch

- Die Verfügbar des Handbuchs
- Bedingungen zur Umsetzung und Einführung
- Mögliche Komplikationen bei der Einführung
- Verfügbarkeit von Updates

Inhalt eines Compliance-Handbuchs

- Genereller Aufbau
- Dokumentationsnummern
- Revisionsverfolgung

Inhalt des Compliance-Handbuchs

- Umgang mit Gesetzen, Normen und Regeln
- Schwerpunkt: DSGVO

Verfahrensverzeichnis

- Aufbau- und Ablauforganisation
- Strukturanalyse
- Beschreibung eines Verfahrens
- GAP-Analyse
- Kontinuierlicher Verbesserungsprozess

Schwerpunkt „personenbezogene Daten“

- Umgang mit Daten gemäß Telemediengesetz
- Verwendung von Sozialdaten
- Umsetzung der DSGVO

Q05 - Risiko- und Notfallmanagement

Dieses Seminar behandelt die Themen Risiko- und Notfallmanagement. Beide Themengebiete greifen ineinander, und können deshalb nicht getrennt voneinander gesehen werden.
Durch die Höhe einer möglichen Strafe bei einem Datenschutzvorfall gewinnt das Risiko- und Notfallmanagement noch einmal erheblich an Bedeutung.

Zielgruppe	**IT-Leitung / IT-Verantwortliche**
Ziel	Risiken in der IT sowie im Datenschutz erkennen und bewerten, Notfälle planen, testen und vermeiden
Voraussetzung	Kenntnisse entsprechend Q03 und Q04, sofern Ihr Schwerpunkt Datenschutz betrifft, ansonsten keine
Dozent	Dmitri Sorokine, B.Sc.
Dauer	1 Tag
Verpflegung	Mittagessen, Pausensnacks, Kaffee, Kaltgetränke inkl.

Inhalte

Kennen Sie die Risiken, und wie bewerten Sie diese auf einer nicht von Emotionen getriebenen Ebene? Und wie erkennen und bewerten Sie Restrisiken?

Und wenn trotzdem etwas passiert: Wie lange dauert es bis Ihre IT wieder betriebsbereit ist? Was kostet diese Phase, ist sie überhaupt im Ernstfall zu bewältigen, oder sprengt sie den Rahmen dessen, was das Unternehmen bewältigen kann?

Wie groß war im Notfalltest die Wiederanlaufzeit? In welcher Reihenfolge müssen welche Prozesse wieder anlaufen, um die Wiederanlaufzeit so gering wie möglich zu halten, und welche Komponenten müssen wann zur Verfügung stehen, um diesen Plan umzusetzen?

Darüber hinaus schreibt die Datenschutzgrundverordnung (DSGVO) die Bewertung von Risiken im Datenschutz vor. Wie sind diese zu bewerten?
Und die DSGVO schreibt die Sicherheit der gespeicherten personenbezogenen Information vor. Hier schließt sich der Kreis: Ohne Risikomanagement und ohne Notfallplanung haben Sie keine Grundlage zur nachweislichen Vorsorge.

Erlernen Sie in diesem hochwertigen Seminar, wie Sie mit all diesen und weiteren Fragen umzugehen haben. Begleitend erhalten Sie ein aufwändig erstelltes und hochwertiges Handout mit detaillierten Erklärungen und Beispielen.

Agenda Q05

Risikomanagement

- Gefahr, Störung, Krise, Notfall, Katastrophe:
  Der BSI-Standard 100-4
- Die Messbarkeit von Risiken
- Arten von Risiken und deren Bewertung
- Risiken und die ISO 2700x-Familie
- Was ist ein Restrisiko, und wie geht man damit um?
- Der Risikoanalyse-Prozess
- Datenschutz-Risikomanagement

Notfallmanagement

- Was ist Notfallmanagement?
- Wie sieht eine Notfallorganisation aus?
- Die Business Impact Analyse
- Die Notfallvorsorge
- Incident Management
- Notfallplanung
- Notfallbewältigung

Risiken im Datenschutz

- Risikobezog in der DSGVO
- Risikobeurteilung in der DSGVO
- Das „angemessene Schutzniveau“
- Die Datenschutz-Folgeabschätzung
- Beispiele aus der Praxis

Fazit und Zukunftsaussicht

- Ein Ausblick

Q06 - Nutzen eines Information Security Management System

Alle genannten Maßnahmen aus den Moduln Q01 bis Q05 können in ein ineinandergreifendes System überführt werden, das es ermöglicht Informationssicherheit in einem Unternehmen „zu leben“.

Die Sicherheit der Daten und Informationen ist in einem Unternehmen, das ein Information Security Management System (ISMS) etabliert hat, organisiert und beständig.

Ein Unternehmen, das ein ISMS eingeführt hat, kann auf die Informationssicherheit zertifiziert werden. Dieser Schritt sichert letztendlich den Fortbestand im Umgang mit anderen Unternehmen. Zunehmend fordern Kunden von ihren Lieferanten die Garantie abgesicherter Geschäftsprozesse, um gewährleisten zu können, dass sie selbst unterbrechungsfreie Dienste leisten können – trotz Abhängigkeit von ihren Lieferanten. Im internationalen Business ist ein ISMS bereits gelebter Standard, der nun, und insbesondere durch die Einführung des IT-Sicherheitsgesetzes, der Datenschutzgrundverordnung sowie weiterer gesetzlicher Anforderungen, an Bedeutung gewinnt.

Darüber hinaus fragen Banken, Versicherungen, Wirtschaftsprüfer zunehmend nach der Etablierung angemessener Regeln, der Durchführung von Awareness-Maßnahmen, der Durchführung von Notfalltests usw., also nach all dem, was in unseren vorherigen Moduln bereits gezeigt wurde.

All diese Themen können in ein ISMS einfließen, und ergeben dort ein schlüssiges System. Mit einem laufend aktuell gehaltenen ISMS ist es ein Leichtes, Auskunft begehrenden Stellen die notwendigen Informationen zur Verfügung zu stellen, denn sie sind einfach vorhanden. Besonders interessant sind solche Systeme, wenn sie zudem auch ein DSMS, ein Datenschutzmanagementsystem – integrieren.

Kurzum: Je zeitnaher Sie die Einführung eines ISMS oder DSMS in Betracht ziehen, desto sicherer ist Ihr Unternehmen aufgestellt. Eines ist jedoch sonnenklar: Nichts zu tun ist für Ihr Unternehmen schädlich, und etwas zu tun, was nicht in ein langfristiges Konzept passt, ist nicht förderlich und muss früher oder später neu gemacht werden.

Beginnen Sie jetzt mit dem konzeptionellen Entwurf!

„T“

Technische Seminare

Die HEGO Akademie bietet technische Seminare an, die die Kunden in die Lage versetzen, das eingesetzte Produkt so weit kennen zu lernen, dass die Philosophie des Produktes und seine Funktionsweise verstanden, und somit in einem Störfall die Möglichkeit zur Selbsthilfe gegeben ist.

Führt die Selbsthilfe nicht zum gewünschten Erfolgt, so ist mit der erweiterten Kenntnis des Produktes jedoch eine ganz andere Möglichkeit im Dialog mit dem Dienstleister oder Hersteller möglich, beispielsweise wenn die Zusendung eines Logfiles zur weiteren Fehlerdiagnose notwendig wird.

Auf diese Weise rechnet sich der Besuch eines technischen Seminars zum eingesetzten Produkt sehr schnell.

T-F01 – FORTINET – FortiGate Basiskurs

Der FortiGate Basiskurs versetzt den Teilnehmer in die Lage, die FortiGate „richtig kennenzulernen“, optimal für seine Bedürfnisse einzusetzen, Anpassungen durchzuführen, sowie die Behebungszeit einer möglichen Störung durch tiefergehende Kenntnis des Produktes zu optimieren. Darüber hinaus ist er in der Lage einzuschätzen, welche Funktionen das System bereithält, die er eventuell noch nicht nutzt, die aber einen zusätzlichen Wert darstellen, beispielsweise wenn ein Betriebssystem-Update erweiterte Funktionen bereithält.

Zielgruppe	**IT-Administration**
Ziel	Überblick über erweiterte Einsatzmöglichkeiten, Optimierung im Störungsfall sowie möglichst eigenständige Administration
Voraussetzung	Grundkenntnisse über Netzwerke (TCP/IP, Firewalls, VPNs, Mailprotokolle, IDS / IPS)
Dozent	n.n.
Dauer	1 Tag
Verpflegung	Mittagessen, Pausensnacks, Kaffee, Kaltgetränke inkl.

Inhalte

- System Setup
- Warnmeldungen, Alarme und Logdateien
- Firewall Policies
- Antivirus Scanning
- Spamfilter
- Instant Message Filter
- FortiAnalyzer Reporting
- VPN-Einrichtung
- Störungsanalyse

„W“

Workshops

Die HEGO Akademie bietet Workshops und „Hands-On“-Schulungen im Bereich der Informationssicherheit an. In den folgenden Kapiteln finden Sie unsere aktuellen Angebote.

Aktuell wird dieser Bereich stark erweitert – wir werden im Laufe der kommenden Wochen weitere interessante und wichtige Module hinzufügen.

W01 - Angriffsszenarien, Identifikation, Prävention

Zielgruppe	**Technisch interessierte Geschäftsführung / IT-Leitung / IT-Verantwortliche**
Ziel	Wissen über aktuelle Angriffsmodelle und Bedrohungen
Voraussetzungen	Windows Server-Kenntnisse
Dozent	Jörg Hermanns
Dauer	1 Tag
Verpflegung	Mittagessen, Pausensnacks, Kaffee, Kaltgetränke inkl.

Inhalte

Nach „Locky“, „Goldeneye“ & Co. kommen neue Angriffsmodelle, wobei die alten weiterhin „unterwegs“ sind. Da macht es keinen Sinn „hier und da“ nachzubessern. Vielmehr ist jetzt präventives Handeln und ein umfassendes Wissen über die Zusammenhänge notwendig

- welche Angriffsszenarien es gibt,
- welche Ziele diese verfolgen,
- wie sie sich bemerkbar machen
- wie sie in Ihr System eindringen
- und was Sie präventiv und nachhaltig tun können

In unserem Workshop zeigen wir Ihnen live Beispiele aktueller Angriffsszenarien, zeigen und diskutieren Möglichkeiten der Kontrolle, und zeigen Ihnen den Weg wirksamer und langfristiger Prävention auf.

Im Ergebnis verstehen Sie, was die Zusammenhänge der Bedrohungsszenarien sind, und können sich präventiv bestmöglich schützen.

Agenda W01

- Tagesaktuelle Bedrohungen
- Infektionswege und Zugriffsmethoden aktuell aktiver Trojaner
- WLAN und LAN basierte Angriffe
    - Man-in-the-Middle Attacken
    - SSID Hijacking
    - ARP Spoofing
    - DNS Poisoning
    - DDoS Attacken
- Infektion durch Web-Surfen
    - Drive-by-Infections
- (Spear-) Phishing Attacken
    - Social Engineering
    - Schadcode per Mail
- Zugriff auf Smartphones
- USB-basierte Angriffe
    - „Rubber Ducky"
    - „Geiz ist geil"
    - "Das 32GB Dilemma"
- ISO, BSI und Awareness
- Offene Diskussion

W02 – Security Hacking

Zielgruppe	**Technisch interessierte Geschäftsführung / IT-Leitung / IT-Verantwortliche**
Ziel	Sensibilisierung über die Verletzlichkeit ungeschützter Daten
Voraussetzungen	keine
Dozent	n.n.
Dauer	2 Tage
Verpflegung	Mittagessen, Pausensnacks, Kaffee, Kaltgetränke inkl.

Inhalte

Welche Formen des Hacking gibt es? Wo sind ethische Grenzen?
Diskussionen wie die um eine Bewertung der Aktivitäten um Wikileaks zeigen, dass die ethischen Grenzen fließend sind. Welche Formen des Hacking gibt es, und sind sie schädlich oder nützlich? Wann ist Hacking ein Gesetzesverstoß und wann nicht?

Agenda W02

Tag 1

Die Motivation zum Hacking
Methoden:

- Security Scan
- Vulnerability Scan
- Penetrationtest

KALI Linux

- Ursprung, Idee und Motivation
- Ein Betriebssystem für Hacker oder Penetrationtester?

Information Gathering

Google Hacking

- Potentielle Risiken
- Suchoperationen

Tag 2

Scanning

- ICMP
- Grundlagen und Tools
- Auswertung der Ergebnisse
- Vulnerability Scanning
- Verifikation entdeckter Schwachstellen
- Ergebnisauswertung
- Erstellung des Abschlussberichts

Welche Ziele sind lohnenswerte Ziele für Angreifer?

Abschlussdiskussion

Die Referenten

Ralf Gogolin

Herr Ralf Gogolin wurde 1957 geboren, begann seine IT-Laufbahn 1979 bei einem international agierenden amerikanischen Computerhersteller als Technical Engineer, und war nach nur sechs Monaten für die Verfügbarkeit der IT der Kunden in NRW verantwortlich.

Berufsbegleitend studierte er DV-Organisation an der Deutschen Angestellten Akademie, Düsseldorf.

Nach Abschluss des Studiums zum DV-Organisator begleitete er verantwortlich die Herauslösung des deutschen Unternehmenszweiges durch Management By Out. Anschließend wechselte er in das Projektmanagement eines Systemhauses in Wermelskirchen. Dort lernte er Jörg Hermanns kennen, und gründete mit ihm 1997 die HEGO EDV- Beratung.

Das Unternehmen expandierte so stark, dass die beiden Gründer im Januar 1999 zur HEGO Informationstechnologie GmbH firmierten, und das Unternehmen in die Innenstadt von Wermelskirchen umzog.

Heute berät Herr Ralf Gogolin zahlreiche Firmen in strategischen und konzeptionellen Fragen, der langfristigen Planung und Umsetzung, sowie in Fragen der Informationssicherheit.

Herr Ralf Gogolin ist unter anderem IT-Compliance Manager sowie vom TÜV Rheinland zertifizierter und akkreditierter IT-Security Beauftragter, IT-Security Manager und IT-Security Auditor.

In zahlreichen visionären Vorträgen zeigt Herr Ralf Gogolin die künftigen Anforderungen an IT-Umgebungen und Informationssicherheit auf und referiert in zahlreichen Foren. Er ist Mitglied bei nrw_uniTS, dem Netzwerk des Horst-Görtz-Instituts für IT-Sicherheit an der Ruhr-Universität, Bochum, sowie Mitgründer der bundesweit vertretenen Expertengruppe für IT-Sicherheit.

Christian Gollmer

In seiner über 25-jährigen beruflichen Laufbahn war Christian Gollmer in unterschiedlichen Aufgabenbereichen in der Wirtschaft und im sozialen Sektor tätig. Seine kaufmännischen Grundlagen als gelernter Bankkaufmann konnte er in mehrjährigen Tätigkeiten im Vertrieb und Handel, durch umfangreiche Weiterbildungen als CSR-Berater, Projekt- und Qualitätsmanager permanent weiterentwickeln.

Als Sozialpädagoge B.A. gründete Christian Gollmer vor über 10 Jahren gemeinsam mit anderen Mitstreitern einen erfolgreichen sozialen Träger in der Jugendhilfe in Köln. Als geschäftsführender Vorstand verantwortete er vielfältige EU-, Bundes-, Landes- und Stiftungsprogramme in der Angebotspalette.

Durch verschiedenste Modell- und Koordinationsprojekte konnte sich Christian Gollmer in den letzten Jahren ein umfangreiches Netzwerk renommierter Sozialpartner aufbauen. Die enge Vernetzung mit Unternehmen, Ministerien, Stiftungen und sozialen Trägern erweitert die Expertise.

Grundlage der Beratung von Chistian Gollmer stellt der Leitfaden DIN ISO 26000 dar, der ersten globalen Norm für gesellschaftliche Verantwortung und Nachhaltigkeit.

Jörg Hermanns

Jörg Hermanns wurde 1970 geboren und hat sich bereits seit dem 14. Lebensjahr mit Computern befasst und erste Programme entwickelt.

Nach seinem Abitur hat er in Dortmund Informatik studiert. Bereits während des Studiums hat er in einem Systemhaus programmiert, in welchem er Ralf Gogolin kennen lernte. Zusammen mit diesem gründete er Anfang 1997 die HEGO EDV-Beratung.

Das Unternehmen expandierte so stark, dass die beiden Gründer im Januar 1999 die HEGO Informationstechnologie GmbH gründeten, und das Unternehmen in die Innenstadt von Wermelskirchen umzog.

Herr Hermanns ist technischer Geschäftsführer der HEGO und berät zahlreiche Firmen in strategischen Fragen, der langfristigen Planung und Umsetzung, sowie in allen sicherheitsrelevanten IT-Fragen.

Herr Hermanns ist unter anderem Certified Ethical Hacker des EC-Councils, sowie vom TÜV Rheinland zertifizierter und akkreditierter IT-Security-Beauftragter, IT-Security-Manager und IT-Security-Auditor.

Dr. Matthias Rudolph

Dr. Matthias Rudolph, Jahrgang 1972, ist Partner von FREY Rechtsanwälte Partnerschaft. Er studierte in Passau, Tours und Bonn. Während seines einjährigen Studienaufenthalts in Frankreich erwarb er ein Diplom im Bereich des Europarechts und der Europapolitik.

Nach dem ersten Staatsexamen im Jahre 1999 widmete er sich seiner Promotion und arbeitete für eine international tätige Anwaltssozietät in Düsseldorf (heute Beiten Burkhardt). Durch die Befassung mit einem filmrechtlichen Thema im Rahmen seiner Promotion spezialisierte er sich auf dem Gebiet des Urheber- und Filmrechts.

2003 legte er das zweite Staatsexamen ab und stellte seine Promotion fertig.

Herr Dr. Rudolph konzentriert sich auf die umfassende rechtliche Beratung und gerichtliche Vertretung von Mandanten in den Bereichen des Urheber- und Medienrechts, des gewerblichen Rechtsschutzes sowie des Telekommunikations- und Datenschutzrechts. Arbeitssprachen sind Deutsch, Englisch und Französisch.

Herr Dr. Rudolph ist Fachanwalt für Urheber- und Medienrecht und Lehrbeauftragter an der Hochschule Fresenius. Er ist Mitglied der Deutsch-Französischen Juristenvereinigung, des Freundeskreis der Düsseldorfer juristischen Fakultät e.V. und Mitinitiator des kölner forum medienrecht e. V. (kfm).

Herr Dr. Rudolph ist Mitautor des Beck’schen Onlinekommentars zum Urheberrecht Möhring/Nicolini (§§ 112-119 UhrG und Teil Insolvenzrecht) und des neuen Heidelberger Kommentars zur Datenschutz-Grundverordnung (§ 20 DS-GVO), veröffentlicht regelmäßig wissenschaftliche Beiträge und hält Vorträge zu aktuellen Themen des Urheber-, Medien-, Datenschutz- und Telekommunikationsrechts.

Dmitri Sorokine

Herr Dmitri Sorokine wurde 1990 geboren und begann seine IT-Laufbahn 2013. Er studierte IT Produkt Management an der Hochschule Furtwangen University, die für ihre Fakultät Informatik national und international bekannt ist.

Parallel zu seinem Studium arbeitete Herr Sorokine unteranderem am „Herkules IT-Projekt“ der deutschen Bundeswehr, im App-Support der Deutsche Bahn AG und erstellte Software-Entwicklungskonzepte für ein Softwarehaus.

Im Juli 2018 begann Herr Sorokine sein Arbeitsverhältnis als Technical Security Engineer bei der HEGO Informationstechnologie GmbH.

Zu Seinen Aufgaben gehören unteranderem die Beratung und Konzeptionierung von IT-Infrastrukturen, alle Tätigkeiten im Bereich Datenschutz als Datenschutzbeauftragter und das Halten von den Tagesseminaren Q05 „Risiko- und Notfallmanagement“ und Q06 „Nutzen eines Information Security Management System“ der HEGO Akademie.

Termine, Orte und Preise 1. Halbjahr 2019

[Tag] / [K = Köln, WK = Wermelskirchen]

2019							
	Jan	**Feb**	**Mrz**	**Apr**	**Mai**	**Jun**	**Preis[1]**
A01		12 / WK	12 / WK	09 / WK	07 / WK	04 / WK	350 €
Q01	10 / WK		07 / WK		14 / WK		590 €
Q02	17 / WK		14 / WK		16 / WK		590 €
Q03	31 / K		20 / K		23 / K		690 €
Q04		07 / K	28 / K			12 / K	690 €
Q05		14 / WK		04 / WK		13 / WK	790 €
Q06	24 / WK	21 / WK		11 / WK		27 / WK	790 €
W01	22 / WK	19 / WK	19 / WK	10 / WK	21 / WK	18 / WK	490 €
W02	auf Anfrage						
T-F01	auf Anfrage						

Termine, Orte und Preise 2. Halbjahr 2019

[Tag] / [K = Köln, WK = Wermelskirchen]

2019							
	Jul	**Aug**	**Sep**	**Okt**	**Nov**	**Dez**	**Preis**[1]
A01	02 / WK		03 / WK	02 / WK	05 / WK	03 / WK	350 €
Q01		27 / WK					590 €
Q02		29 / WK					590 €
Q03			05 / K	30 / K			690 €
Q04			11 / K		05 / K		690 €
Q05					07 / WK		790 €
Q06					14 / WK		790 €
W01	09 / WK	06 / WK	10 / WK	08 / WK	12 / WK	10 / WK	490 €
W02	auf Anfrage						
T-F01	auf Anfrage						

Alle Preise je Teilnehmer(in) bei Teilnahme an einem offenen Seminar.

[1] zzgl. aktuell gültiger MwSt.

Anmeldung zur Teilnahme

Bitte tragen Sie hier die Teilnahme an den gewünschten Seminare und Workshops ein.

Senden Sie das ausgefüllte Formular an akademie@hego-it.com oder per Fax an 02196 88297-23.

Modul	Name des Teilnehmers	Termin	Preis

Hiermit melde ich die oben genannten Personen verbindlich zu den jeweiligen Schulungen bzw. Workshops zu den genannten Bedingungen (siehe Katalogende) an.

Rechnungsadresse:

Firma / Kundennummer

Adresse

Name Datum Unterschrift / Stempel

E-Mail-Adresse

Inhouse-Seminare

Alle genannten Seminare können auch als Inhouse-Seminar durchgeführt werden.

Ein Inhouse-Seminar kann für Ihr Unternehmen wesentlich lukrativer sein, wenn mehrere Mitarbeiter an dem Seminar teilnehmen sollen, denn die Kosten geteilt durch die Teilnehmerzahl ist dann schnell wesentlich geringer als bei Teilnahme an einem offenen Seminar. Darüber hinaus entstehen nur für den Trainer Reise- und andere Nebenkosten, anstelle für jeden Teilnehmer.

Es lohnt sich also generell die Frage zu stellen, ob das Interesse an einem Seminarinhalt auch für andere Mitarbeiter des Unternehmens relevant, wichtig oder vielleicht auch nur interessant sein könnte.

Darüber hinaus wird das Thema unweigerlich für genau Ihren Bedarf sein, denn die Fragen, die die Teilnehmer stellen, sind dann ausschließlich Belange Ihres Unternehmens. Die Folge ist ein wesentlich intensiveres Seminar.

Einige Seminare sind, wie zum Beispiel eine Anwenderschulung, für ein Inhouse-Seminar besser geeignet.

Sind Sie an einem Inhouse-Seminar interessiert? Schreiben Sie uns eine Mail an akademie@hego-it.com.

Das Kleingedruckte

Anmeldung

Die Anmeldung zu unseren Seminaren erfolgt schriftlich anhand des Anmeldeformulars, das Sie im aktuellen Schulungskatalog finden. Die Anmeldung ist verbindlich.

Ort der Durchführung

Der Ort der Durchführung ist für den Ort geplant, der im Schulungskatalog genannt ist. Melden sich mehrheitlich Teilnehmer aus einem Ort an, der einem anderen Schulungsort näher oder besser erreichbar ist, so kann sich der Durchführungsort ändern.

Rechnungstellung

Nach der Buchung erhalten Sie eine Rechnung über die gesamte Seminargebühr.

Stornierung

Die Stornierung eines gebuchten Seminars 14 Tage oder länger vor Durchführungstermin erfolgt kostenfrei, innerhalb des Zeitraums 13 bis drei Tage vor Durchführung sind 50% der Gebühren zahlbar, bei drei Tagen oder kürzer vor Durchführung sind die vollen Seminargebühren zu zahlen.

Die HEGO Informationstechnologie GmbH kann bei zu geringen Anmeldezahlen, Krankheit des Dozenten und anderen Fällen vom Vertrag zurücktreten. Die HEGO Informationstechnologie GmbH wird in einem solchen Fall einen Ersatztermin für die Durchführung nennen. Der Kunde hat das Recht in diesem Fall ebenfalls vom Vertrag zurückzutreten und bereits geleistete Zahlungen zurück zu verlangen. Weitergehende Ansprüche des Kunden sind ausgeschlossen.