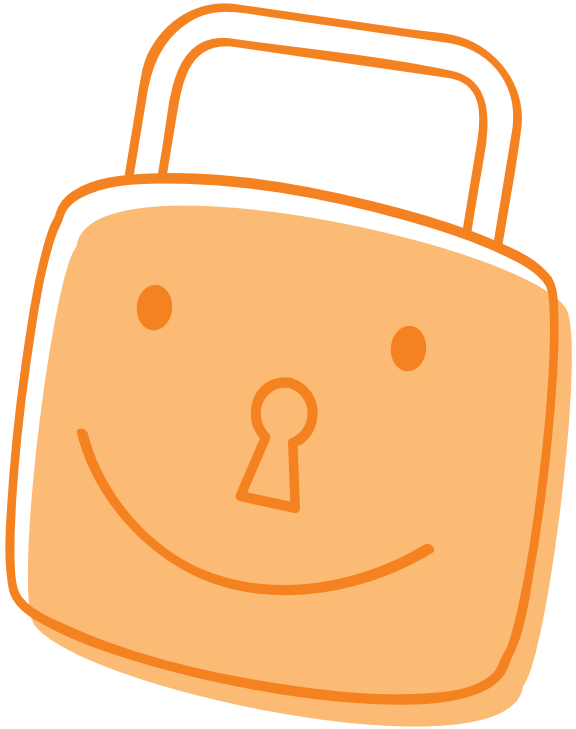
BIEG
Neutrale Online-Marketing-Beratung



# Informationssicherheit für kleine und mittlere Unternehmen

LEITFADEN

## Informationssicherheit für kleine und mittlere Unternehmen

IT-Sicherheit ist unverzichtbar für Unternehmen jeder Größe, doch die existierenden Standards und Rahmenwerke, die Unternehmen bei ihrer IT-Sicherheit helfen, sind wegen ihrer Komplexität und ihrem Aufwand für den Großteil der kleinen und mittleren Unternehmen nicht umsetzbar. Im Jahr 2015 wurde von der VdS Schadenverhütung mit den VdS-Richtlinien 3473 – Cyber-Security für kleine und mittlere Unternehmen ein neuer Mitspieler in diesem Bereich vorgestellt, der versucht, genau diese Kritikpunkte zu vermeiden. Die Richtlinien wurden im Jahr 2018 überarbeitet und in diesem Zuge in VdS 10000 umgetauft. Dieser Leitfaden gibt Ihnen einen Überblick.

## Informationssicherheitsmanagement

Um Informationssicherheit wirksam und nachhaltig umzusetzen, bedarf es eines sogenannten Informationssicherheitsmanagementsystems (ISMS), also einer strukturierten Vorgehensweise. In seinem Mittelpunkt steht der PDCA-Zyklus (auch: Demingkreis): PDCA steht für *Plan, Do, Check, Act* und beschreibt die sich immer wiederholenden Schritte, die Sie ergreifen müssen, um Informationssicherheit zu schaffen und zu erhalten. Die VdS 10000 beschreibt ein solches ISMS.

## Organisation der Informationssicherheit

Es müssen klare Verantwortlichkeiten für die Informationssicherheit definiert und die notwendigen Ressourcen (Geld, Personal, Wissen…) bereitgestellt werden. Dies kann nur durch das Topmanagement, also die „oberste Leitungsebene", die Geschäftsführung bzw. den Vorstand erfolgen. Denn hier liegt immer die Gesamtverantwortlichkeit für Informationssicherheit. Es bedarf also einer klaren Bekennung und Verpflichtung des Topmanagements zur Informationssicherheit, erst dann können die nächsten Schritte folgen.

## Rollen und Verantwortlichkeiten

Die zentrale Rolle im ISMS ist die des Informationssicherheitsbeauftragten (ISB). Er initiiert, plant, überwacht und steuert sämtliche Tätigkeiten in diesem Bereich. Er ist der Ansprechpartner für alle Mitarbeiter und für ihre Sensibilisierung verantwortlich. Ihm zur Seite gestellt ist das Informationssicherheitsteam (IST), das neben einem Vertreter des Topmanagements, dem ISB und dem IT-Verantwortlichen auch aus weiteren Vertretern des Personals und – sofern vorhanden – dem Datenschutzbeauftragten besteht. Es unterstützt den ISB bei seinen Aufgaben und ist für die Erstellung der Richtlinien zur Informationssicherheit (IS-Richtlinien) verantwortlich. Durch diese Zusammensetzung wird erreicht, dass möglichst viele Interessen im Unternehmen ausreichend Beachtung finden und umgekehrt das Thema Informationssicherheit in alle Bereiche des Unternehmens getragen wird. Dabei sollte neben dem notwendigen Fachwissen insbesondere auf Vertrauenswürdigkeit und das Ansehen der jeweiligen Person im Unternehmen geachtet werden.

Besonders in kleinen Unternehmen können diese Rollen von wenigen oder sogar ein und derselben Person besetzt werden, Interessenskonflikten sollten dabei jedoch möglichst vermieden werden. Sind die Verantwortlichkeiten schlussendlich zugewiesen, obliegt es dem Topmanagement, die Personen für die Erfüllung ihrer Aufgaben im ISMS von anderen Tätigkeiten im erforderlichen Maß freizustellen.

## Richtlinien zur Informationssicherheit

Das zentrale Dokument des ISMS ist die Leitlinie zur Informationssicherheit (IS-Leitlinie). In ihr bekennt und verpflichtet sich das Topmanagement zur Informationssicherheit, es werden die zu erreichenden Ziele mit den jeweiligen Verantwortlichkeiten definiert, und es wird auf die Konsequenzen ihrer Nichtbeachtung hingewiesen.

Daneben ist es erforderlich, weitere Vorgaben zu verabschieden und in einzelnen Dokumenten – den oben angesprochenen IS-Richtlinien – zu sammeln. Neben Regelungen für die Nutzer der IT sind dies z.B. Richtlinien für mobile IT-Systeme, mobile Datenträger und zur Datensicherung sowie Richtlinien, wie Sicherheitsvorfälle oder andere Störungen behandelt werden.

## Regelungen für Nutzer

Generell muss für Mitarbeiter die missbräuchliche oder gesetzeswidrige Nutzung von IT verboten werden; dies betrifft insbesondere das Abrufen oder Verbreiten von strafrechtlich relevanten oder sittenwidrigen Inhalten. Wenn Privatnutzung erlaubt wird, kann der Missbrauch rechtliche Konsequenzen für den Täter zur Folge haben; das betrifft insbesondere arbeits- und datenschutzrechtliche Verstöße. Diese Entscheidung sollte daher ausgiebig mit den Bedarfsträgern (z.B. auch mit dem Betriebsrat) diskutiert und anschließend schriftlich fixiert werden. Grundlegende Verhaltensregeln, wie das Verbot der Nutzung nicht freigegebener Hard- oder Software oder das Verbot der Weitergabe von Zugangsdaten müssen verständlich und unmissverständlich geregelt sein. Wichtig ist, dass auch Möglichkeiten für Ausnahmen existieren sollten, um allen geschäftlichen Anforderungen gerecht zu werden. Diese Regelungen sollten auch für Lieferanten und Dienstleister oder andere Externe Gültigkeit besitzen. Die Praxis zeigt, dass diese Personen oft ein Risiko für die eigene Informationssicherheit darstellen.

**BIEG-Leitfaden: Social Media am Arbeitsplatz**

Viele Unternehmen nutzen inzwischen Soziale Medien, sei es für Marketingzwecke, Unternehmenskommunikation oder Bewerbersuche. Wenn sich Mitarbeiter in ihrer Arbeitszeit mit Facebook, Twitter und Co. beschäftigen, stellt sich für den Arbeitgeber jedoch schnell die Frage: Was ist erlaubt, wo liegen die Grenzen und welche Risiken bestehen für das Unternehmen? Der BIEG-Leitfaden Social Media am Arbeitsplatz: Rechtliche Rahmenbedingungen nimmt Sie bei der Formulierung Ihrer Social-Media-Guidelines an ieHand.

www.bieg-hessen.de/leitfaeden



**Schutzziele der Informationssicherheit**

Vertraulichkeit: Informationen dürfen nur von Berechtigten eingesehen oder verarbeitet werden

Integrität: Informationen dürfen nicht verfälscht werden

Verfügbarkeit: Informationen stehen dann zur Verfügung, wenn sie benötigt werden

## Personal

Es muss geregelt werden, welche (sicherheitsrelevanten) Tätigkeiten bei der Einstellung sowie einem möglichen Wechsel und der Beendigung des Arbeitsverhältnisses erfolgen müssen. Die Vermittlung von Wissen in Bezug auf Informationssicherheit ist wesentlich: So sollte geregelt werden, dass das Personal über die Sicherheitsvorgaben des Unternehmens informiert wird und die entsprechenden Regelungen kennt und versteht. Bei dem Wechsel einer Anstellung, z.B. in eine andere Abteilung, muss sichergestellt werden, dass nicht mehr benötigte Zugriffsrechte entzogen werden, bei der Beendigung der Anstellung müssen Zugänge gesperrt oder gelöscht werden.

## Schutzziele

Informationssicherheit kennt drei maßgeblichen Schutzziele: Es muss sichergestellt werden, dass die Informationen nicht verfälscht werden (Integrität), dass Informationen dann zur Verfügung stehen, wenn sie benötigt werden (Verfügbarkeit) und dass Informationen nur von Berechtigten eingesehen bzw. verarbeitet werden können (Vertraulichkeit). Zu diesem Zweck müssen technische und organisatorische Maßnahmen

definiert, nach einem genauen Plan implementiert und regelmäßig auf ihre Wirksamkeit kontrolliert werden.

## Identifizieren kritischer IT-Ressourcen

Die Auswahl der geeigneten Sicherheitsmaßnahmen spielt dabei eine zentrale Rolle. Werden Maßnahmen zu groß oder zu umfangreich dimensioniert, ist das für das Unternehmen nicht wirtschaftlich. Wird zu wenig getan, steigt die Wahrscheinlichkeit eines Schadens. Ein risikobasiertes Vorgehen bei der Auswahl von Sicherheitsmaßnahmen ist daher der Königsweg.

Zunächst muss ermittelt werden, welche Geschäftsprozesse für das Unternehmen unerlässlich sind. Aus dieser „Business-Sicht" wird festgelegt, wie lange Geschäftsprozesse ausfallen dürfen, bis es zu einem katastrophalen Schaden kommt („Maximal tolerierbare Ausfallzeit", kurz MTA). Katastrophale Schäden entstehen z.B., wenn Menschen verletzt werden oder ums Leben kommen, wenn zentrale Werte des Unternehmens zerstört, Gesetze gebrochen werden oder die Schadenshöhe den Fortbestand des Unternehmens gefährdet.

Im nächsten Schritt wird die Kritikalität der Informationen des Unternehmens bestimmt. „Kritisch" kann für jedes Unternehmen unterschiedlich definiert werden. In jedem Fall sollten Informationen als kritisch gelten, wenn eine Verletzung der Schutzziele Vertraulichkeit, Integrität oder Verfügbarkeit wiederum zu katastrophalen Schäden für das Unternehmen führt („Kronjuwelen").

Sind kritische Geschäftsprozesse und kritische Informationen identifiziert, wird ermittelt, welche IT-Systeme diese Informationen verarbeiten, über welche Netzwerke die Informationen übertragen oder auf welchen mobilen Datenträgern diese Informationen gespeichert werden. Alle diese Komponenten sowie die unterstützende IT-Infrastruktur sind als kritisch einzustufen.

## Sicherheitsmaßnahmen

Durch die Unterscheidung in kritische und nicht-kritische Informationen und IT-Systeme können nun auf das jeweilige Risiko zugeschnittene Sicherheitsmaßnahmen ausgewählt und implementiert werden. Sie sind in folgenden Kategorien unterteilt:

- IT-Systeme (z.B. Server, Clients, Drucker, Mobiltelefone, Smartphones, Telefonanlagen, Laptops, Tablets, aktive Netzwerkkomponenten)
- Netzwerke und Verbindungen
- Mobile Datenträger (z.B. USB-Sticks, externe Festplatten)
- Physische Umgebung (z.B. Klimatisierung, Feuerschutz, Verkabelung)
- IT-Outsourcing und Cloud Computing
- Zugänge und Zugriffsrechte
- Datensicherung und Archivierung
- Störungen und Ausfälle
- Sicherheitsvorfälle

Für kritische IT-Systeme und besonders exponierte Komponenten, wie z.B. Firewalls, fordert die VdS 10000 die Durchführung eine Risikoanalyse. Bei diesem strukturierten Vorgehen wird ermittelt, welche Gefährdungen auf die kritischen IT-Komponenten einwirken können und welche

Auswirkung dies haben kann. Umso höher die Eintrittswahrscheinlichkeit eines Schadens und umso größer der zu erwartende Schaden ist, desto größer wird das Risiko. Große Risiken sollten in jedem Fall behandelt werden, z.B. durch weitere Sicherheitsmaßnahmen abgeschwächt oder durch Versicherungen kompensiert werden.

## Resümee

Informationssicherheit ist ein sich ständig wiederholender Prozess. Das Ziel ist, sie ständig zu verbessern und so die Risiken für das Unternehmen nachhaltig auf ein akzeptables Maß zu reduzieren. Mit den VdS-Richtlinien 10000 erhalten kleine und mittlere Unternehmen ein Kochrezept für die Erreichung dieses Ziels. Die dort beschriebenen Anforderungen sind kompatibel zu den Standards ISO 27001 und IT-Grundschutz, so dass bei Bedarf auf diese „aufgerüstet" werden kann. Die VdS-Richtlinien 10000 sind frei verfügbar und können kostenfrei auf der Homepage des VdS Schadenverhütung GmbH heruntergeladen werden.

### Checkliste: Sicherheitstipps

✓ Updates: Verfügbare Updates sollten zeitnah eingespielt werden. Dies betrifft nicht nur das Betriebssystem, sondern auch die installierte Software (Webbrowser, Office, PDF Reader, Medienplayer etc.).

✓ Schadsoftware: Der Schutz vor Schadsoftware (Antivirus) sollte auf möglichst allen IT-Systemen vorhanden sein. Auch wenn der Echtzeitschutz aktiviert ist, sind regelmäßige Komplettscans unerlässlich.

✓ Kennwörter: Keine leicht zu erratende Kennwörter verwenden. Groß-/Kleinbuchstaben, Zahlen, Sonderzeichen und mindestens 8 Zeichen sind das Minimum. Kennwörter nicht mehrfach verwenden (z.B. gleiches Kennwort für die Anmeldung am PC und im Onlineshop).

✓ Datenklassifizierung: Welche Informationen sind besonders wichtig und dürfen nicht in falsche Hände geraten? Identifizieren Sie Ihre „Kronjuwelen", schützen sie diese durch geeignete Maßnahmen (z.B. durch Verschlüsselung).

✓ Netzwerksegmentierung: Netzwerke je nach Vertrauenswürdigkeit voneinander trennen. Überlegen Sie, welcher Datenfluss zwischen LAN, WLAN, Internet etc. unbedingt notwendig ist. Firewalls unterstützen bei der Durchsetzung von Datenverkehrsbeschränkungen.

✓ Notfallbewältigung: Überlegen Sie sich im Vorfeld, was bei Störungen oder Ausfällen zu tun ist, um wieder normal arbeiten zu können. Umso schneller dies wieder möglich ist, desto geringer der Schaden.

**Links**

Die VdS-Richtlinien 10000 zum freien Download
www.vds.de/cyber

BSI IT-Grundschutz
www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

Download aller BIEG-Leitfäden unter
**www.bieg-hessen.de**

Stand: Februar 2019

Über den Autor

**Michael Wiesner**
Michael Wiesner GmbH

Michael Wiesner unterstützt seit 25 Jahren Unternehmen bei der Absicherung ihrer Informationen und IT-Infrastrukturen. Er ist Co-Autor der VdS-Richtlinien 10000 für Cyber-Security in KMU sowie VdS 10010 zur Umsetzung der europäischen Datenschutzgrundverordnung (DSGVO), gefragter Dozent, Impulsgeber und Live Hacker.

**www.wiesner.eu**

## Impressum

**Herausgeber**

**BIEG Hessen GbR**
**Beratungs- und Informationszentrum**
**elektronischer Geschäftsverkehr Hessen GbR**
c/o IHK Frankfurt am Main
Börsenplatz 4 | 60313 Frankfurt am Main
Telefon: +49 (0)69 2197-1380 | Telefax: +49 (0)69 2197-1497
info@bieg-hessen.de | www.bieg-hessen.de

**Das BIEG Hessen ist eine Gesellschaft bürgerlichen Rechts und wird durch folgende persönlich haftende Gesellschafter vertreten:**

**IHK Frankfurt am Main** vertreten durch den Präsidenten Prof. Dr. Mathias Müller und den Hauptgeschäftsführer Matthias Gräßle
Börsenplatz 4 | 60313 Frankfurt am Main

**IHK Fulda** vertreten durch den Präsidenten Bernhard Juchheim und den Hauptgeschäftsführer Stefan Schunck
Heinrichstraße 8 | 36037 Fulda

**IHK Hanau-Gelnhausen-Schlüchtern** vertreten durch den Präsidenten Dr. Norbert Reichhold und den Hauptgeschäftsführer Dr. Gunther Quidde
Am-Pedro-Jung-Park 14 | 63450 Hanau

**IHK Offenbach am Main** vertreten durch die Präsidentin Kirsten Schoder-Steinmüller und den Hauptgeschäftsführer Markus Weinbrenner
Frankfurter Str. 90 | 63067 Offenbach am Main

**IHK Wiesbaden** vertreten durch den Präsidenten Dr. Christian Gastl und die Hauptgeschäftsführerin Sabine Meder
Wilhelmstr. 24-26 | 65183 Wiesbaden

Die Führung der laufenden Geschäfte des BIEG Hessen obliegt der IHK Frankfurt am Main.

**Verantwortlich für den Inhalt**
Detlev Osterloh, Geschäftsführer
BIEG Hessen, IHK Frankfurt am Main | Börsenplatz 4 | 60313 Frankfurt am Main
Telefon: +49 (0)69 2197-1380 | Telefax: +49 (0)69 2197-1497
detlev.osterloh@bieg-hessen.de

**Druck:** Daab Druck & Werbe GmbH, Reinheim

**Layout und Titelbild:** Birgit Dürr




## Informationssicherheit für kleine und mittlere Unternehmen

Dieser Leitfaden gibt Ihnen einen Überblick über die VdS-Richtlinien *3473 – Cyber-Security für kleine und mittlere Unternehmen*: eine Sicherheitsrichtlinie, die speziell entwickelt wurde, um kleinen und mittleren Unternehmen auf dem Weg zu mehr Informationssicherheit eine Anleitung an die Hand zu geben. So wappnen Sie sich gegen Risiken und wirtschaftliche Schäden.


Träger des BIEG Hessen | Industrie- und Handelskammern:
Frankfurt am Main| Fulda | Hanau-Gelnhausen-Schlüchtern | Offenbach am Main



HERAUSGEBER

BIEG Hessen
c/o IHK Frankfurt am Main
Börsenplatz 4
60313 Frankfurt am Main

Telefon 069 2197-1380
Telefax 069 2197-1497
info@bieg-hessen.de
www.bieg-hessen.de