Mehr Sicherheit für Ihr Unternehmen

Nur wer seine Risiken kennt, kann auch vorausschauend und verantwortungsbewusst handeln. Das gilt insbesondere für Unternehmen, die einer Vielzahl von rechtlichen Regularien und technischen Anforderungen unterworfen sind. Insbesondere die IT ist heute häufig Dreh- und Angelpunkt in Unternehmen mit hohen Anforderungen an Sicherheit, Zuverlässigkeit und Haftungsaspekten.

Ein IT-Sicherheitskonzept kann hier helfen, bereits im Vorfeld ganzheitlich Risiken zu erkennen, zu bewerten und mögliche Schäden vom Unternehmen abzuwenden.

„Als Kunstschmiedebetrieb leben wir von der Individualität unserer Gestaltung und der Einzigartigkeit unserer Produkte. Entwürfe und Konstruktionszeichnungen, die wir mit unseren Kunden austauschen, sind für uns Güter von hohem Wert. Bislang haben wir schon einiges für den Schutz unserer Daten und Systeme getan. Nicht zuletzt geht es darum, etwaige Haftungsrisiken auszuschließen und für unsere Kunden verfügbar zu sein. Daher werden wir das Thema systematisch und ganzheitlich angehen, um schrittweise einen angemessenen Schutz zu erreichen."

Michael Haase, Inhaber
Kunstschmiede und Werkstatt
für Metallgestaltung, Krefeld

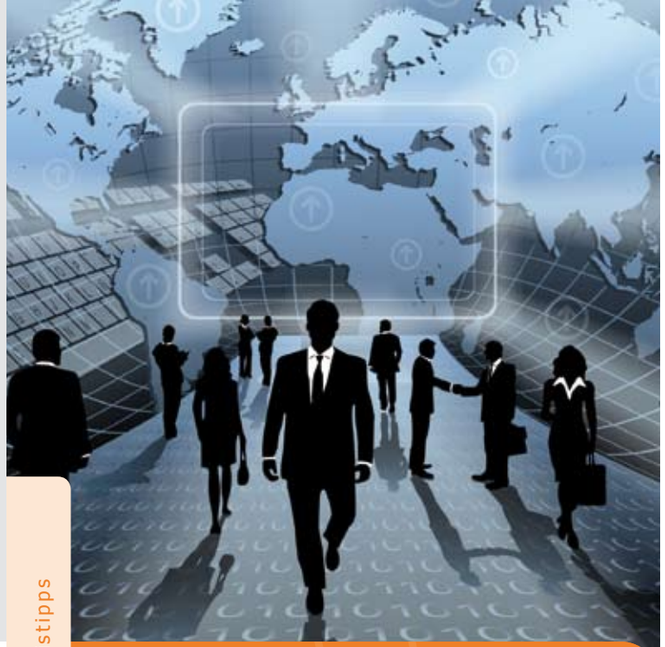
Regionales Kompetenzzentrum
Branchen-Kompetenzzentrum
Externer Netzwerkpartner

Das Netzwerk Elektronischer Geschäftsverkehr

Seit 1998 berät und begleitet das Netzwerk Elektronischer Geschäftsverkehr, in 27 über das Bundesgebiet verteilten regionalen Kompetenzzentren und einem Branchenkompetenzzentrum für den Handel, Mittelstand und Handwerk bei der Einführung von E-Business Lösungen. In dieser Zeit hat sich das Netzwerk mit über 30.000 Veranstaltungen und Einzelberatungen mit über 300.000 Teilnehmern als unabhängiger und unparteiischer Lotse für das Themengebiet „E-Business in Mittelstand und Handwerk" etabliert. Das Netzwerk stellt auch Informationen in Form von Handlungsanleitungen, Studien und Leitfäden zur Verfügung, die auf dem zentralen Auftritt www.ec-net.de heruntergeladen werden können. Die Arbeit des Netzwerks wird durch das Bundesministerium für Wirtschaft und Technologie gefördert.

Netzwerk Elektronischer Geschäftsverkehr

www.ec-net.de



Praxistipps

Aus der Praxis für die Praxis

IT-Sicherheits-konzept erstellen

10 Praxistipps für kleine und mittlere Unternehmen und das Handwerk

Gefördert durch:

Bundesministerium
für Wirtschaft
und Technologie

aufgrund eines Beschlusses
des Deutschen Bundestages

Netzwerk Elektronischer
Geschäftsverkehr

TeleTrusT

TeleTrusT – Bundesverband IT-Sicherheit e.V. ist Partner des Begleitprojektes „Sichere E-Geschäftsprozesse in KMU und Handwerk" des Netzwerkes Elektronischer Geschäftsverkehr und veranstaltet bundesweit „Stammtische" rund um das Thema Informationssicherheit.

TeleTrusT ist mit mehr als 130 Mitgliedern aus Wirtschaft, Wissenschaft und Verwaltung ein führendes Kompetenznetzwerk in Fragen der IT-Sicherheit in Deutschland und Europa.

TeleTrusT
Pioneers in IT security.

Impressum

Seit 1998 berät und begleitet das Netzwerk Elektronischer Geschäftsverkehr in 27 über das Bundesgebiet verteilten regionalen Kompetenzzentren und einem Branchenkompetenzzentrum für den Handel, Mittelstand und Handwerk bei der Einführung von E-Business-Lösungen.

Herausgeber:
TeleTrusT – Bundesverband IT-Sicherheit e.V.,
Chausseestraße 17, D-10115 Berlin

Konzeption und Redaktion:
Hans-Joachim Bierschenk, Harald Kesberg

Grafik und Gestaltung:
Karl-Heinz Kottenhahn

Druck:
Buersche Druck- und Medien GmbH

Bildnachweis:
artcop/Fotolia.com, NAN/Fotolia.com,
xiaoliangge/Fotolia.com

Stand: 12/2011

10 Tipps, die wirklich helfen

Wie können Sie ein ganzheitliches IT-Schutzkonzept einrichten?

10 grundlegende Praxistipps helfen, vorbeugend Schäden von Ihrem Unternehmen abzuwenden.

Die Tipps stammen aus der betrieblichen Praxis kleiner und mittlerer Unternehmen und dem Handwerk. Sie wurden in enger Zusammenarbeit mit Unternehmen erarbeitet. Weiterführende Informationen und Tipps rund um das Thema finden Sie unter www.ec-net.de und www.kmu-sicherheit.de.

Ein IT-Sicherheitskonzept kann helfen, vorausschauend zu handeln und mögliche Schäden für das Unternehmen zu vermeiden.

Was muss ich bei einem IT-Sicherheitskonzept beachten?

Verantwortlichkeiten

Der Erfolg des IT-Sicherheitskonzeptes beruht zum großen Teil darauf, dass seine Erstellung und Umsetzung in den richtigen Händen liegt.

Tipp 1: Verantwortlichkeiten festlegen
Legen Sie Verantwortlichkeiten fest, beachten Sie aber, dass die Geschäftsführung die letztendliche Verantwortung hat. Bestimmen Sie, welcher Mitarbeiter sich in welchen Bereichen um die Umsetzung und Aktualisierung des Konzeptes kümmern soll. Achten Sie dabei auf die fachliche Eignung des Mitarbeiters.

Tipp 2: Vorgaben sorgfältig beachten
Achten Sie als Verantwortlicher darauf, dass die Vorgaben aus dem Konzept auch eingehalten werden. Überprüfen Sie dies regelmäßig.

Gesetze und Regeln

Bei der Umsetzung des IT-Sicherheitskonzeptes müssen Sie auch die einschlägigen Gesetze und Regeln beachten. Dazu zählen z.B. das Bundesdatenschutzgesetz (BDSG) und das Handelsgesetzbuch (HGB) sowie zahlreiche weitere Bestimmungen und Verordnungen.

Tipp 3: Gültige Softwarelizenzen
Beachten Sie, dass für die von Ihnen eingesetzte Software auch gültige Lizenzen vorliegen.

Tipp 4: Aufbewahrungsfristen beachten
Informieren Sie sich über die Aufbewahrungsfristen von Daten und halten sie diese konsequent ein. Sorgen Sie insbesondere dafür, dass die Fristen auch technisch (z.B. Haltbarkeit von Datenträgern) eingehalten werden können.

Wie erfasse ich mögliche Risiken und Bedrohungen?

Gefahren erkennen

Sie sollten genau wissen, welchen Gefahren, Bedrohungen und Risiken Ihre IT ausgesetzt ist. Dazu sollten in einer Übersicht festgehalten werden, welche wichtigen IT-Anwendungen, Dienste und Informationswerte wo und wie genutzt werden.

Tipp 5: IT-Infrastruktur dokumentieren
Erstellen Sie die Übersicht in tabellarischer Form und berücksichtigen Sie auch alle Arten von externen Dienstleistungen.

Bedrohungen analysieren

Mögliche Bedrohungen, wie z.B. höhere Gewalt, vorsätzliche Handlungen, Fahrlässigkeit oder Fehlbedienungen sind abzuschätzen und in der Übersicht zu dokumentieren.

Tipp 6: Gefahrenpotenziale einordnen
Erfassen Sie die Bedrohungen systematisch nach Verlust der Verfügbarkeit, der Integrität (z.B. Unversehrtheit) und der Vertraulichkeit.

Risiken bewerten

In die Risikoabschätzung gehen die Bestandsaufnahmen, Bedrohungsanalysen sowie die Wichtigkeit und Sensibilität der Daten ein. Die möglichen Auswirkungen und die Wahrscheinlichkeit des Eintretens der Bedrohung bestimmen die Schutzbedürftigkeit von Daten, Software und Hardware.

Tipp 7: Schutzbedarfe ermitteln
Zur Bestimmung der Schutzbedarfe können Sie in vielen Fällen die Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zu Rate ziehen.

Welche Schutzmaßnahmen sollte ich berücksichtigen?

Felder der IT-Sicherheit

Das IT-Sicherheitskonzept sollte eine Reihe von unterschiedlichen Regelungen beinhalten. Eine wichtige Schutzmaßnahme ist die Reduzierung der Risiken durch menschlichen Irrtum, Diebstahl, Betrug oder Missbrauch der Einrichtungen.

Tipp 8: Mitarbeiter sensibilisieren
Die Mitarbeiter sollten, ggf. durch Schulung, die Bedrohungen und Risiken verstehen und ihre Verantwortlichkeiten und den Umgang mit der IT kennen.

Der Schutz der Infrastrukturen beinhaltet die Verhinderung von unberechtigtem Zugang zu Gebäuden und Räumen, der Beschädigung von Kommunikationsanlagen und Informationsträgern und die Störung der Geschäftsabläufe.

Tipp 9: Umfassenden Schutz sicherstellen
Die Sicherheitsmaßnahmen sollten sowohl vor menschlichen Aktivitäten als auch vor höherer Gewalt schützen.

Zur technischen Sicherheit gehören z.B. die Zugriffskontrolle, die Wartung der Hard- und Software, die Inbetriebnahme neuer Systeme und die Datensicherung.

Notfallplanung

Bei einem Schaden hilft eine Notfallplanung, um die IT schnellstens wieder ans Laufen zu bringen.

Tipp 10: Detaillierte Notfallpläne erstellen
Entwickeln Sie detaillierte Notfallpläne für wichtige Prozesse und halten Sie diese in Papierform vor.