IT-Sicherheit durch Mitarbeiter

Immer mehr Unternehmen wissen inzwischen um die Gefahren aus dem Internet. Vorbeugend setzen sie häufig auf technische Lösungen wie etwa Firewalls oder Virenscanner. Das ist sehr hilfreich, das alleine reicht aber noch nicht aus.

Wenn die eigenen Mitarbeiter über IT-Sicherheitsrisiken nicht oder nur unzulänglich informiert sind und dadurch sorglos und nachlässig mit Daten, Programmen und Rechnern umgehen, helfen auch die besten technischen Schutzmaßnahmen nicht.

Das menschliche Handeln ist zu einem Risiko geworden: Unvorsichtiges Herunterladen von Daten und Programmen aus dem Internet, die Nutzung von infizierten Laptops, USB-Geräten oder Smartphones oder etwa der sorglose Umgang mit Passwörtern oder Email-Anhängen können wichtige Unternehmensdaten gefährden.

Sensibilisierung der Mitarbeiter hilft

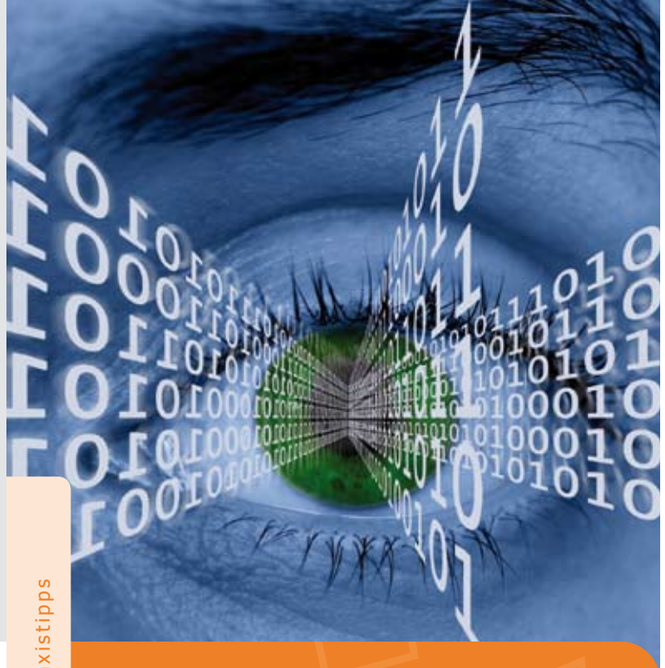
Die Mitarbeiter spielen eine entscheidende Rolle für den sicheren Umgang mit der IT. Sollen sie in den entscheidenden Momenten richtig handeln, müssen sie ein grundlegendes Verständnis für die Bedeutung von IT-Sicherheit haben. Hilfreich ist es, Mitarbeiter zu schulen und über mögliche Gefahrenquellen zu informieren. Machen Sie Ihre Mitarbeiter zu einem Aktivposten für Ihre IT-Sicherheit.

Das Netzwerk Elektronischer Geschäftsverkehr

Seit 1998 berät und begleitet das Netzwerk Elektronischer Geschäftsverkehr, in 28 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 unparteilicher 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-Sicherheit – Faktor Mensch

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 Deutschland 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 100 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 28 über das Bundesgebiet verteilten regionalen Kompetenzzentren und einem Branchenkompetenzzentrum für den Handel, Mittelstand und Handwerk bei der Einführung von E-Business-Lösungen.

Herausgeber:
TeleTrusT Deutschland e.V., Chausseestraße 17, D-10115 Berlin

Konzeption und Redaktion:
Hans-Joachim Bierschenk, Harald Kesberg

Grafik und Gestaltung:
Karl-Heinz Kottenhahn

Druck:
Buersche Druckerei Neufang KG

Bildnachweis:
bellemedia/fotolia.de, Miqul/Fotolia.com, Nmedia/fotolia.de

Stand: 07/2011

10 Tipps, die wirklich helfen

Mitarbeiter für IT-Sicherheit sensibilisieren

10 grundlegende Praxistipps helfen Ihnen, Ihre Mitarbeiter für einen sicheren Umgang mit der Unternehmens-IT fit zu machen.

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 Datensicherung und Datensicherheit finden Sie unter www.ec-net.de und www.kmu-sicherheit.de.

Mitarbeiter zu schulen und über mögliche Gefahrenquellen zu informieren hilft, IT-Sicherheitsrisiken zu reduzieren.

Wie erkenne und vermeide ich Risiken im Unternehmen?

Technische Sicherheitsmaßnahmen wie Firewalls und Virenscanner oder organisatorische Schutzmaßnahmen wie die Vergabe von Zugriffsrechten sind die Grundlage für ein sicheres Arbeiten mit der IT. Doch ein umfassender Schutz ist erst dann möglich, wenn auch das Verhalten der Mitarbeiter in puncto IT-Sicherheit berücksichtigt wird.

Bevor Sie Ihre Mitarbeiter über mögliche Gefahrenquellen und den richtigen Umgang mit Daten informieren, sollten Sie sich in einem ersten Schritt selbst einen Überblick verschaffen, wo Risiken für Ihre IT bestehen.

Tipp 1: Ermittlung schutzbedürftiger Daten
Ermitteln Sie Ihre schutzbedürftigen Daten (z.B. Personaldaten, Angebote, Rechnungen oder technologische Daten) und legen Sie fest, wer darauf Zugriff hat und haben sollte. Achten Sie darauf, dass die Daten nur demjenigen Mitarbeiter zugänglich sind, der sie auch wirklich benötigt.

Tipp 2: Regeln für den sicheren Umgang
Nachdem Sie die Risiken erfasst haben, sollten Sie für jede Nutzergruppe schriftliche Regeln für den sicheren Umgang aufstellen: verantwortungsvoll mit Passwörtern umgehen, nicht auf jeden Button von Webseiten klicken oder nicht auf unbekannte Links aus Emails klicken, etc. Dabei gilt: je einfacher, desto besser. Ziehen Sie ggf. einen externen Berater hinzu.

Tipp 3: Verantwortlichkeiten festlegen
Benennen Sie Mitarbeiter, die in Ihrem Unternehmen für die unterschiedlichen Sicherheitsaufgaben verantwortlich sind und z.B. die regelmäßige Sicherung der Daten und die Aktualisierung der Schutzsoftware durchführen.

Wie spreche ich meine Mitarbeiter richtig an?

Am besten lernt, der aus eigenem Interesse und mit Freude lernt. Gefragt sind daher praktische Beispiele, die die Risiken im Unternehmen anschaulich aufzeigen und entsprechende Lösungen anbieten. Motivieren und befähigen Sie Ihre Mitarbeiter zu mehr Eigenverantwortlichkeit im Umgang mit der IT.

Tipp 4: Mitarbeiter als Sicherheitspartner
Leben Sie als Chef das Thema Sicherheit vor und machen es zu einem wichtigen Teil Ihrer Unternehmenskultur. Motivieren Sie Ihre Mitarbeiter, indem Sie sie aktiv beteiligen und im Rahmen des Sicherheitskonzeptes verantwortlich beteiligen.

Tipp 5: Eigenverantwortung aufzeigen
Zeigen Sie Mitarbeitern die Konsequenzen ihres Umgangs mit Passwörtern, Emails oder Einbindung privater Laptops und PDAs durch geeignete Beispiele praxisnah auf. Geben Sie auch Lösungen vor, die aktiv von den Mitarbeiter umgesetzt werden können.

Tipp 6: Mitarbeiter „mitnehmen“
Wenn Sie Mitarbeiter informieren oder schulen, achten Sie darauf, dass die Aufmerksamkeit und die Aufnahmefähigkeit der Mitarbeiter höher ist, wenn Sie ihre „Sprache“ sprechen und die Inhalte unterhaltsam vermitteln. Auf diese Weise können Sie Ihre Mitarbeiter „mitnehmen“ und deren Emotionen ansprechen.

Welche Maßnahmen können hilfreich sein?

Die möglichen Maßnahmen reichen von einfachen Informationen über Schulungen bis hin zu ganzen Maßnahmenpaketen. Denken Sie immer daran: Mit Freude lässt sich es leichter lernen und sich sogar für das Thema begeistern.

Tipp 7: Kenntnisstand der Mitarbeiter
Bevor Sie Mitarbeiter informieren oder zu Schulungen schicken, sollten Sie deren Kenntnisstand einschätzen können. Greifen Sie dabei ggf. auf externe Berater zurück.

Tipp 8: Schulungen im Betrieb
Führen Sie mit Ihren Mitarbeitern Schulungen durch. Berücksichtigen Sie insbesondere deren Reaktion und Anregungen, um die Maßnahmen zu optimieren.

Tipp 9: Lernmaterialien einsetzen
Setzen Sie z.B. Flyer, Newsletter oder Poster ein. Psychologen haben darüber hinaus sehr wirkungsvolle Lernspiele zum Thema IT-Sicherheit entwickelt. Diese Materialien können Sie auch bei externen Anbietern erhalten.

Tipp 10: Regelmäßigkeit schafft Nachhaltigkeit
Nachhaltigkeit im IT-Sicherheitsbewusstsein lässt sich nur durch ständiges Training erzielen. Führen Sie Informations- und Schulungsmaßnahmen deshalb regelmäßig durch.