Risikofaktor IT in Unternehmen

In den meisten Unternehmen geht heute ohne IT nichts mehr – sei es bei der Steuerung der Produktion, in der Buchhaltung oder Verwaltung von Lieferanten und Kundendaten.

Der Schutz der IT ist für das Unternehmen eine Überlebensfrage. Damit sind auch etliche Haftungsfragen verbunden. Will man Hackern, Schäden durch Fehlbedienung, Stromausfall oder sonstigen Schadensfällen vorbeugen und rechtliche Auflagen erfüllen, muss man u.a. wissen: Welche Daten und Anwendungen sind besonders wichtig und sensibel? Wo befinden sie sich? Welchen möglichen Risiken sind sie ausgesetzt und an welcher Stelle empfiehlt es sich, besonders vorsichtig zu sein?

Wenn Sie mögliche Risiken kennen, können Sie auch rechtzeitig vorbeugen und das Schlimmste vermeiden.

„Wir produzieren Dreh- und Frästeile mit höchster Präzision u.a. für die optische und feinmechanische Industrie. Unsere IT ermöglicht es erst, Aufträge effizient durchzuführen. Wir verwalten die Konstruktionszeichnungen IT-gestützt, ebenso arbeiten unsere Maschinen alle programmgesteuert. Ein Ausfall der IT wäre für unsere Produktion eine Katastrophe, gleichzeitig möchten wir unsere Haftungsrisiken möglichst gering halten. Wir haben uns daher einen Überblick über die möglichen Risiken für unsere IT verschafft und begonnen, entsprechende Maßnahmen zu treffen. So wird unser Unternehmen weitestgehend vor Schäden geschützt und fit für die Zukunft."

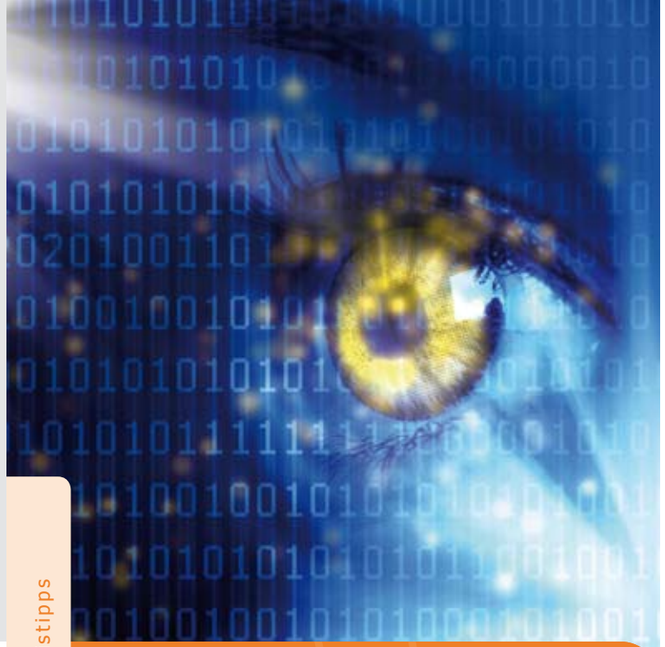
Recep Yildiz, Geschäftsführer
Yildiz CNC-Drehtechnik, Wetzlar

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-Risiken erkennen und vermeiden

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:
Gina Sanders/Fotolia.com, pressmaster/Fotolia.com,
Sergej Khackimullin/Fotolia.com,

Stand: 12/2011

10 Tipps, die wirklich helfen

Wie können Sie sich vor Risiken in Ihrer IT schützen?

10 grundlegende Praxistipps helfen Ihnen, Risiken zu erkennen und zu minimieren.

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.

Eine IT-Risikoanalyse ist die Grundlage, um mögliche Risiken für Ihr Unternehmen abzuschätzen und erfolgreich Maßnahmen zu treffen.

Wie stelle ich fest, welchen Risiken meine IT ausgesetzt ist?

Rechtliche Anforderungen

Die Informationssicherheit ist ein wichtiger Teil des Risikomanagements Ihres Unternehmens, die auch vom Gesetzgeber durch verschiedene rechtliche Vorgaben gefordert wird. So können u.a. eigenständige Haftungsverpflichtungen bei grob fahrlässigen Verstößen z.B. aus dem Gesellschaftsrecht oder dem Datenschutzrecht hergeleitet werden. Bei Verstößen, die z.B. aufgrund unterschätzter IT-Risiken entstehen, können sogar ernsthafte rechtliche Konsequenzen drohen.

Tipp 1: Über rechtliche Vorgaben informieren
Informieren Sie sich umfassend über die gesetzlichen Anforderungen für Ihre IT. Lassen Sie sich hierbei ggf. von einem Experten beraten.

Risiken erkennen

Die Beeinträchtigung der Unternehmens-IT kann zu einem großen finanziellen Schaden führen, wenn z.B. ganze Produktionsketten lahm liegen oder sensible Daten ausspioniert werden. Das Erkennen der Gefahrenpotenziale ist daher ein wichtigen Schritt zu einem wirkungsvollen Schutz Ihrer IT.

Tipp 2: Gefahrenquellen feststellen
Stellen Sie fest, was in Ihrem Unternehmen an Hardware, Software und Daten besonders wichtig ist und auf keinen Fall ausfallen, manipuliert oder ausspioniert werden darf.

Tipp 3: Gefahrenpotenziale erkennen
Untersuchen Sie nach einer Risikobewertung die möglichen Schwachstellen Ihrer IT (z.B. Gefährdungen von außen, mögliche Fehlbedienungen oder technische Sicherheitsmängel) und prüfen Sie anhand Ihrer vorhandenen Schutzmaßnahmen, ob diese ausreichend sind.

Wie kann ich feststellen, welche IT-Risiken besonders hoch sind?

Risiken bewerten

Stellen Sie einem weiteren Schritt fest, welcher (geschätzte) Schaden in Ihrem Unternehmen durch Ausfall oder Datendiebstall entstehen könnte. Bewerten Sie das Risiko, indem Sie die Schadenshöhe abschätzen und die Wahrscheinlichkeit und Dauer eines Ausfalls beurteilen. Hierbei sollten Sie auf eigene Erfahrungswerte, wie z.B. vergangene Vorfälle, und einschlägige Veröffentlichungen zurückgreifen. Es ist allerdings oft schwierig, den möglichen Schaden genau in Euro zu beziffern. Lassen Sie sich im Zweifelsfall von einem externen Experten helfen.

Tipp 4: Schadenskategorien festlegen
Legen Sie Kategorien für die Abschätzung der Schadenshöhe fest, wie z.B. „Schaden darf unter keinen Umständen eintreten“, „hoher Schaden“ und „niedriger Schaden“.

Tipp 5: Schadenshöhe einschätzen
Schätzen Sie nach den Schadenskategorien ein, wie hoch der jeweilige Schaden inkl. Folgekosten sein könnte, wenn z.B. Daten manipuliert oder nicht verfügbar sind, das System aufgrund eines Defektes, Stromausfalls oder Wasserschadens nicht funktioniert oder Unbefugte Dateneinsicht nehmen können.

Tipp 6: Ausfallwahrscheinlichkeit feststellen
Bei ungeplanter Nichtverfügbarkeit von Systemen und Daten berücksichtigen Sie unbedingt auch die Ausfallwahrscheinlichkeit, z.B. wie viele Tage Sie keine Anfragen entgegen nehmen oder nicht produzieren können, weil wichtige Programme fehlen.

Was kann ich tun, um meine IT vor Risiken zu schützen?

Risiken minimieren

Wenn Sie die IT-Risiken in Ihrem Unternehmen erkannt und eingeschätzt haben, können Sie entscheiden, wie Sie mit ihnen umgehen.

Tipp 7: Über Handlungsoptionen informieren
Überlegen Sie, welche Sicherheitsmaßnahmen möglich bzw. zusätzlich möglich und praktikabel sind. Informieren Sie sich über Standards und „best practices“.

Tipp 8: Arbeitsläufe verändern
Überlegen Sie, ob eine Änderung Ihrer Arbeitsabläufe das Risiko mit erträglichem Aufwand minimieren kann.

Tipp 9: Risiken verlagern
Prüfen Sie, ob Sie Risiken verlagern können, indem Sie eine Versicherung abschließen oder die risikobehafteten Prozesse mit entsprechenden Verträgen auslagern.

Tipp 10: Risiken bewusst eingehen
Sie können sich auch bewusst dafür entscheiden, ein Risiko zu tragen, wenn alle in Frage kommenden Maßnahmen unwirtschaftlich sind und/oder das Risiko begrenzt ist. Behalten Sie das Risiko aber unbedingt im Auge.

Nicht nur die IT, auch Arbeitskräfte und Know-how-Träger können z.B. wegen einer Krankheit oder einem Unfall ausfallen. Diese Faktoren sollten Sie bei Ihren Überlegungen ebenfalls mit berücksichtigen.