IT-Sicherheit kompakt.
Berechtigungen.

[m] IT SICHERHEIT

Schutz vor internem Datenmissbrauch

Unterschiedliche Benutzerberechtigungen im Unternehmensnetzwerk gewährleisten strukturierte und transparente Zugriffe auf Daten und sind ein wesentlicher Bestandteil der Unternehmenssicherheit. Durch entsprechende Rollen- und Berechtigungskonzepte erhalten Arbeitsgruppen, Abteilungen oder bestimmte Personen nur Zugriffe auf die Dateien und Programme, die Sie für Ihren Kompetenzbereich benötigen. Zum Beispiel dürfen auf die Personaldaten nur Mitarbeiter der Personalabteilung Zugriff haben. Abmahnungen und Krankheitsdaten sind hoch sensibel und sollten daher auch innerhalb der Personalabteilung nur einem kleinstmöglichen Teil von Mitarbeitern zugänglich sein. Hier ist der Unternehmer gesetzlich verpflichtet dafür Sorge zu tragen, dass ausschließlich berechtigte Einsichten erfolgen. Auch Forschungsergebnisse, Projektstände oder Unterlagen zu sensiblen Vertragsverhandlungen gilt es so zu schützen, dass niemand unbefugt Einsicht nehmen kann.

Stand: November 2013 | Foto: Thorben Wengert / pixelio.de

Gefördert durch:

Bundesministerium für Wirtschaft und Technologie

aufgrund eines Beschlusses des Deutschen Bundestages

TASK FORCE
IT-SICHERHEIT IN DER WIRTSCHAFT
Mehrwert und Schutz für Rechner.

BVMW
Bundesverband mittelständische Wirtschaft

www.bvmw.de

Testen Sie den internen Schutz Ihrer Daten durch Berechtigungen:

- Haben Sie ein Rollenkonzept in die Benutzerverwaltung integriert, um die Zugriffsrechte jedes Mitarbeiters klar zu definieren?
- Haben Sie Passwortrichtlinien aufgestellt, um vorzuschreiben, welches Format die benutzten Passwörter haben sollten und wie oft man diesen ändern sollte?
- Wurden Ihre Mitarbeiter auf die Wahrung des Geschäfts- und Datengeheimnisses gemäß §5 des Bundesdatenschutzgesetzes hingewiesen und verpflichtet?
- Können Sie in Ihrem Unternehmen gewährleisten, dass der Zugriff auf Daten in Ihrem Netzwerk nur durch befugte Mitarbeiter und zur Erfüllung von Arbeitszwecken erfolgt?
- Haben Sie entsprechende Regelungen für mobile Arbeitsplätze/-medien und Homeoffices getroffen?
- Wissen Sie auf welche Daten Unbefugte im Fall eines Hardware-Diebstahls oder Verlusts zugreifen können?

Folgende Handlungsanweisungen sollten Sie beim Schutz beachten:

1. Legen Sie typische Rollen fest, die ein Mitarbeiter in Ihrem Unternehmen einnehmen kann, z.B. „Auftragsannahme".
2. Definieren Sie, auf welche Datenarten die „Auftragsannahme" Zugriff haben muss.
3. Beschränken Sie die Anzahl der Rollen, die ein Mitarbeiter einnehmen kann, um entsprechende Konflikte zu vermeiden.
4. Achten Sie stets darauf, das Rollenkonzept aktuell zu halten und „tote" Rollen zu löschen.
5. Verknüpfen Sie die Mitarbeiter mit den entsprechenden Rollen.
6. Tragen Sie dafür Sorge, dass nachträglich festgestellt werden kann, ob und von wem Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle).

Die Task Force „IT-Sicherheit in der Wirtschaft" ist eine Initiative des Bundesministeriums für Wirtschaft und Technologie, die gemeinsam mit IT-Sicherheitsexperten aus Wissenschaft, Wirtschaft und Verwaltung vor allem kleine und mittelständische Unternehmen für IT-Sicherheit sensibilisieren und dabei unterstützen will, die Sicherheit der IKT-Systeme zu verbessern. Weitere Informationen zur Task Force und ihren Angeboten sind abrufbar unter: www.it-sicherheit-in-der-wirtschaft.de.

Der BVMW. Die Stimme des Mittelstands.

BVMW - Bundesverband mittelständische Wirtschaft Unternehmerverband Deutschlands e.V.
Bundesgeschäftsstelle Berlin ▪ Mosse Palais ▪ Leipziger Platz 15 ▪ 10117 Berlin
Telefon: + 49 30 533206-0 ▪ Telefax: + 49 30 533206-50
mit-sicheheit@bvmw.de ▪ www. mit-sicheheit.bvmw.de