IT-Sicherheit kompakt.
E-Mail-Archivierung.

[m] IT SICHERHEIT

Archivierung unter Wahrung der Privatsphäre

Die Archivierung privater E-Mails verletzt die Privatsphäre des Mitarbeiters. Der Unternehmer ist jedoch verpflichtet alle steuerrelevanten Daten in maschinell auswertbarer Form vorzeigbar aufzubewahren, auch E-Mails und deren Dateianhänge. Kann der private E-Mail-Verkehr nicht ausdrücklich ausgeschlossen werden, müssen Regelungen geschaffen werden, die eine zentrale Ablage steuerrelevanter E-Mails ermöglichen aber private E-Mails nicht archiviert. Hierfür ist eine serverbasierte Lösung mit einem Regelwerk zu empfehlen. Das System sollte in der Lage sein, E-Mails und andere elektronische Dokumente zu einer Akte zusammenzufügen. Dazu zählen auch gescannte Dokumente.

Testen Sie hier, ob Sie die notwendigen Voraussetzungen für die sichere Archivierung Ihrer E-Mails geschaffen haben:

- Archivieren Sie alle steuerrelevanten E-Mails?
- Gibt es ein Verbot für den privaten E-Mail-Verkehr im Unternehmen?
- Können Sie alle steuerrelevanten E-Mails zur Prüfung bereitstellen, ohne die Privatsphäre eines Mitarbeiters zu verletzen?
- Können Sie E-Mails und andere Dokumente (unterschiedlicher Formate), die ein Zusammenhang haben, zu einer Akte zusammenfügen?
- Gibt es elektronische Abläufe für die Behandlung von E-Mails und anderen Dokumenten?

Auswertung: Wenn Sie nicht alle Fragen beantworten können, dann folgen Sie den Lösungsansätzen auf der Rückseite.

Stand: Juli 2013

Gefördert durch:

Bundesministerium für Wirtschaft und Technologie

aufgrund eines Beschlusses des Deutschen Bundestages

BVMW Bundesverband mittelständische Wirtschaft

Schritte zur sicheren Archivierung von E-Mails:

1. Analysieren Sie die für das Geschäft üblichen E-Mail-Typen. (z. B. typische Absender, übliche Adressdaten, spezielle Betreffs, verschiedene Datei-Anhänge)
2. Bestimmen Sie die Verfahrensregeln für diese E-Mails. (z. B. wird immer archiviert, wird unter folgenden Bedingungen archiviert, wird nie archiviert)
3. Legen Sie fest, was mit E-Mails passiert, die keiner der aufgestellten Regeln entsprechen. (z. B. Eintrag im Header: „wurde nicht archiviert", „E-Mail mit steuerrelevanten Inhalt manuell archivieren", „weiterleiten an")
4. Erfassen Sie alle Wege und Verfahren zur Ablage anderer Dokumente. (z. B. elektronische Dokumente, Dokumente in Papierform, gescannte Dokumente)
5. Prüfen Sie, ob nach dem Eingang weitere Arbeitsschritte erforderlich sind. (z.B. entschlüsseln, zur Kenntnis, prüfen, signieren, zuordnen)
6. Fassen Sie alle Anforderungen zusammen und holen Sie sich entsprechende Angebote ein. (z. B. Lizenzkosten, Softwarepflege, Kosten für Implementierung, Schulung und Support)
7. Überprüfen Sie, ob Sie und die anderen Nutzer das gewählte System in absehbarer Zeit beherrschen können. (z. B. Regelwerk, Arbeitsabläufe)
8. Führen Sie das System ein. (z. B. Grundinstallation, Aufstellen der Regeln, Implementierung der Arbeitsabläufe)
9. Belehren Sie die Mitarbeiter über das neue Verfahren und ihre Pflichten.
10. Überprüfen Sie stichprobenartig die Wirksamkeit der Regeln und passen Sie diese bei Notwendigkeit an.

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

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