



10 Punkte für einen sicheren Umgang mit Unternehmensdaten im Internet

Ein modernes Unternehmen gleich welcher Größe und Branche ist ohne die Nutzung von Informations- und Kommunikationstechnologien kaum noch vorstellbar. Der Auf- und Ausbau sicherer IKT-Systeme ist daher eine unerlässliche Investition in die Zukunft eines jeden Unternehmens.

Das Bundesministerium für Wirtschaft und Energie hat daher die Task Force „IT-Sicherheit in der Wirtschaft“ eingerichtet. Mit der Task Force sollen vor allem kleine und mittelständische Unternehmen für das Thema IT-Sicherheit sensibilisiert und dabei unterstützt werden, ihr IT-Sicherheitsniveau zu verbessern.

Gemeinsam mit IT-Sicherheitsexperten aus Wirtschaft, Wissenschaft und Verwaltung wurden die zehn wichtigsten Punkte für einen sicheren Umgang mit Unternehmensdaten im Internet zusammengestellt:

1. Halten Sie Ihre IT-Systeme, mobilen Geräte und Dienste stets aktuell und überprüfen diese regelmäßig auf Viren.
2. Erstellen Sie gut verständliche Sicherheitsrichtlinien (u. a. für Datenträger, Schnittstellen) und Notfallpläne für Ihre IT-Systeme und legen Sie fest, welche Apps und Daten auf mobile Geräte übernommen werden dürfen.
3. Nutzen Sie die qualifizierte elektronische Signatur und verschlüsseln Sie sensible Daten wie Geschäftsgeheimnisse und seien Sie besonders sorgfältig beim Verschicken sowie Speichern.
4. Erstellen Sie ein eindeutiges Berechtigungskonzept für Ihre IT-Systeme, in dem genau geregelt ist, welcher Mitarbeiter welche Zugriffsbefugnisse hat.
5. Sichern Sie regelmäßig Ihre Daten, archivieren Sie sie und sorgen Sie dafür, dass Sie jederzeit darauf zurückgreifen können. Lagern Sie die Datenträger mit den Sicherungen räumlich getrennt voneinander.
6. Wählen Sie stets vertrauenswürdige IT-Dienstleister oder Softwareanbieter aus, die in ihren AGB garantieren, dass Daten nach europäischen Datenschutzstandards gespeichert und verarbeitet werden.
7. Klassifizieren Sie Ihre Daten hinsichtlich der Kritikalität und nutzen Sie für unternehmenskritische Daten eine Organisationsform der Cloud (z. B. Private Cloud), die eine hohe Sicherheit bietet. In Abhängigkeit von der Betriebsform sollten Daten zusätzlich verschlüsselt werden. Wählen Sie einen Cloud-Anbieter aus, der die Daten nach EU-Datenschutzgrundsätzen verarbeitet und entsprechend schützt. Das kann ein Cloud-Anbieter sein, der Daten innerhalb der EU speichert und verarbeitet. Bei Cloud-Service-Providern aus anderen Staaten kann ein angemessenes Schutzniveau dadurch gewährleistet werden, dass der Cloud-Service-Provider mindestens am Safe-Harbor-Programm teilnimmt.
8. Nutzen Sie mit Ihren IT-Geräten stets verschlüsselte Übertragungswege wie VPN und gegebenenfalls Metasuchen und Proxy-Server, die keine Nutzerdaten speichern.
9. Stellen Sie für Ihre Mitarbeiter Richtlinien im Umgang mit sozialen Netzwerken auf, insbesondere welche Daten dort veröffentlicht werden dürfen.
10. Schulen und sensibilisieren Sie Ihre Belegschaft regelmäßig für das Thema IT-Sicherheit.

Weitere Informationen und kostenlose Angebote zu dem Thema IT-Sicherheit finden Sie auf der Internetseite www.it-sicherheit-in-der-wirtschaft.de.