

Checkliste IT-Sicherheit

aufgrund eines Beschlusses
des Deutschen Bundestages

Basisschutz für Desktop-PCs und Notebooks		
Gefahr/ Risiko	Überprüfung des Ist-Zustands	Maßnahme
Angriffe durch Schadprogramme	Verfügen die genutzten Geräte über einen ausreichenden Basisschutz, inklusive Viren-Schutz, und Personal Firewall ?	Nein → Aktivieren Sie Ihre Firewall und richten Sie einen Echtzeitvirenschoner ein. Umgesetzt? <input type="checkbox"/>
	Sind sämtliche auf den Geräten installierten Software-Produkte, insbesondere das Betriebssystem und der Internetbrowser, stets auf dem neuesten Stand?	Nein → Weisen Sie Ihre Mitarbeiter auf automatische Update-Routinen in Programmen hin und motivieren Sie zur Nutzung von Sicherheitsanwendungen wie der App auf it-sicherheit-handwerk.de . Umgesetzt? <input type="checkbox"/>
Verlust von Unternehmens Daten	Werden regelmäßig Backups aller Daten durchgeführt?	Nein → Erarbeiten Sie ein Datensicherungskonzept, in dem festgelegt wird, in welchen Abständen Backups erfolgen. Backups sollten verschlüsselt, redundant abgespeichert und auf fehlerfreie Wiederherstellbarkeit geprüft werden. Umgesetzt? <input type="checkbox"/>
	Löschen Sie Daten vollständig mit geeigneten Programmen?	Nein → Nutzen Sie Programme, die gewährleisten, dass Daten auf externen oder internen Datenträgern sicher gelöscht werden. Umgesetzt? <input type="checkbox"/>
Unberechtigter Zugriff auf unternehmenseigene Daten	Sind die Zugänge aller IT-Geräte mit einem Zugriffsschutz versehen?	Nein → Versehen Sie alle Ihre IT-Geräte mit einem zeitgesteuerten Passwortschutz. Umgesetzt? <input type="checkbox"/>
	Werden starke Passwörter genutzt?	Nein → Verwenden Sie nur ausreichend lange und sinnfrei zusammengesetzte Passwörter (min. 10 Zeichen) aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen. Passwörter sollten in keinem Fall automatisch abgespeichert werden. Nutzen Sie stattdessen einen Passwortsafe. Frei wählbare Benutzernamen sind zu präferieren. Umgesetzt? <input type="checkbox"/>

Firewall/Virenschutz

Patchmanagement

Datensicherung

Passwörter

Werden nach Möglichkeit verschlüsselte Internet-Verbindungen genutzt?

Nein

Umgesetzt?

Klären Sie Ihre Mitarbeiter über die Verwendung von „https“ statt „http“ auf. Animieren Sie zur Kontrolle des „https“-Zertifikats und zur Nutzung von Tools wie "HTTPS Everywhere".

Sind Sie über die Gefahren von „Phishing“ und „Social Engineering“ informiert?

Nein

Umgesetzt?

Informieren Sie Ihre Mitarbeiter über Sicherheitsrisiken und verpflichten Sie diese zur Einhaltung folgender Regeln: Niemals dem Aufruf zur Übermittlung von persönlichen Daten, wie z.B. PIN oder Passwörtern folgen. Keine sensiblen Informationen an Personen weitergeben, die Sie nicht als berechtigte Person verifiziert haben.

Öffnen Sie E-Mails samt Anhang von unbekanntem Absendern?

Ja

Umgesetzt?

Öffnen Sie unter keinen Umständen E-Mail-Anhänge von unbekanntem Absendern.

Wurde auf weitere Sicherheitstipps zur Steigerung der IT-Sicherheit hingewiesen?

Nein

IT-Sicherheit im Handwerk
it-sicherheit-handwerk.de

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

Task Force „IT-Sicherheit in der Wirtschaft“

Die Task-Force „IT-Sicherheit in der Wirtschaft“ ist eine Initiative des Bundesministeriums für Wirtschaft und Energie, 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 unter:

www.it-sicherheit-in-der-wirtschaft.de abrufbar

www.it-sicherheit-handwerk.de



itb- Institut für Technik der Betriebsführung im Deutschen Handwerksinstitut e.V.



Heinz-Piast-Institut für Handwerkstechnik an der Leibniz Universität Hannover



Handwerkskammer Rheinhessen, Kompetenzzentrum für IT-Sicherheit und qualifizierte digitale Signatur



if(is)- Institut für Internet-Sicherheit der Westfälischen Hochschule