

handwerk. magazin

www.handwerk-magazin.de

Checkliste:

So schützen Sie Ihren Betrieb vor HACKERANGRIFFEN

Autorin: **Irmela Schwab**, Journalistin/ Task Force „IT-Sicherheit in der Wirtschaft“

IMMER AUF DER SICHEREN SEITE



Von unserer Fachredaktion geprüft. Die Inhalte dieses Downloads sind nach bestem Wissen und gründlicher Recherche entstanden. Für eventuell enthaltene Fehler übernehmen jedoch Autor/in, Chefredakteur sowie die Holzmann Medien GmbH & Co. KG keine rechtliche Verantwortung.

Checkliste **Schutz vor Hackerangriffen**

Eine Übersicht über die vielen lauernden Gefahren und die nötigen Maßnahmen dagegen hat die Task Force „IT-Sicherheit in der Wirtschaft“ für kleine und mittelständische Unternehmen erstellt. Hinter der Initiative steht das Bundesministerium für Wirtschaft und Energie (BMWi), das gemeinsam mit IT-Sicherheitsexperten aus Wissenschaft, Wirtschaft und Verwaltung mehr Firmen vor Hackerangriffen schützen will.

GEFAHR/RISIKO	ÜBERPRÜFUNG DES IST-ZUSTANDS	MASSNAHME
ANGRIFFE DURCH SCHADPROGRAMME	Verfügen die genutzten Geräte über einen ausreichenden Basisschutz, inklusive Virenschutz, und Personal Firewall?	<input checked="" type="checkbox"/> Aktivieren Sie Ihre Firewall und richten Sie einen Echtzeit-virens Scanner ein.
	Sind sämtliche auf den Geräten installierten Software-Produkte, insbesondere das Betriebssystem und der Internetbrowser, stets auf dem neuesten Stand?	<input checked="" type="checkbox"/> Weisen Sie Ihre Mitarbeiter auf automatische Update-Routinen in Programmen hin und motivieren Sie zur Nutzung von Sicherheitsanwendungen wie der App auf <i>it-sicherheit-handwerk.de</i>.
VERLUST VON UNTERNEHMENS DATEN	Werden regelmäßig Back-ups aller Daten durchgeführt?	<input checked="" type="checkbox"/> Erarbeiten Sie ein Datensicherungskonzept, in dem festgelegt wird, in welchen Abständen Back-ups erfolgen. Back-ups sollten verschlüsselt, redundant abgespeichert und auf fehlerfreie Wiederherstellbarkeit geprüft werden.
	Löschen Sie Daten vollständig mit geeigneten Programmen?	<input checked="" type="checkbox"/> Nutzen Sie Programme, die gewährleisten, dass Daten auf externen oder internen Datenträgern sicher gelöscht werden.
UNBERECHTIGTER ZUGRIFF AUF UNTERNEHMENSEIGENE DATEN	Sind die Zugänge aller IT-Geräte mit einem Zugriffsschutz versehen?	<input checked="" type="checkbox"/> Versehen Sie alle Ihre IT-Geräte mit einem zeitgesteuerten Passwortschutz.
	Werden starke Passwörter genutzt?	<input checked="" type="checkbox"/> 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.
	Werden nach Möglichkeit verschlüsselte Internet-Verbindungen genutzt?	<input checked="" type="checkbox"/> 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?	<input checked="" type="checkbox"/> Informieren Sie Ihre Mitarbeiter über Sicherheitsrisiken und verpflichten Sie diese zur Einhaltung folgender Regeln: Niemals dem Aufruf zur Übermittlung von persönlichen Daten, wie 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?	<input checked="" type="checkbox"/> Öffnen Sie unter keinen Umständen E-Mail-Anhänge von unbekanntem Absendern.
	Wurde auf weitere Sicherheitstipps zur Steigerung der IT-Sicherheit hingewiesen?	<input checked="" type="checkbox"/> Motivieren Sie zur Nutzung von Sicherheitsanwendungen wie der App auf <i>it-sicherheit-handwerk.de</i>.