_Gemeinsam digital

CHECK

IT-Sicherheitsrisiko Mensch

Die Mehrheit der Sicherheitsvorfälle geht auf das Fehlverhalten von Mitarbeitern zurück. Sind Ihre Mitarbeiter auf digitale Angriffe vorbereitet und ausreichend zum Thema IT-Sicherheit informiert?

	Ja	Nein
_Gibt es eine Sicherheitsleitlinie, die von Ihren Mitarbeitern unterschrieben wird?	○	○

In einer umfassenden Sicherheitsleitlinie können Sie festhalten, wie Mitarbeiter mit vertraulichen Daten umgehen sollen. Darin können Sie begründen, welche Verhaltensweisen warum untersagt sind und somit IT-Sicherheit ins Bewusstsein bringen.

_Gibt es eine zentrale Anlaufstelle für Mitarbeiter, denen etwas Verdächtiges auffällt?	○	○

Ein klarer Ansprechpartner ist wichtig. So wissen Mitarbeiter an wen sie sich wenden können, wenn sie beispielsweise Opfer eines Hackerangriffs wurden oder einen solchen vermuten. Damit verringern Sie Risiken und begrenzen den Schaden.

_Haben Sie Regeln für den Umgang mit USB-Sticks festgelegt?	○	○

Klären Sie Ihre Mitarbeiter insbesondere über den Umgang mit externen oder nicht zuordenbaren USB-Sticks auf. Diese können Schadsoftware enthalten, welche Firmenrechner infizieren und sensible Daten ausspionieren. Nutzen Sie zum Testen ggf. einen gesonderten Rechner, der nicht am Firmennetz angeschlossen ist.

_Gibt es in Ihrem Unternehmen festgelegte Regeln für den Umgang mit Passwörtern?	○	○

Ein sicheres Passwort beinhaltet laut BSI mind. 8 Zeichen, Buchstaben, Zahlen, Sonderzeichen sowie Groß- und Kleinschreibung. Außerdem sollten Sie es nie mehrfach verwenden und in regelmäßigen Abständen ändern. Ganz wichtig: Passwort-Manager statt für alle einsehbarer Klebezettel am Bildschirm!

Mittelstand-Digital

Mittelstand 4.0 Kompetenzzentrum Berlin

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

	Ja	Nein
_Gibt es klare Regeln zum Umgang mit dem persönlichen Arbeitsplatz jedes Einzelnen?	○	○

Mitarbeiter sollten wissen, dass sie bei Verlassen ihres Arbeitsplatzes (Mittagspause, Meetings, Feierabend, etc.) ihren Computer blockieren müssen und sensible Dokumente nicht offen einsehbar auf ihrem Schreibtisch liegen lassen dürfen.

_Gibt es etablierte Kontrollmechanismen zur Vermeidung von Betrugsfällen?	○	○

Nicht selten wird versucht, Entscheidungsträger in Unternehmen so zu manipulieren, dass vermeintlich im Auftrag des Top-Managements Überweisungen getätigt werden („CEO Fraud"). Individuelle Kontaktdaten sollten daher nicht öffentlich auffindbar sein und Absenderadressen müssen insbesondere bei Zahlungsaufträgen stets durch Rücksprache verifiziert werden.

_Schulen Sie Ihre Mitarbeiter regelmäßig zu Spionage- bzw. „Social Engineering"-Angriffen?	○	○

Wer innovativ ist, wird oft auch ausspioniert. Sogenannte „Social Engineering"-Angriffe zielen darauf ab, Ihren Mitarbeitern mit manipulativen Anrufen oder E-Mails sensible Daten zu entlocken. Kennen Ihre Mitarbeiter gängige Methoden und sind hierfür sensibilisiert, haben Sie bereits ein großes Risiko eliminiert.

_Haben Sie die Mehrheit der Aussagen mit „Nein" beantwortet?
Es gibt zahlreiche Experten, die Sie bei der Durchsetzung von IT-Sicherheitsmaßnahmen unterstützen können. Schauen Sie in das Mittelstand 4.0-Kompetenzzentrum Berlin und sein Kompetenznetzwerk: Gemeinsam-digital.de | info@gemeinsam-digital.de

_Sie benötigen mehr Informationen zum Thema?
IT-Sicherheit in Unternehmen ist auch immer wieder Thema in unserem Newsblog. Reinschauen lohnt sich: **gemeinsam-digital.de/news-blog**

Stand: September 2017 | Design: www.kattrin-richter.de

_Impressum

Verleger: BVMW - Bundesverband mittelständische Wirtschaft, Unternehmerverband Deutschlands e.V., Bundeszentrale, Potsdamer Straße 7 | Potsdamer Platz, 10785 Berlin, Telefon: +49 30 533206-0, Telefax: +49 30 533206-50, E-Mail: info@bvmw.de
Vertretungsberechtigter Vorstand: M. Ohoven, W. Grothe, Dr. H.-M. Pott, Dr. H. Baur, J. Bormann, Dr. J. Leonhardt, A. Zimmermann
Umsatzsteuer-Identifikationsnummer gem. §27a, UStG DE 230883382 | **Vereinsregister:** Berlin Charlottenburg Nr. 19361 Nz
Soweit keine redaktionelle Kennzeichnung **für den Inhalt Verantwortlicher** i.S.v. § 5 TMG: A. Horn, Leiterin _Gemeinsam digital