CHECK

IT-Notfallplan: Im Ernstfall richtig reagieren

Sie können viel tun, um digitalen Angriffen auf Ihr Unternehmen vorzubeugen. Doch wie reagieren Sie richtig, wenn der Ernstfall bereits eingetreten ist und es gilt, Schaden einzugrenzen?

	Ja	Nein
_Aktivieren Sie sofort Ihr Krisenteam?	○	○

Eine schnelle Reaktion ist dringend nötig, soll der Schaden minimiert werden. Rufen Sie Ihr abteilungsübergreifend organisiertes Krisenteam zusammen! Es besteht aus proaktiv festgelegten Personen, die stets verfügbar sind. Hierbei hilft Ihnen eine zuvor erstellte und ausgedruckte Liste von allen Verantwortlichen und ihren Aufgaben im Notfall.

_Haben Sie den Vorfall rekonstruiert und die aktuelle Lage analysiert?	○	○

Der Krisenstab muss zuerst die Lage beurteilen und eine Bestandsaufnahme durchführen. Nur so können schnellstmöglich die richtigen Maßnahmen ergriffen und Entscheidungen getroffen werden.

_Leiten Sie schnell Sofortmaßnahmen ein?	○	○

Um weiteren Schaden einzudämmen oder gar zu vermeiden, ist sofortiges Handeln erforderlich. Dazu zählen u.a. das Melden des Vorfalls und das Informieren der Betroffenen. Erstatten Sie bei den Behörden Anzeige. So nehmen Sie Ihre Verantwortung für Datensicherheit wahr.

_Dokumentieren Sie so früh wie möglich?	○	○

Ergriffene Maßnahmen und getroffene Entscheidungen sollten detailliert dokumentiert werden. Nur so kann u.U. später auftretenden Nachweispflichten nachgekommen werden.

Mittelstand-Digital

Mittelstand 4.0 Kompetenzzentrum Berlin

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

	Ja	Nein
_Ermöglichen Sie einen Ausweichbetrieb und nutzen Sie alternative Kommunikationskanäle?	○	○

Rechnen Sie damit, dass Angreifer auf Ihren infizierten Systemen mithören können. Nutzen Sie daher für die Krisenbewältigung alternative Kanäle und halten Sie Endgeräte bereit, mit denen Sie zum Normalbetrieb zurückkehren können, etwa durch das Aufspielen von Back-Ups.

_Beachten Sie wichtige Aspekte bei der Wiederaufnahme der IT-Systeme?	○	○

Nach einem Ausfall sollten Ihre ursprünglichen Systeme schnell den gewohnten Betrieb wiederaufnehmen. Spielen Sie Betriebssysteme, Schutzprogramme und weitere Anwendungen neu auf und laden Sie aktuelle Updates herunter.

_Melden Sie Verletzungen des Schutzes personenbezogener Daten?	○	○

Laut Art. 33 Abs. 3 EU-DSGVO müssen Sie Datenpannen innerhalb von 72 Stunden nach Bekanntwerden der zuständigen Aufsichtsbehörde melden, falls Sie zu Risiken für die Betroffenen führen können. U. U. müssen Sie auch die betroffenen Personen informieren. Achtung: Bei Nichtbeachtung drohen hohe Bußgelder!

_Haben Sie die Mehrheit der Aussagen mit „Nein“ beantwortet?
Es gibt zahlreiche Experten, die Sie beim Thema IT-Sicherheit unterstützen können. Schauen Sie in unser Kompetenznetzwerk:
gemeinsam-digital.de | info@gemeinsam-digtial.de

_Sie wollen digitalen Angriffen vorbeugen?
Wie Sie Ihre Mitarbeiter zum Thema „IT-Sicherheit“ sensibilisieren, lesen Sie in unserer Checkliste „IT-Sicherheitsrisiko Mensch“. Auch verfügbar auf:
gemeinsam-digital.de/materialien

Stand: April 2018 | 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
Text und Redaktion: M. Dönges (BVMW e.V.), M. Schaletzky (Softline AG), A. Liefeith (procilon IT-Solutions GmbH)