Mittelstand-Digital
Zentrum
Berlin

Check

# IT-Notfallplan: Bei Cyberangriffen richtig reagieren

## Wie reagieren Sie richtig, wenn der Ernstfall bereits eingetreten ist und es gilt, Schaden einzugrenzen?

**Haben Sie das betroffene System direkt vom internen Netzwerk und dem Internet getrennt?** ◯ Ja ◯ Nein

→ Ziehen Sie im Notfall das Netzwerkkabel damit sich Schadsoftware nicht weiter ausbreiten kann. Schalten Sie das Gerät nicht aus, sofern eine technische Analyse beabsichtigt ist.

**Haben Sie sofort die festgelegten Ansprechpartner:innen und Ihr Krisenteam kontaktiert?** ◯ Ja ◯ Nein

→ 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 (ausgedruckte) Liste mit den Telefonnummern von allen Verantwortlichen und ihren Aufgaben im Notfall.

**Haben Sie den Vorfall rekonstruiert und die aktuelle Lage analysiert?** ◯ Ja ◯ Nein

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

**Dokumentieren Sie so früh wie möglich?** ◯ Ja ◯ Nein

→ Alle ergriffenen Maßnahmen und getroffenen Entscheidungen sollten detailliert dokumentiert werden. Nur so kann u. U. später auftretenden Nachweispflichten nachgekommen werden.

**Ermöglichen Sie einen Ausweichbetrieb und nutzen alternative Kommunikationskanäle?** ◯ Ja ◯ Nein

→ Rechnen Sie damit, dass Angreifende 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?** ◯ Ja ◯ Nein

→ Gehen Sie grundsätzlich davon aus, dass Ihre Systeme vollständig kompromittiert sind. Eine gezielte Säuberung ist nur dann vielversprechend, wenn umfassende Fachkenntnisse vorhanden sind. In den meisten Fällen empfiehlt es sich jedoch, eine vollständige Neuinstallation zu planen.

**Melden Sie Verletzungen des Schutzes personenbezogener Daten?** ◯ Ja ◯ Nein

→ Laut Art. 33 Abs. DSGVO und § 65 BDSG müssen Sie Datenpannen innerhalb von 72 Stunden nach Bekanntwerden der zuständigen Aufsichtsbehörde melden, falls sie zu Risiken für die Betroffenen führen können. Die zuständige Datenschutz-Aufsichtsbehörde variiert je nach Unternehmen oder Institution. Unter Umständen müssen Sie auch die betroffenen Personen informieren. Achtung: Bei Nichtbeachtung drohen hohe Bußgelder!

**Optimieren Sie Ihr Notfallmanagement fortlaufend?** ◯ Ja ◯ Nein

→ Angreifende werden es ein zweites Mal versuchen! Erhöhen Sie Ihre Sicherheitsvorkehrungen z. B. mithilfe des CyberRisiko-Checks der Transferstelle für Cybersicherheit im Mittelstand.

## Sie benötigen mehr Informationen zum Thema Cybersicherheit?

Weitere Informationen und kostenfreie Unterstützung für Ihr Unternehmen finden Sie im Mittelstand-Digital Netzwerk und bei der Transferstelle Cybersicherheit im Mittelstand: **www.transferstelle-cybersicherheit.de**.

**Impressum**
**Verleger:** Der Mittelstand, BVMW e. V. | Potsdamer Straße 7, 10785 Berlin
**Vereinsregister** Berlin Charlottenburg Nr. 19361 Nz | **USt.-ID-Nr.** DE 230883382
**Text & Redaktion:** Christel Schmuck (BVMW) | **Design:** simpelplus.de | Stand: März 2024

Mittelstand-Digital

Gefördert durch:

Bundesministerium für Wirtschaft und Klimaschutz

aufgrund eines Beschlusses des Deutschen Bundestages