IT-Notfallmanagement

„Ziel eines IT-Notfallmanagements ist es, sicherzustellen, dass wichtige Geschäftsprozesse selbst in kritischen Situationen nicht oder nur temporär unterbrochen werden und die wirtschaftliche Existenz der Institution auch bei einem größeren Schadensereignis gesichert bleibt." (BSI Standard 100-4, Zielsetzung)

Nur die wenigsten kleinen und mittelständischen Unternehmen sind entsprechend vorbereitet, um in Notfallsituationen z. B. durch Notfallpläne oder ein etabliertes Notfallmanagement gut zu reagieren und Schadensereignisse zu erkennen.

Typische Schadensereignisse

Schadensereignisse im Unternehmen werden in der Regel in die vier Kategorien bzw. Eskalationsstufen betriebliche Störung, Notfall, Krise und Katastrophe eingeordnet. Betriebliche Störungen sind zumeist kurzfristige Ausfälle im Arbeitsablauf, wohingegen Notfälle länger wirken und ein höheres Schadenspotenzial besitzen. Ein Beispiel hierfür ist ein Brand im Serverraum, welcher nur durch spezielle Aktivitäten bewältigt werden kann.

Krisen sind noch intensiver und können neben der Existenz der Organisation auch die Gesundheit oder das Leben von Personen bedrohen. Ein wichtiges Merkmal ist die Einmaligkeit, wie z. B. ein vollständiger Datenverlust. Eine Katastrophe als höchstmögliche Eskalationsstufe ist innerbetrieblich nicht zu lösen und erfordert externe Hilfe. Beispiele sind Großschadensereignisse wie Pandemien oder großflächige und langanhaltende Versorgungsprobleme (z. B. Elektrizität, Kommunikation).

Mittelstand 4.0-Kompetenzzentrum Chemnitz

Als Mittelstand 4.0-Kompetenzzentrum Chemnitz unterstützen wir Sie als kleines und mittelständisches Unternehmen! Wir zeigen Ihnen die technologischen und wirtschaftlichen Potenziale der Digitalisierung, Vernetzung und Anwendung von Industrie 4.0 und begleiten Sie auf dem herausfordernden Weg in eine digitale Zukunft. Mit der Expertise und Erfahrung unserer Partner wollen wir das Thema Industrie 4.0 für Sie als Unternehmen greifbar machen, Ihre Führungskräfte und Mitarbeiter qualifizieren und die Umsetzung der Digitalisierung bei Ihnen vor Ort unterstützen. Unsere Angebote umfassen ein umfangreiches Leistungsportfolio – von der Sensibilisierung über den Kompetenzaufbau bis hin zur Umsetzung im Unternehmen. Die Leistungs-bereiche bauen aufeinander auf und werden vor Ort in den Unternehmen, in den Testumgebungen der Partner und auf unserer Onlineplattform angeboten. Im Rahmen unserer kostenfreien und praxisnahen Angebote können Sie sich intensiv mit diesen Themen beschäftigen.

Dabei bearbeiten wir folgende Themenfelder:

- **Menschen machen's! –** Der Mensch in der digitalen Arbeitswelt.
- **Alles Unternehmen! –** Das Unternehmen für morgen aufstellen.
- **Leistung bringen! –** Den Prozess digital verbessern.
- **Produkte gestalten! –** Das Produkt für den Nutzer machen.
- **Recht behalten! –** Recht, Sicherheit & Schutz beim digitalen Miteinander.
- **Sicher bleiben! –** Digitalisieren und vernetzen, aber sicher.

Was ist Mittelstand-Digital?

Mittelstand-Digital informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalisierung. Die geförderten Kompetenzzentren helfen mit Expertenwissen, Demonstrationszentren, Best-Practice-Beispielen sowie Netzwerken, die dem Erfahrungsaustausch dienen. Das Bundesministerium für Wirtschaft und Energie (BMWi) ermöglicht die kostenfreie Nutzung aller Angebote von Mittelstand-Digital.

Der DLR Projektträger begleitet im Auftrag des BMWi die Projekte fachlich und sorgt für eine bedarfs- und mittelstandsgerechte Umsetzung der Angebote.
Das Wissenschaftliche Institut für Infrastruktur und Kommunikationsdienste (WIK) unterstützt mit wissenschaftlicher Begleitung, Vernetzung und Öffentlichkeitsarbeit.

Weitere Informationen finden Sie unter:
www.mittelstand-digital.de

Impressum

Text und Redaktion:
Andreas Neuenfels, Mike Wäsche, Roland Hallau,
Mittelstand 4.0-Kompetenzzentrum Chemnitz

Herausgeber:
Mittelstand 4.0-Kompetenzzentrum Chemnitz
c/o tti Technologietransfer und Innovationsförderung Magdeburg GmbH
Bruno-Wille-Straße 9, 39108 Magdeburg
Tel.: +49 391 74435-24 • Fax: +49 391 74435-11
E-Mail: rhallau@tti-md.de
Geschäftsführer: Dr. Michael Klaeger, Marko Wunderlich
Amtsgericht Stendal, HRB 104429
Umsatzsteuer-Identifikationsnummer: DE 139 310 185

Grafische Konzeption und Gestaltung:
toolboxx-media UG (haftungsbeschränkt)

Druckerei: KOCH-DRUCK

Bildnachweis: Shock, kjekol – stock.adobe.com

Magdeburg, April 2020

Mittelstand 4.0 Kompetenzzentrum Chemnitz

Betrieb 4.0 machen!

Wie gelingt ein IT-Notfallmanagement?

10 Goldene Regeln aus der Praxis

www.mittelstand-digital.de

Mittelstand-Digital

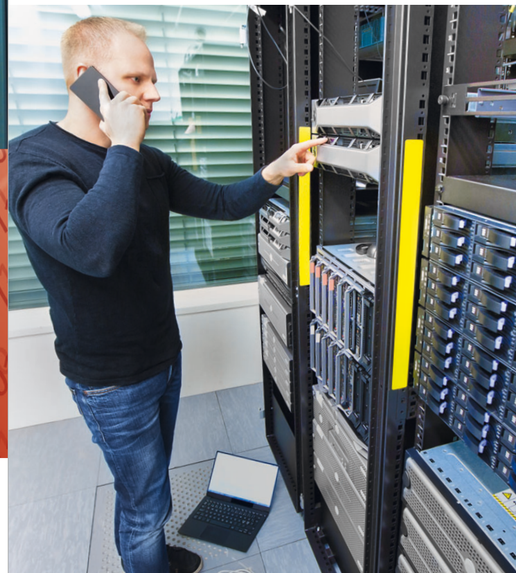
Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

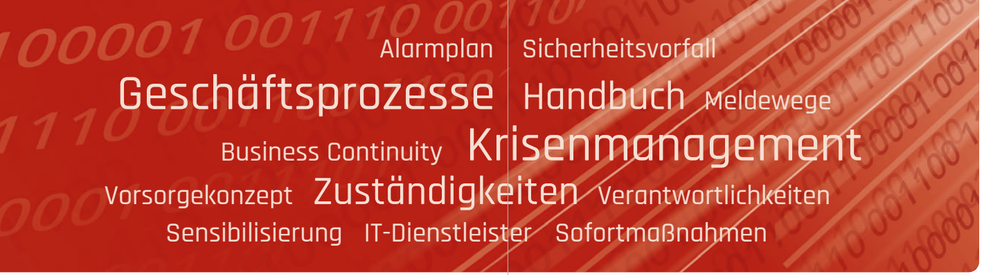
10 Goldene Regeln zum IT-Notfallmanagement

Die 10 Goldenen Regeln sollen Ihnen helfen, die Geschäftsfähigkeit Ihres Unternehmens bei Notfällen und Krisen in Bezug auf IT-Systeme aufrecht zu erhalten. Diese Tipps stammen aus der betrieblichen Praxis kleiner und mittlerer Unternehmen sowie dem Handwerk. Sie wurden in enger Zusammenarbeit mit Unternehmen erarbeitet und basieren auf den Inhalten des BSI-Standard 100-4 – Notfallmanagement (**www.bsi.de**).

Weiterführende Informationen und Anregungen rund um die Themen IT-Sicherheit und Digitalisierung finden Sie unter

www.mittelstand-digital.de.





Wie sollten Sie sich richtig vorbereiten?

Regel 1: Legen Sie Verantwortlichkeiten für IT-Notfälle fest

Insofern ein durch vordefinierte Kriterien erkannter IT-Notfall auftritt, müssen im Unternehmen zur Bewältigung verantwortliche Personen festgelegt sein. Hier bietet sich ein „Notfallmanager" an, der zusammen mit einem Verantwortlichen für „Informationssicherheit" als Team agiert und die Koordination zur Bewältigung der Schadensereignisse übernimmt. Weiterhin sollten diese Personen eng in den Prozess zur Erarbeitung des Notfallmanagements einbezogen und zur Thematik geschult werden.

Regel 2: Analyse der Organisation und ihrer Geschäftsprozesse

Es ist essentiell, dass Sie im Falle einer Notsituation geschäftsfähig bleiben. Daher müssen Sie sich im Klaren sein, welche Prozesse besonders zeitkritisch sind bzw. Ihre unternehmerischen „Kronjuwelen" beinhalten. Diese Vorgänge müssen in der Regel zuerst wieder zum Laufen gebracht werden und sollten in Ihrem Notfallmanagement oberste Priorität genießen.

Regel 3: Dokumentieren Sie Ihre IT-Systeme und Kommunikationswege

Zur Vorbereitung des Notfallmanagements sollten Sie zunächst sicherstellen, dass Ihnen alle im Unternehmen befindlichen IT- bzw. Kommunikationssysteme, -technologien und -schnittstellen bekannt sind.

Hilfreich ist hierbei eine vollständige Dokumentation. Falls Sie diese noch nicht vorliegen haben oder gerne verbessern möchten, sollten Sie sich am besten vom „Groben" in das „Feine" innerhalb der Organisation vorarbeiten. Zur Umsetzung können Sie auf konzeptionell-unterstützende oder automatisierte Netzwerkanalysetools, wie den Demonstrator des Mittelstand 4.0-Kompetenzzentrums (Angebot: „Automatische Sicherheitsprüfung vernetzter Geräte), zurückgreifen.

Regel 4: Holen Sie sich Unterstützung

Bei der Gestaltung des Notfallmanagements sollten Sie Ihre IT-Dienstleister mit einbeziehen. Klären Sie im Vorfeld, für welche Sicherheitsvorfälle Ihnen Unterstützung gegeben werden kann, damit eine zeitnahe Bewältigung des Notfalls gesichert wird! Lassen Sie sich dabei die Unterstützung verbindlich bzw. vertraglich zusichern, so dass z. B. die Verfügbarkeit und die Reaktionszeit der angebotenen Services geregelt werden.

Wie wird ein Notfallmanagement in der Praxis dokumentiert und umgesetzt?

Regel 5: Definieren Sie die Leitlinien zum Notfallmanagement

Gemeinsam mit der Geschäftsleitung müssen Leitlinien zum Notfallmanagement erarbeitet werden, in denen diese sich zu den weitreichenden Folgen des Notfallmanagements bekennt sowie Verantwortung übernimmt. In Abhängigkeit der vorliegenden Informationen müssen, zusammen mit den vorher bestimmten Verantwortlichen, die Zielstellungen und Strategien im Rahmen des Notfallmanagements definiert werden. Auch die organisatorischen Voraussetzungen sowie die Bereitstellung von Ressourcen zur Behebung bzw. Behandlung des Notfalls sollten im Rahmen der Leitlinien geschaffen werden.

Regel 6: Erarbeiten Sie ein Vorsorgekonzept

„Vorsorge ist besser als Nachsorge" – in diesem Sinne sollten Sie schon im Vorfeld Maßnahmen konzipieren, welche präventiv auf die Schadenshöhe oder Eintrittswahrscheinlichkeit einwirken. Zusätzlich sollten Sie sich auch Handlungsweisen zurechtlegen, um die Reaktionsfähigkeit nach einem Schadensereignis sicherzustellen.

Regel 7: Erstellen Sie ein Notfallhandbuch

Das Notfallhandbuch ist der Dreh- und Angelpunkt Ihres Notfallmanagements. Dieses umfasst sämtliche zur Notfallbewältigung notwendigen Dokumente, woraus sich anhand des eingetretenen Schadensereignisses die notwendigen Maßnahmen und Handlungsanweisungen für die Mitarbeiter ableiten lassen. Achten Sie dabei auf kurze Formulierungen und eine übersichtliche Informationsgestaltung. Zur Umsetzung bieten sich sogenannte „IT-Notfallkarten" an. Die „Allianz für Cybersicherheit" bietet diese als PDF-Dateien unter **www.allianz-fuer-cybersicherheit.de** zum Download an.Weiterhin sollte das Notfallhandbuch Geschäftsfortführungspläne enthalten, die einen Notbetrieb im Unternehmen regeln und die in Regel 2 festgestellten Prioritäten in den Geschäftsprozessen umsetzt. Hierzu sind ebenfalls Wiederanlaufpläne (z. B. durch Zuständigkeiten, Schnittstellen, Ressourcen) beizulegen.

Exkurs: IT-Sicherheitsvorfall

Notfälle und Krisen mit Bezug auf die Informationstechnologie resultieren in der Regel aus einem Sicherheitsvorfall, welcher [...] „ein Ereignis bezeichnet, das die Vertraulichkeit, Verfügbarkeit und Integrität der Informationen, Geschäftsprozesse, IT-Dienste, IT-Systeme oder IT-Anwendungen mit hohem oder sehr hohem Schutzbedarf derart beeinträchtigt, dass ein großer Schaden für das Unternehmen / Behörde / Kunden / Geschäftspartner entstehen kann." (BSI Grundschutz M 6.122). Somit sollten die Themen IT-Notfallmanagement und Sicherheitsvorfall nicht getrennt voneinander betrachtet werden. Weitere Informationen zu dieser Thematik finden Sie u. a. in unserem Flyer „Was tun bei einem Sicherheitsvorfall? – 10 Goldene Regeln aus der Praxis" im Wissensbereich „Nachgelesen" unter Angebote auf unserer Webseite www.betrieb-machen.de finden.

Regel 8: Kommunizieren Sie richtig!

Das Notfallhandbuch sollte durch Kommunikationspläne ergänzt werden. Nur wenn die interne und externe Kommunikation richtig und zielgerichtet verläuft, können Sie die Not- bzw. Krisensituationen effektiv und ressourcenschonend bestreiten. Es sollten bei den zuvor erstellten Plänen definierte Ansprechpartner im Unternehmen oder auch bei den Dienstleistern vorliegen. Ebenfalls sollten Sie auch weitere interessierte Parteien bei möglichen Schadensereignissen in Betracht ziehen. Möglich sind hierbei Kunden, Behörden, Angehörige von Mitarbeitern oder die allgemeine Gesellschaft. Insbesondere bei Datenverlusten oder kritischen Datenabflüssen kann es notwendig sein, die Öffentlichkeit zu informieren. Ein gutes und weitverbreitetes Beispiel für ein gelungenes Not- und Krisenmanagement ist hierbei das Unternehmen „Norsk Hydro ASA", welches zeitnah die Kunden und Partner durch zielgerichtete Kommunikationsmaßnahmen über einen Sicherheitsvorfall informiert hat.

Was sollten Sie abschließend unternehmen?

Regel 9: Proben und Schulen

Ihre Mitarbeiter sind sowohl das stärkste als auch das schwächste Glied zur Bewältigung von Notfällen. Schulen Sie daher Ihre Mitarbeiter regelmäßig zum Notfallmanagement und sensibilisieren Sie diese, um Sicherheitsvorfälle zu erkennen. Ferner sollten Sie regelmäßig die Erkennung von Notsituationen und damit verbunden die Wirksamkeit des Notfallmanagements (z. B. durch Anwendung der Notfallpläne im Handbuch) proben. So kann sichergestellt werden, dass Sie auch in echten Notsituationen zielgerichtete Maßnahmen durchführen und der Geschäftsbetrieb zeitnah wiederhergestellt wird.

Regel 10: Ziehen Sie Lehren aus Notfällen

Jedes Schadensereignis ist anders und reale Vorfälle zeigen häufig Schwachstellen an eigenen Plänen und Systemen, denn nicht alle Szenarien können bis ins letzte Detail vorausgeplant werden. Ziehen Sie also im Sinne der kontinuierlichen Verbesserung Lehren aus der bewältigten Notsituation. Passen Sie Ihre Dokumentation sowie Maßnahmen an und optimieren Sie die Meldewege inner- und außerhalb des Unternehmens. Binden Sie dabei auch die eigenen Mitarbeiter mit ein. Wichtig ist es hierbei auch, die durchgeführten Schritte in Abhängigkeit des Sicherheitsvorfalls zu dokumentieren.

Literatur, Standards und Normen zum Notfallmanagement:

- BSI-Standard 100-4 Notfallmanagement (Standard 200-4 in Erarbeitung) des Bundesamtes für Sicherheit in der Informationstechnik
- BSI-Standard 100-4 Notfallmanagement (Standard 200-4 in Erarbeitung)
- DIN EN ISO 22301:2014 (2019 Entwurf) „Sicherheit und Schutz des Gemeinwesens – Business Continuity Management System – Anforderungen"
- IT-Notfallkarte der Allianz für Cybersicherheit
- Good Practice Guidelines (GPG) 2018 Edition des „The Business Continuity Institute (BCI)"

Weitere Informationen finden Sie unter nebenstehendem QR-Code oder unter: **www.betrieb-machen.de**