LSI-Info I#04

# NOTFALLMANAGEMENT

## GRUNDLAGEN DES NOTFALLMANAGEMENTS

*Version 1.1 vom: 16.05.2022*


### Management Summary

„Sicher ist, dass nichts sicher ist, selbst das nicht.“. Obgleich dieses Zitat von Joachim Ringelnatz (1883 - 1934) weit vor der Informationstechnik entstand, gilt es für diese im hohen Maße. IT-Systeme können nicht hundertprozentig geschützt werden. Ein Restrisiko bleibt immer bestehen, unter anderem auch weil potentielle Angreifer in der Regel Schwachstellen zuerst entdecken. Vor allem aber spielt bei Sicherheitsvorfällen der Mensch eine immer größer werdende Rolle. Um hier auf Notfälle vorbereitet zu sein bedarf es eines Plans beziehungsweise eines Konzepts – das Notfallmanagement. Diese LSI-Info soll helfen sich in diese Thematik einzuarbeiten. Durch eine klare Vorgehensweise kann definiert werden, wie in einem solchen Fall gehandelt werden soll. Mit der Handreichung Notfallmanagement welche vom Landesamt für Sicherheit in der Informationstechnik (LSI) bereitgestellt wird, soll ein möglicher Weg bei der Umsetzung des Notfallmanagements aufgezeigt und somit der Einstieg erleichtert werden.

## NUTZEN DES NOTFALLMANAGEMENTS

Die Integration eines Notfallmanagements in die behördliche Organisation ist essentiell. Durch das Notfallmanagement wird ein Vorgehen definiert, wodurch im Ernstfall, von den Einflüssen unabhängig, die Ausfallzeit und der Schaden so gering wie möglich gehalten werden soll. Das Notfallmanagement nutzt einen Überblick über die vorhandenen Informationsverbünde zur Ableitung von Maßnahmen, definiert verantwortliche Personen und beschreibt Meldewege. Wenn Mitarbeiter und die verantwortlichen Fachkräfte wissen, was zu tun ist, kann strukturiert und schnell reagiert werden.
Die Handreichung Notfallmanagement des LSI stellt einen unterstützenden „Roten Faden" für die Umsetzung des Notfallmanagements und die Integration in die Prozesse der Kommune dar. Die Handreichung orientiert sich am BSI-Standard 100-4 und wurde bereits in der Praxis erprobt.

## UMFANG DES NOTFALLMANAGEMENTS

Neben der vorweg genannten Übersicht, sollte sich das Notfallmanagement nicht nur auf die Ressource IT konzentrieren, sondern auch auf weitere relevante Ressourcen wie beispielsweise Prozesse, Personal und Gebäude bzw. Anlagen. Es gibt somit einige Bereiche, die berücksichtigt werden müssen. Im Rahmen eines Risikomanagements sollte für jede dieser Ressourcen folgende Frage beantwortet sein:  Was passiert, wenn diese aufgrund eines Vorfalls nicht mehr zugänglich sind. Auf diesen Erkenntnissen wird das Notfallmanagement aufgebaut.

## VORBEREITUNG

Das Notfallmanagement erreicht schnell eine gewisse Komplexität, daher bedarf es einer gewissen Vorbereitung und Einarbeitung. Wenn nötig kann dabei auf qualifizierte Dienstleister zurückgegriffen werden, die bei der Umsetzung unterstützen. Zusätzlich kann sich mittels relevanter Dokumente (z.B. LSI-Handreichung), Standards, sowie Richt- und Leitlinien über die Erstellung eines Notfallmanagements informiert werden. Für einen guten Start sollten alle verantwortlichen und beteiligten Personen in den Entstehungsprozess eingebunden werden.

## VORSORGE

Ein definierter Ansprechpartner sollte benannt und bekanntgegeben werden. Es empfiehlt sich eine IT-Notfallkarte mit den wichtigsten Schritten, die ein Mitarbeiter in einem Notfall beherzigen sollte. Jeder Mitarbeiter sollte über den Inhalt der IT-Notfallkarte informiert werden, damit sichergestellt ist, dass jeder die zuständigen Verantwortlichen kennt und bei notwendigen Meldungen richtig und schnell reagiert.
Allerdings sollte bedacht werden, dass nicht jede Störung gleich einen Notfall darstellt. Es ist eine der Herausforderungen bei der Umsetzung eines Notfallmanagements, hier die richtigen Beurteilungskriterien zu definieren.
Da sich ein möglicher Notfall nicht zwingend sofort auf den laufenden Betrieb auswirkt, sollte in regelmäßigen Abständen überprüft werden, ob die IT-Systeme einwandfrei laufen und bei Auffälligkeiten entsprechend reagiert werden.
Generell ist es empfehlenswert einen Vorsorgekalender zu führen, der die wichtigsten Maßnahmen des Notfallvorsorgekonzepts enthält.

## DURCHFÜHRUNG

Bei einem Notfall ist es wichtig, Ruhe zu bewahren und alle wichtigen Informationen wie beispielsweise Aktionen und Schritte am betroffenen System und die Beobachtungen zu dokumentieren. Es sollten umgehend alle definierten Ansprechpartner informiert und das weitere Vorgehen besprochen werden.
Wenn möglich sollten u.a. Protokolle und Log-Dateien vor weiteren Maßnahmen gesammelt werden, um diese Daten ggf. für eine spätere Analyse weitergeben zu können. Zudem müssen gegebenenfalls weitere Meldepflichten (z.B. DSGVO) berücksichtigt werden.

## NACHBEREITUNG

Nach einem Notfall ist es besonders wichtig, die wiederhergestellten Systeme zu beobachten, um sicherstellen zu können, dass diese wieder einwandfrei laufen und sich der Notfall nicht sofort wiederholt.
Eventuell vorhandene Schwachstellen sollten, sofern nicht früher möglich, unmittelbar nach der Wiederherstellung der Systeme geschlossen werden. Nach einem Notfall kann auch geprüft werden, ob das vorhandene Notfallmanagement gut umgesetzt wurde oder ob Änderungen sinnvoll sind. Das Notfallmanagement sollte fortlaufend ergänzt und verbessert werden.

## REFERENZEN

- Handreichung des LSI für das Notfallmanagement – erhältlich beim kommunalen Beratungsteam des LSI
- Maßnahmenkatalog zum Notfallmanagement – Fokus IT-Notfälle – https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Unternehmen-allgemein/IT-Notfallkarte/Massnahmenkatalog/massnahmenkatalog_node.html
- BSI-Standard 100-4: Notfallmanagement https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-100-4-Notfallmanagement/bsi-standard-100-4-notfallmanagement_node.html

## KONTAKT

Weitere Informationen finden Sie unter:
https://lsi.bayern.de/kommunen/
Für Unterlagen und Beratung wenden Sie sich bitte per E-Mail an:
Beratung-Kommunen@lsi.bayern.de.
Gerne ist das kommunale Beratungsteam auch telefonisch unter 0911 21549-523 für Sie erreichbar.

Landesamt für Sicherheit in der Informationstechnik – Leitfaden T#07 Notfallmanagement (Stand: 16.05.2022)