

# IT Notfall-Planung – Notwendigkeit und Nutzen

Warum der Blick auf die IT-Systeme nicht der richtige Startpunkt ist. Zum Erfolg in sieben Schritten.

Durch die immer größere Abhängigkeit aller Unternehmen von der Datenverarbeitung im Zuge der notwendigen Digitalisierung von Prozessen und ganzen Organisationen gewinnt auch die Notfall-Planung immer mehr an Gewicht. Gerade in KMU können Ausfälle sehr schnell unternehmenskritisch werden, da bereits die Nichtverfügbarkeit von Daten oder bestimmten Services für wenige Stunden oder Tage nicht zu kompensieren ist.

In diesem Whitepaper wollen wir die allgemeine Herangehensweise an das Thema betrachten, die unterschiedlichen Gefahrenbereiche ansprechen und erste Handlungshilfen geben. Die Erfahrung zeigt, dass gerade die „ersten Schritte“ die schwierigsten sind.

Instinktiv wählen viele, die sich an die Erstellung von Notfallplänen machen (müssen), den Ansatz über die physikalisch vorhandenen Systeme und beschränken sich auf die daraus entstehenden Ausfallszenarien. Mit dieser Herangehensweise werden jedoch z. Bsp. ausgelagerte Services nicht erfasst. Auch im eher konservativen Deutschland gibt es nur noch wenige Unternehmen, die sich „der Cloud“ komplett entziehen können. Letztendlich ist daher eine aktuelle IT-Dokumentation ein wichtiges Hilfsmittel zur Notfall-Planung, deckt aber nur Teile des gesamten Szenarios ab. Erst die vom Anwender ausgehende, serviceorientierte Betrachtungsweise ermöglicht die vollständige Behandlung aller für den Unternehmenserfolg wichtigen Aspekte.

Notfallplanung setzt grundlegend eines voraus: Transparenz. Ohne Wissen über die wesentlichen Geschäftsprozesse und die beeinflussenden Faktoren bleibt eine Notfall-Planung Stückwerk und birgt für den „Fall der Fälle“ Risiken.

Daher wählen wir für den Ansatz einer Notfall-Planung immer die Geschäftsprozesse.

## **Schritt 1: Auflistung der (wichtigen Kern-) Prozesse im Unternehmen**

Die Prozessdokumentation ist in vielen Unternehmen aufgrund z. Bsp. einer ISO-Zertifizierung bereits vorhanden. Ansonsten ist die Erstellung elementar und nicht nur für eine Notfall-Planung verwendbar. Auch die EU Datenschutz-Grundverordnung bedingt eine entsprechende Dokumentation. Je nach Unternehmensgröße und einsetzbaren Mitteln (Mitarbeiter, Zeit) können die vermeintlich wichtigsten Prozesse zuerst betrachtet werden. Diese Einschätzung kann sich aber nach Betrachtung vorhandener Abhängigkeiten nochmals verändern.

# IT Notfall-Planung – Notwendigkeit und Nutzen

Sind die Prozesse aufgelistet, nehmen wir eine erste Bewertung vor.

## Schritt 2: Bewertung

Die dokumentierten Prozesse werden einer Bewertung unterzogen. Hierbei beantworten wir die Fragen:

- Wie wichtig ist der Prozess für das Unternehmen insgesamt?
- Wie lang darf der Prozess maximal ausfallen? (Wann kommt es zu ernststen Schwierigkeiten für das Unternehmen (-> Unmöglichkeit der Leistungserbringung -> Schadenersatzforderungen -> Kundenverlust -> Unternehmensuntergang etc.)

Weiterhin betrachten wir auch die für den Prozess benötigten Daten und Informationen:

- Welchen Datenverlust können wir maximal verkraften?
- Wie alt dürfen die nach einem Ausfall wiederhergestellten Daten maximal sein?

Hieraus ergibt sich eine erste Bewertungsmatrix der Prozesse (z.B. Wichtigkeit kritisch, hoch, normal, niedrig).

Nun bestimmen wir die jeden Prozess beeinflussenden Faktoren.

## Schritt 3: Dokumentation aller beeinflussenden Faktoren pro Prozess.

Neben den technischen Elementen (benötigte IT-Systeme etc.) beeinflussen auch andere Faktoren - insbesondere Menschen und Wissen - die Prozesse. Gibt es beispielsweise Spezialwissen, das nur ein oder wenige Mitarbeiter haben? Dieses Wissen muss (nicht nur zur Notfallplanung, sondern auch im allgemeinen Unternehmensinteresse) transparent und für alle Berechtigten zur Verfügung stehen.

Externe Einflüsse wie gesetzliche Bestimmungen und sonstige (branchenspezifische) Auflagen und Vorgaben können wesentlichen Einfluss auf die Bewertung und vor allem das spätere Handeln bei Eintritt eines Notfalls haben. Hier sei nochmals die EU-Datenschutz Grundverordnung (DSGVO) erwähnt, die entsprechende Informationspflichten z.B. bei unbefugten Datenzugriffen vorschreibt. Auch diese müssen wir zu jedem Prozess dokumentieren.

Kommen wir nun zu den möglichen Störungen.

## Schritt 4: Betrachtung der möglichen Gefährdungen und Ausfallszenarien

Die möglichen Gefährdungen sind sehr umfangreich. Um kein Szenario zu übersehen, können wir uns der Hilfe des Bundesamtes für Sicherheit in der Informationstechnik

# IT Notfall-Planung – Notwendigkeit und Nutzen

(BSI) bedienen. Im IT-Grundschutz-Kompendium listet das BSI 47 „Elementare Gefährdungen“ auf, die wir in unsere Überlegungen einbeziehen. Diese sind unter folgendem Link zu finden:

[https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/elementare\\_gefaehrungen/elementare\\_Gefaehrungen\\_Uebersicht\\_node.html](https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/elementare_gefaehrungen/elementare_Gefaehrungen_Uebersicht_node.html)

Jede dieser Gefährdungen bewerten wir daraufhin, ob sich für den betrachteten Prozess eine Handlungsnotwendigkeit ergibt. Jede potentielle Gefährdungssituation versehen wir mit einer Eintrittswahrscheinlichkeit.

Somit haben wir die Grundlage für die Notfall-Behandlung geschaffen. Auf Basis der nun vorliegenden Dokumentation erstellen wir Rollen für die Mitarbeiter, die diese bei Eintritt eines Ausfallszenarios einnehmen.

## **Schritt 5: Erstellen von Rollen für die Notfallbehandlung**

Da es in Notfällen unabdingbar ist, schnell und zielgerichtet zu handeln, beschreiben wir die notwendigen Aufgaben in Rollen. Diese werden von den dafür vorgesehenen Mitarbeitern eingenommen. Wir beschreiben Aufgaben und Befugnisse, damit Notfallteams schnell handeln können. Dabei orientieren wir uns an den unterschiedlichen Ausfallszenarien, gestaffelt nach Eintrittswahrscheinlichkeit.

Als Grundlage für künftiges Handeln dienen Notfall-Dokumente.

## **Schritt 6: Erfassung und Bereitstellung aller benötigten Dokumente und Informationen**

Notfälle gehören glücklicherweise nicht zum Tagesgeschäft und sind in der Regel immer Stresssituationen. Gerade deswegen ist es wichtig, den handelnden Personen alle notwendigen Dokumente und Informationen auf einfache Weise zur Verfügung zu stellen. Alle benötigten Informationen müssen zentral verzeichnet sein und in geeigneter Form bereitstehen. Es bietet sich an, diese digital erfasst in z.B. einem Wiki vorzuhalten. Zusätzlich müssen Vorkehrungen getroffen sein, falls genau dieses System nicht zur Verfügung steht. Eventuell vorgehaltene analoge Dokumente müssen regelmäßig aktualisiert werden. Zu den benötigten Dokumenten gehören Handlungsanweisungen, Ablaufpläne und Checklisten ebenso wie Systemhandbücher, Lage- bzw. Raumpläne und Lizenzinformationen sowie die Kontaktinformationen aller beteiligten Mitarbeiter, Dienstleister, Lieferanten und ggf. Behörden.

Erst zum Abschluss befassen wir uns mit den IT-Systemen.

# IT Notfall-Planung – Notwendigkeit und Nutzen

## Schritt 7: Zuordnung von IT-Systemen zu den betrachteten Prozessen

Vorausgesetzt, es existiert eine aktuelle IT-Dokumentation (Inventarisierung) ordnen wir nun die Prozesse den zu Grunde liegenden IT-Systemen (Server, Netzwerke, Sicherheitssysteme, CloudServices etc.) zu. Andernfalls ist die IT-Dokumentation zwingend zu erstellen. Hierdurch erkennen wir Abhängigkeiten und können auch einzelne IT-Systeme damit in Bezug auf Wichtigkeit, maximal tolerierbare Ausfallzeit etc. bewerten. Somit erkennen wir Handlungsbedarf, wenn entsprechende Systeme die Anforderungen nicht erfüllen können.

### Fazit

Die prozessorientierte Vorgehensweise stellt sicher, dass keine Lücken in der Notfallplanung „übersehen“ werden. Gleichzeitig gibt sie den Entscheidungsträgern im Unternehmen die Möglichkeit, bestehende Risiken zu erkennen und Entscheidungen entsprechend der Dringlichkeit zu steuern. Sie ermöglicht die aus IT-technischer Sicht notwendige Betrachtung als Serviceverbund. (= Summe aller notwendigen Systeme, um dem Anwender einen bestimmten Service oder ein bestimmte „App“ wie z.B. Mail oder CRM zur Verfügung zu stellen.)

Die erarbeiteten Anforderungen und die serviceorientierte Betrachtung bieten eine belastbare Grundlage für Ausschreibungen sowohl für eigene Investitionen und Eigenbetrieb von Systemen und Anlagen als auch für das Outsourcing einzelner Services bis hin zur kompletten IT.

Darüber hinaus wird eine IT Notfallplanung in nahezu allen Fällen auch von Wirtschaftsprüfern und Versicherungen gefordert, beeinflusst unter Umständen das Kreditranking einer Organisation und ist für Inhaber, Geschäftsführung bzw. Vorstand auch aus haftungstechnischen Fragen weit mehr als ein notwendiges Übel.



**Andreas Gradl** ist Gründungsgesellschafter bei GCT und als Geschäftsführer für Finanzen, Rechtliches und Organisation verantwortlich.

**GCT** ist seit 1989 Ihr professioneller IT-Dienstleister im Rhein-Main-Gebiet mit Sitz in Bad Homburg v.d.H. Als klassisches IT-Systemhaus betreuen wir Ihre IT im eigenen Haus, als Outsourcer bringen wir Ihre IT in eine private Cloud im GCT Rechenzentrum in Frankfurt am Main oder in die public Cloud namhafter Anbieter und als Managed Service Anbieter liefern wir Ihnen Anwendungen und Security „as a Service“.

# IT Notfall-Planung – Notwendigkeit und Nutzen

Warum der Blick auf die IT-Systeme nicht der richtige Startpunkt ist. Zum Erfolg in sieben Schritten.

Durch die immer größere Abhängigkeit aller Unternehmen von der Datenverarbeitung im Zuge der notwendigen Digitalisierung von Prozessen und ganzen Organisationen gewinnt auch die Notfall-Planung immer mehr an Gewicht. Gerade in KMU können Ausfälle sehr schnell unternehmenskritisch werden, da bereits die Nichtverfügbarkeit von Daten oder bestimmten Services für wenige Stunden oder Tage nicht zu kompensieren ist.

In diesem Whitepaper wollen wir die allgemeine Herangehensweise an das Thema betrachten, die unterschiedlichen Gefahrenbereiche ansprechen und erste Handlungshilfen geben. Die Erfahrung zeigt, dass gerade die „ersten Schritte“ die schwierigsten sind.

Instinktiv wählen viele, die sich an die Erstellung von Notfallplänen machen (müssen), den Ansatz über die physikalisch vorhandenen Systeme und beschränken sich auf die daraus entstehenden Ausfallszenarien. Mit dieser Herangehensweise werden jedoch z. Bsp. ausgelagerte Services nicht erfasst. Auch im eher konservativen Deutschland gibt es nur noch wenige Unternehmen, die sich „der Cloud“ komplett entziehen können. Letztendlich ist daher eine aktuelle IT-Dokumentation ein wichtiges Hilfsmittel zur Notfall-Planung, deckt aber nur Teile des gesamten Szenarios ab. Erst die vom Anwender ausgehende, serviceorientierte Betrachtungsweise ermöglicht die vollständige Behandlung aller für den Unternehmenserfolg wichtigen Aspekte.

Notfallplanung setzt grundlegend eines voraus: Transparenz. Ohne Wissen über die wesentlichen Geschäftsprozesse und die beeinflussenden Faktoren bleibt eine Notfall-Planung Stückwerk und birgt für den „Fall der Fälle“ Risiken.

Daher wählen wir für den Ansatz einer Notfall-Planung immer die Geschäftsprozesse.

## **Schritt 1: Auflistung der (wichtigen Kern-) Prozesse im Unternehmen**

Die Prozessdokumentation ist in vielen Unternehmen aufgrund z. Bsp. einer ISO-Zertifizierung bereits vorhanden. Ansonsten ist die Erstellung elementar und nicht nur für eine Notfall-Planung verwendbar. Auch die EU Datenschutz-Grundverordnung bedingt eine entsprechende Dokumentation. Je nach Unternehmensgröße und einsetzbaren Mitteln (Mitarbeiter, Zeit) können die vermeintlich wichtigsten Prozesse zuerst betrachtet werden. Diese Einschätzung kann sich aber nach Betrachtung vorhandener Abhängigkeiten nochmals verändern.

# IT Notfall-Planung – Notwendigkeit und Nutzen

Sind die Prozesse aufgelistet, nehmen wir eine erste Bewertung vor.

## Schritt 2: Bewertung

Die dokumentierten Prozesse werden einer Bewertung unterzogen. Hierbei beantworten wir die Fragen:

- Wie wichtig ist der Prozess für das Unternehmen insgesamt?
- Wie lang darf der Prozess maximal ausfallen? (Wann kommt es zu ernststen Schwierigkeiten für das Unternehmen (-> Unmöglichkeit der Leistungserbringung -> Schadenersatzforderungen -> Kundenverlust -> Unternehmensuntergang etc.)

Weiterhin betrachten wir auch die für den Prozess benötigten Daten und Informationen:

- Welchen Datenverlust können wir maximal verkraften?
- Wie alt dürfen die nach einem Ausfall wiederhergestellten Daten maximal sein?

Hieraus ergibt sich eine erste Bewertungsmatrix der Prozesse (z.B. Wichtigkeit kritisch, hoch, normal, niedrig).

Nun bestimmen wir die jeden Prozess beeinflussenden Faktoren.

## Schritt 3: Dokumentation aller beeinflussenden Faktoren pro Prozess.

Neben den technischen Elementen (benötigte IT-Systeme etc.) beeinflussen auch andere Faktoren - insbesondere Menschen und Wissen - die Prozesse. Gibt es beispielsweise Spezialwissen, das nur ein oder wenige Mitarbeiter haben? Dieses Wissen muss (nicht nur zur Notfallplanung, sondern auch im allgemeinen Unternehmensinteresse) transparent und für alle Berechtigten zur Verfügung stehen.

Externe Einflüsse wie gesetzliche Bestimmungen und sonstige (branchenspezifische) Auflagen und Vorgaben können wesentlichen Einfluss auf die Bewertung und vor allem das spätere Handeln bei Eintritt eines Notfalls haben. Hier sei nochmals die EU-Datenschutz Grundverordnung (DSGVO) erwähnt, die entsprechende Informationspflichten z.B. bei unbefugten Datenzugriffen vorschreibt. Auch diese müssen wir zu jedem Prozess dokumentieren.

Kommen wir nun zu den möglichen Störungen.

## Schritt 4: Betrachtung der möglichen Gefährdungen und Ausfallszenarien

Die möglichen Gefährdungen sind sehr umfangreich. Um kein Szenario zu übersehen, können wir uns der Hilfe des Bundesamtes für Sicherheit in der Informationstechnik

# IT Notfall-Planung – Notwendigkeit und Nutzen

(BSI) bedienen. Im IT-Grundschutz-Kompendium listet das BSI 47 „Elementare Gefährdungen“ auf, die wir in unsere Überlegungen einbeziehen. Diese sind unter folgendem Link zu finden:

[https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/elementare\\_gefaehrungen/elementare\\_Gefaehrungen\\_Uebersicht\\_node.html](https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/elementare_gefaehrungen/elementare_Gefaehrungen_Uebersicht_node.html)

Jede dieser Gefährdungen bewerten wir daraufhin, ob sich für den betrachteten Prozess eine Handlungsnotwendigkeit ergibt. Jede potentielle Gefährdungssituation versehen wir mit einer Eintrittswahrscheinlichkeit.

Somit haben wir die Grundlage für die Notfall-Behandlung geschaffen. Auf Basis der nun vorliegenden Dokumentation erstellen wir Rollen für die Mitarbeiter, die diese bei Eintritt eines Ausfallszenarios einnehmen.

## **Schritt 5: Erstellen von Rollen für die Notfallbehandlung**

Da es in Notfällen unabdingbar ist, schnell und zielgerichtet zu handeln, beschreiben wir die notwendigen Aufgaben in Rollen. Diese werden von den dafür vorgesehenen Mitarbeitern eingenommen. Wir beschreiben Aufgaben und Befugnisse, damit Notfallteams schnell handeln können. Dabei orientieren wir uns an den unterschiedlichen Ausfallszenarien, gestaffelt nach Eintrittswahrscheinlichkeit.

Als Grundlage für künftiges Handeln dienen Notfall-Dokumente.

## **Schritt 6: Erfassung und Bereitstellung aller benötigten Dokumente und Informationen**

Notfälle gehören glücklicherweise nicht zum Tagesgeschäft und sind in der Regel immer Stresssituationen. Gerade deswegen ist es wichtig, den handelnden Personen alle notwendigen Dokumente und Informationen auf einfache Weise zur Verfügung zu stellen. Alle benötigten Informationen müssen zentral verzeichnet sein und in geeigneter Form bereitstehen. Es bietet sich an, diese digital erfasst in z.B. einem Wiki vorzuhalten. Zusätzlich müssen Vorkehrungen getroffen sein, falls genau dieses System nicht zur Verfügung steht. Eventuell vorgehaltene analoge Dokumente müssen regelmäßig aktualisiert werden. Zu den benötigten Dokumenten gehören Handlungsanweisungen, Ablaufpläne und Checklisten ebenso wie Systemhandbücher, Lage- bzw. Raumpläne und Lizenzinformationen sowie die Kontaktinformationen aller beteiligten Mitarbeiter, Dienstleister, Lieferanten und ggf. Behörden.

Erst zum Abschluss befassen wir uns mit den IT-Systemen.

# IT Notfall-Planung – Notwendigkeit und Nutzen

## Schritt 7: Zuordnung von IT-Systemen zu den betrachteten Prozessen

Vorausgesetzt, es existiert eine aktuelle IT-Dokumentation (Inventarisierung) ordnen wir nun die Prozesse den zu Grunde liegenden IT-Systemen (Server, Netzwerke, Sicherheitssysteme, CloudServices etc.) zu. Andernfalls ist die IT-Dokumentation zwingend zu erstellen. Hierdurch erkennen wir Abhängigkeiten und können auch einzelne IT-Systeme damit in Bezug auf Wichtigkeit, maximal tolerierbare Ausfallzeit etc. bewerten. Somit erkennen wir Handlungsbedarf, wenn entsprechende Systeme die Anforderungen nicht erfüllen können.

### Fazit

Die prozessorientierte Vorgehensweise stellt sicher, dass keine Lücken in der Notfallplanung „übersehen“ werden. Gleichzeitig gibt sie den Entscheidungsträgern im Unternehmen die Möglichkeit, bestehende Risiken zu erkennen und Entscheidungen entsprechend der Dringlichkeit zu steuern. Sie ermöglicht die aus IT-technischer Sicht notwendige Betrachtung als Serviceverbund. (= Summe aller notwendigen Systeme, um dem Anwender einen bestimmten Service oder ein bestimmte „App“ wie z.B. Mail oder CRM zur Verfügung zu stellen.)

Die erarbeiteten Anforderungen und die serviceorientierte Betrachtung bieten eine belastbare Grundlage für Ausschreibungen sowohl für eigene Investitionen und Eigenbetrieb von Systemen und Anlagen als auch für das Outsourcing einzelner Services bis hin zur kompletten IT.

Darüber hinaus wird eine IT Notfallplanung in nahezu allen Fällen auch von Wirtschaftsprüfern und Versicherungen gefordert, beeinflusst unter Umständen das Kreditranking einer Organisation und ist für Inhaber, Geschäftsführung bzw. Vorstand auch aus haftungstechnischen Fragen weit mehr als ein notwendiges Übel.



**Andreas Gradl** ist Gründungsgesellschafter bei GCT und als Geschäftsführer für Finanzen, Rechtliches und Organisation verantwortlich.

**GCT** ist seit 1989 Ihr professioneller IT-Dienstleister im Rhein-Main-Gebiet mit Sitz in Bad Homburg v.d.H. Als klassisches IT-Systemhaus betreuen wir Ihre IT im eigenen Haus, als Outsourcer bringen wir Ihre IT in eine private Cloud im GCT Rechenzentrum in Frankfurt am Main oder in die public Cloud namhafter Anbieter und als Managed Service Anbieter liefern wir Ihnen Anwendungen und Security „as a Service“.



# IT Notfall-Planung – Notwendigkeit und Nutzen

Warum der Blick auf die IT-Systeme nicht der richtige Startpunkt ist. Zum Erfolg in sieben Schritten.

Durch die immer größere Abhängigkeit aller Unternehmen von der Datenverarbeitung im Zuge der notwendigen Digitalisierung von Prozessen und ganzen Organisationen gewinnt auch die Notfall-Planung immer mehr an Gewicht. Gerade in KMU können Ausfälle sehr schnell unternehmenskritisch werden, da bereits die Nichtverfügbarkeit von Daten oder bestimmten Services für wenige Stunden oder Tage nicht zu kompensieren ist.

In diesem Whitepaper wollen wir die allgemeine Herangehensweise an das Thema betrachten, die unterschiedlichen Gefahrenbereiche ansprechen und erste Handlungshilfen geben. Die Erfahrung zeigt, dass gerade die „ersten Schritte“ die schwierigsten sind.

Instinktiv wählen viele, die sich an die Erstellung von Notfallplänen machen (müssen), den Ansatz über die physikalisch vorhandenen Systeme und beschränken sich auf die daraus entstehenden Ausfallszenarien. Mit dieser Herangehensweise werden jedoch z. Bsp. ausgelagerte Services nicht erfasst. Auch im eher konservativen Deutschland gibt es nur noch wenige Unternehmen, die sich „der Cloud“ komplett entziehen können. Letztendlich ist daher eine aktuelle IT-Dokumentation ein wichtiges Hilfsmittel zur Notfall-Planung, deckt aber nur Teile des gesamten Szenarios ab. Erst die vom Anwender ausgehende, serviceorientierte Betrachtungsweise ermöglicht die vollständige Behandlung aller für den Unternehmenserfolg wichtigen Aspekte.

Notfallplanung setzt grundlegend eines voraus: Transparenz. Ohne Wissen über die wesentlichen Geschäftsprozesse und die beeinflussenden Faktoren bleibt eine Notfall-Planung Stückwerk und birgt für den „Fall der Fälle“ Risiken.

Daher wählen wir für den Ansatz einer Notfall-Planung immer die Geschäftsprozesse.

## **Schritt 1: Auflistung der (wichtigen Kern-) Prozesse im Unternehmen**

Die Prozessdokumentation ist in vielen Unternehmen aufgrund z. Bsp. einer ISO-Zertifizierung bereits vorhanden. Ansonsten ist die Erstellung elementar und nicht nur für eine Notfall-Planung verwendbar. Auch die EU Datenschutz-Grundverordnung bedingt eine entsprechende Dokumentation. Je nach Unternehmensgröße und einsetzbaren Mitteln (Mitarbeiter, Zeit) können die vermeintlich wichtigsten Prozesse zuerst betrachtet werden. Diese Einschätzung kann sich aber nach Betrachtung vorhandener Abhängigkeiten nochmals verändern.

# IT Notfall-Planung – Notwendigkeit und Nutzen

Sind die Prozesse aufgelistet, nehmen wir eine erste Bewertung vor.

## Schritt 2: Bewertung

Die dokumentierten Prozesse werden einer Bewertung unterzogen. Hierbei beantworten wir die Fragen:

- Wie wichtig ist der Prozess für das Unternehmen insgesamt?
- Wie lang darf der Prozess maximal ausfallen? (Wann kommt es zu ernststen Schwierigkeiten für das Unternehmen (-> Unmöglichkeit der Leistungserbringung -> Schadenersatzforderungen -> Kundenverlust -> Unternehmensuntergang etc.)

Weiterhin betrachten wir auch die für den Prozess benötigten Daten und Informationen:

- Welchen Datenverlust können wir maximal verkraften?
- Wie alt dürfen die nach einem Ausfall wiederhergestellten Daten maximal sein?

Hieraus ergibt sich eine erste Bewertungsmatrix der Prozesse (z.B. Wichtigkeit kritisch, hoch, normal, niedrig).

Nun bestimmen wir die jeden Prozess beeinflussenden Faktoren.

## Schritt 3: Dokumentation aller beeinflussenden Faktoren pro Prozess.

Neben den technischen Elementen (benötigte IT-Systeme etc.) beeinflussen auch andere Faktoren - insbesondere Menschen und Wissen - die Prozesse. Gibt es beispielsweise Spezialwissen, das nur ein oder wenige Mitarbeiter haben? Dieses Wissen muss (nicht nur zur Notfallplanung, sondern auch im allgemeinen Unternehmensinteresse) transparent und für alle Berechtigten zur Verfügung stehen.

Externe Einflüsse wie gesetzliche Bestimmungen und sonstige (branchenspezifische) Auflagen und Vorgaben können wesentlichen Einfluss auf die Bewertung und vor allem das spätere Handeln bei Eintritt eines Notfalls haben. Hier sei nochmals die EU-Datenschutz Grundverordnung (DSGVO) erwähnt, die entsprechende Informationspflichten z.B. bei unbefugten Datenzugriffen vorschreibt. Auch diese müssen wir zu jedem Prozess dokumentieren.

Kommen wir nun zu den möglichen Störungen.

## Schritt 4: Betrachtung der möglichen Gefährdungen und Ausfallszenarien

Die möglichen Gefährdungen sind sehr umfangreich. Um kein Szenario zu übersehen, können wir uns der Hilfe des Bundesamtes für Sicherheit in der Informationstechnik

# IT Notfall-Planung – Notwendigkeit und Nutzen

(BSI) bedienen. Im IT-Grundschutz-Kompendium listet das BSI 47 „Elementare Gefährdungen“ auf, die wir in unsere Überlegungen einbeziehen. Diese sind unter folgendem Link zu finden:

[https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/elementare\\_gefaehrungen/elementare\\_Gefaehrungen\\_Uebersicht\\_node.html](https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/elementare_gefaehrungen/elementare_Gefaehrungen_Uebersicht_node.html)

Jede dieser Gefährdungen bewerten wir daraufhin, ob sich für den betrachteten Prozess eine Handlungsnotwendigkeit ergibt. Jede potentielle Gefährdungssituation versehen wir mit einer Eintrittswahrscheinlichkeit.

Somit haben wir die Grundlage für die Notfall-Behandlung geschaffen. Auf Basis der nun vorliegenden Dokumentation erstellen wir Rollen für die Mitarbeiter, die diese bei Eintritt eines Ausfallszenarios einnehmen.

## **Schritt 5: Erstellen von Rollen für die Notfallbehandlung**

Da es in Notfällen unabdingbar ist, schnell und zielgerichtet zu handeln, beschreiben wir die notwendigen Aufgaben in Rollen. Diese werden von den dafür vorgesehenen Mitarbeitern eingenommen. Wir beschreiben Aufgaben und Befugnisse, damit Notfallteams schnell handeln können. Dabei orientieren wir uns an den unterschiedlichen Ausfallszenarien, gestaffelt nach Eintrittswahrscheinlichkeit.

Als Grundlage für künftiges Handeln dienen Notfall-Dokumente.

## **Schritt 6: Erfassung und Bereitstellung aller benötigten Dokumente und Informationen**

Notfälle gehören glücklicherweise nicht zum Tagesgeschäft und sind in der Regel immer Stresssituationen. Gerade deswegen ist es wichtig, den handelnden Personen alle notwendigen Dokumente und Informationen auf einfache Weise zur Verfügung zu stellen. Alle benötigten Informationen müssen zentral verzeichnet sein und in geeigneter Form bereitstehen. Es bietet sich an, diese digital erfasst in z.B. einem Wiki vorzuhalten. Zusätzlich müssen Vorkehrungen getroffen sein, falls genau dieses System nicht zur Verfügung steht. Eventuell vorgehaltene analoge Dokumente müssen regelmäßig aktualisiert werden. Zu den benötigten Dokumenten gehören Handlungsanweisungen, Ablaufpläne und Checklisten ebenso wie Systemhandbücher, Lage- bzw. Raumpläne und Lizenzinformationen sowie die Kontaktinformationen aller beteiligten Mitarbeiter, Dienstleister, Lieferanten und ggf. Behörden.

Erst zum Abschluss befassen wir uns mit den IT-Systemen.

# IT Notfall-Planung – Notwendigkeit und Nutzen

## Schritt 7: Zuordnung von IT-Systemen zu den betrachteten Prozessen

Vorausgesetzt, es existiert eine aktuelle IT-Dokumentation (Inventarisierung) ordnen wir nun die Prozesse den zu Grunde liegenden IT-Systemen (Server, Netzwerke, Sicherheitssysteme, CloudServices etc.) zu. Andernfalls ist die IT-Dokumentation zwingend zu erstellen. Hierdurch erkennen wir Abhängigkeiten und können auch einzelne IT-Systeme damit in Bezug auf Wichtigkeit, maximal tolerierbare Ausfallzeit etc. bewerten. Somit erkennen wir Handlungsbedarf, wenn entsprechende Systeme die Anforderungen nicht erfüllen können.

### Fazit

Die prozessorientierte Vorgehensweise stellt sicher, dass keine Lücken in der Notfallplanung „übersehen“ werden. Gleichzeitig gibt sie den Entscheidungsträgern im Unternehmen die Möglichkeit, bestehende Risiken zu erkennen und Entscheidungen entsprechend der Dringlichkeit zu steuern. Sie ermöglicht die aus IT-technischer Sicht notwendige Betrachtung als Serviceverbund. (= Summe aller notwendigen Systeme, um dem Anwender einen bestimmten Service oder ein bestimmte „App“ wie z.B. Mail oder CRM zur Verfügung zu stellen.)

Die erarbeiteten Anforderungen und die serviceorientierte Betrachtung bieten eine belastbare Grundlage für Ausschreibungen sowohl für eigene Investitionen und Eigenbetrieb von Systemen und Anlagen als auch für das Outsourcing einzelner Services bis hin zur kompletten IT.

Darüber hinaus wird eine IT Notfallplanung in nahezu allen Fällen auch von Wirtschaftsprüfern und Versicherungen gefordert, beeinflusst unter Umständen das Kreditranking einer Organisation und ist für Inhaber, Geschäftsführung bzw. Vorstand auch aus haftungstechnischen Fragen weit mehr als ein notwendiges Übel.



**Andreas Gradl** ist Gründungsgesellschafter bei GCT und als Geschäftsführer für Finanzen, Rechtliches und Organisation verantwortlich.

**GCT** ist seit 1989 Ihr professioneller IT-Dienstleister im Rhein-Main-Gebiet mit Sitz in Bad Homburg v.d.H. Als klassisches IT-Systemhaus betreuen wir Ihre IT im eigenen Haus, als Outsourcer bringen wir Ihre IT in eine private Cloud im GCT Rechenzentrum in Frankfurt am Main oder in die public Cloud namhafter Anbieter und als Managed Service Anbieter liefern wir Ihnen Anwendungen und Security „as a Service“.

# IT Notfall-Planung – Notwendigkeit und Nutzen

Warum der Blick auf die IT-Systeme nicht der richtige Startpunkt ist. Zum Erfolg in sieben Schritten.

Durch die immer größere Abhängigkeit aller Unternehmen von der Datenverarbeitung im Zuge der notwendigen Digitalisierung von Prozessen und ganzen Organisationen gewinnt auch die Notfall-Planung immer mehr an Gewicht. Gerade in KMU können Ausfälle sehr schnell unternehmenskritisch werden, da bereits die Nichtverfügbarkeit von Daten oder bestimmten Services für wenige Stunden oder Tage nicht zu kompensieren ist.

In diesem Whitepaper wollen wir die allgemeine Herangehensweise an das Thema betrachten, die unterschiedlichen Gefahrenbereiche ansprechen und erste Handlungshilfen geben. Die Erfahrung zeigt, dass gerade die „ersten Schritte“ die schwierigsten sind.

Instinktiv wählen viele, die sich an die Erstellung von Notfallplänen machen (müssen), den Ansatz über die physikalisch vorhandenen Systeme und beschränken sich auf die daraus entstehenden Ausfallszenarien. Mit dieser Herangehensweise werden jedoch z. Bsp. ausgelagerte Services nicht erfasst. Auch im eher konservativen Deutschland gibt es nur noch wenige Unternehmen, die sich „der Cloud“ komplett entziehen können. Letztendlich ist daher eine aktuelle IT-Dokumentation ein wichtiges Hilfsmittel zur Notfall-Planung, deckt aber nur Teile des gesamten Szenarios ab. Erst die vom Anwender ausgehende, serviceorientierte Betrachtungsweise ermöglicht die vollständige Behandlung aller für den Unternehmenserfolg wichtigen Aspekte.

Notfallplanung setzt grundlegend eines voraus: Transparenz. Ohne Wissen über die wesentlichen Geschäftsprozesse und die beeinflussenden Faktoren bleibt eine Notfall-Planung Stückwerk und birgt für den „Fall der Fälle“ Risiken.

Daher wählen wir für den Ansatz einer Notfall-Planung immer die Geschäftsprozesse.

## **Schritt 1: Auflistung der (wichtigen Kern-) Prozesse im Unternehmen**

Die Prozessdokumentation ist in vielen Unternehmen aufgrund z. Bsp. einer ISO-Zertifizierung bereits vorhanden. Ansonsten ist die Erstellung elementar und nicht nur für eine Notfall-Planung verwendbar. Auch die EU Datenschutz-Grundverordnung bedingt eine entsprechende Dokumentation. Je nach Unternehmensgröße und einsetzbaren Mitteln (Mitarbeiter, Zeit) können die vermeintlich wichtigsten Prozesse zuerst betrachtet werden. Diese Einschätzung kann sich aber nach Betrachtung vorhandener Abhängigkeiten nochmals verändern.

# IT Notfall-Planung – Notwendigkeit und Nutzen

Sind die Prozesse aufgelistet, nehmen wir eine erste Bewertung vor.

## Schritt 2: Bewertung

Die dokumentierten Prozesse werden einer Bewertung unterzogen. Hierbei beantworten wir die Fragen:

- Wie wichtig ist der Prozess für das Unternehmen insgesamt?
- Wie lang darf der Prozess maximal ausfallen? (Wann kommt es zu ernststen Schwierigkeiten für das Unternehmen (-> Unmöglichkeit der Leistungserbringung -> Schadenersatzforderungen -> Kundenverlust -> Unternehmensuntergang etc.)

Weiterhin betrachten wir auch die für den Prozess benötigten Daten und Informationen:

- Welchen Datenverlust können wir maximal verkraften?
- Wie alt dürfen die nach einem Ausfall wiederhergestellten Daten maximal sein?

Hieraus ergibt sich eine erste Bewertungsmatrix der Prozesse (z.B. Wichtigkeit kritisch, hoch, normal, niedrig).

Nun bestimmen wir die jeden Prozess beeinflussenden Faktoren.

## Schritt 3: Dokumentation aller beeinflussenden Faktoren pro Prozess.

Neben den technischen Elementen (benötigte IT-Systeme etc.) beeinflussen auch andere Faktoren - insbesondere Menschen und Wissen - die Prozesse. Gibt es beispielsweise Spezialwissen, das nur ein oder wenige Mitarbeiter haben? Dieses Wissen muss (nicht nur zur Notfallplanung, sondern auch im allgemeinen Unternehmensinteresse) transparent und für alle Berechtigten zur Verfügung stehen.

Externe Einflüsse wie gesetzliche Bestimmungen und sonstige (branchenspezifische) Auflagen und Vorgaben können wesentlichen Einfluss auf die Bewertung und vor allem das spätere Handeln bei Eintritt eines Notfalls haben. Hier sei nochmals die EU-Datenschutz Grundverordnung (DSGVO) erwähnt, die entsprechende Informationspflichten z.B. bei unbefugten Datenzugriffen vorschreibt. Auch diese müssen wir zu jedem Prozess dokumentieren.

Kommen wir nun zu den möglichen Störungen.

## Schritt 4: Betrachtung der möglichen Gefährdungen und Ausfallszenarien

Die möglichen Gefährdungen sind sehr umfangreich. Um kein Szenario zu übersehen, können wir uns der Hilfe des Bundesamtes für Sicherheit in der Informationstechnik

# IT Notfall-Planung – Notwendigkeit und Nutzen

(BSI) bedienen. Im IT-Grundschutz-Kompendium listet das BSI 47 „Elementare Gefährdungen“ auf, die wir in unsere Überlegungen einbeziehen. Diese sind unter folgendem Link zu finden:

[https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/elementare\\_gefaehrungen/elementare\\_Gefaehrungen\\_Uebersicht\\_node.html](https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/elementare_gefaehrungen/elementare_Gefaehrungen_Uebersicht_node.html)

Jede dieser Gefährdungen bewerten wir daraufhin, ob sich für den betrachteten Prozess eine Handlungsnotwendigkeit ergibt. Jede potentielle Gefährdungssituation versehen wir mit einer Eintrittswahrscheinlichkeit.

Somit haben wir die Grundlage für die Notfall-Behandlung geschaffen. Auf Basis der nun vorliegenden Dokumentation erstellen wir Rollen für die Mitarbeiter, die diese bei Eintritt eines Ausfallszenarios einnehmen.

## **Schritt 5: Erstellen von Rollen für die Notfallbehandlung**

Da es in Notfällen unabdingbar ist, schnell und zielgerichtet zu handeln, beschreiben wir die notwendigen Aufgaben in Rollen. Diese werden von den dafür vorgesehenen Mitarbeitern eingenommen. Wir beschreiben Aufgaben und Befugnisse, damit Notfallteams schnell handeln können. Dabei orientieren wir uns an den unterschiedlichen Ausfallszenarien, gestaffelt nach Eintrittswahrscheinlichkeit.

Als Grundlage für künftiges Handeln dienen Notfall-Dokumente.

## **Schritt 6: Erfassung und Bereitstellung aller benötigten Dokumente und Informationen**

Notfälle gehören glücklicherweise nicht zum Tagesgeschäft und sind in der Regel immer Stresssituationen. Gerade deswegen ist es wichtig, den handelnden Personen alle notwendigen Dokumente und Informationen auf einfache Weise zur Verfügung zu stellen. Alle benötigten Informationen müssen zentral verzeichnet sein und in geeigneter Form bereitstehen. Es bietet sich an, diese digital erfasst in z.B. einem Wiki vorzuhalten. Zusätzlich müssen Vorkehrungen getroffen sein, falls genau dieses System nicht zur Verfügung steht. Eventuell vorgehaltene analoge Dokumente müssen regelmäßig aktualisiert werden. Zu den benötigten Dokumenten gehören Handlungsanweisungen, Ablaufpläne und Checklisten ebenso wie Systemhandbücher, Lage- bzw. Raumpläne und Lizenzinformationen sowie die Kontaktinformationen aller beteiligten Mitarbeiter, Dienstleister, Lieferanten und ggf. Behörden.

Erst zum Abschluss befassen wir uns mit den IT-Systemen.

# IT Notfall-Planung – Notwendigkeit und Nutzen

## Schritt 7: Zuordnung von IT-Systemen zu den betrachteten Prozessen

Vorausgesetzt, es existiert eine aktuelle IT-Dokumentation (Inventarisierung) ordnen wir nun die Prozesse den zu Grunde liegenden IT-Systemen (Server, Netzwerke, Sicherheitssysteme, CloudServices etc.) zu. Andernfalls ist die IT-Dokumentation zwingend zu erstellen. Hierdurch erkennen wir Abhängigkeiten und können auch einzelne IT-Systeme damit in Bezug auf Wichtigkeit, maximal tolerierbare Ausfallzeit etc. bewerten. Somit erkennen wir Handlungsbedarf, wenn entsprechende Systeme die Anforderungen nicht erfüllen können.

### Fazit

Die prozessorientierte Vorgehensweise stellt sicher, dass keine Lücken in der Notfallplanung „übersehen“ werden. Gleichzeitig gibt sie den Entscheidungsträgern im Unternehmen die Möglichkeit, bestehende Risiken zu erkennen und Entscheidungen entsprechend der Dringlichkeit zu steuern. Sie ermöglicht die aus IT-technischer Sicht notwendige Betrachtung als Serviceverbund. (= Summe aller notwendigen Systeme, um dem Anwender einen bestimmten Service oder ein bestimmte „App“ wie z.B. Mail oder CRM zur Verfügung zu stellen.)

Die erarbeiteten Anforderungen und die serviceorientierte Betrachtung bieten eine belastbare Grundlage für Ausschreibungen sowohl für eigene Investitionen und Eigenbetrieb von Systemen und Anlagen als auch für das Outsourcing einzelner Services bis hin zur kompletten IT.

Darüber hinaus wird eine IT Notfallplanung in nahezu allen Fällen auch von Wirtschaftsprüfern und Versicherungen gefordert, beeinflusst unter Umständen das Kreditranking einer Organisation und ist für Inhaber, Geschäftsführung bzw. Vorstand auch aus haftungstechnischen Fragen weit mehr als ein notwendiges Übel.



**Andreas Gradl** ist Gründungsgesellschafter bei GCT und als Geschäftsführer für Finanzen, Rechtliches und Organisation verantwortlich.

**GCT** ist seit 1989 Ihr professioneller IT-Dienstleister im Rhein-Main-Gebiet mit Sitz in Bad Homburg v.d.H. Als klassisches IT-Systemhaus betreuen wir Ihre IT im eigenen Haus, als Outsourcer bringen wir Ihre IT in eine private Cloud im GCT Rechenzentrum in Frankfurt am Main oder in die public Cloud namhafter Anbieter und als Managed Service Anbieter liefern wir Ihnen Anwendungen und Security „as a Service“.



# IT Notfall-Planung – Notwendigkeit und Nutzen

Warum der Blick auf die IT-Systeme nicht der richtige Startpunkt ist. Zum Erfolg in sieben Schritten.

Durch die immer größere Abhängigkeit aller Unternehmen von der Datenverarbeitung im Zuge der notwendigen Digitalisierung von Prozessen und ganzen Organisationen gewinnt auch die Notfall-Planung immer mehr an Gewicht. Gerade in KMU können Ausfälle sehr schnell unternehmenskritisch werden, da bereits die Nichtverfügbarkeit von Daten oder bestimmten Services für wenige Stunden oder Tage nicht zu kompensieren ist.

In diesem Whitepaper wollen wir die allgemeine Herangehensweise an das Thema betrachten, die unterschiedlichen Gefahrenbereiche ansprechen und erste Handlungshilfen geben. Die Erfahrung zeigt, dass gerade die „ersten Schritte“ die schwierigsten sind.

Instinktiv wählen viele, die sich an die Erstellung von Notfallplänen machen (müssen), den Ansatz über die physikalisch vorhandenen Systeme und beschränken sich auf die daraus entstehenden Ausfallszenarien. Mit dieser Herangehensweise werden jedoch z. Bsp. ausgelagerte Services nicht erfasst. Auch im eher konservativen Deutschland gibt es nur noch wenige Unternehmen, die sich „der Cloud“ komplett entziehen können. Letztendlich ist daher eine aktuelle IT-Dokumentation ein wichtiges Hilfsmittel zur Notfall-Planung, deckt aber nur Teile des gesamten Szenarios ab. Erst die vom Anwender ausgehende, serviceorientierte Betrachtungsweise ermöglicht die vollständige Behandlung aller für den Unternehmenserfolg wichtigen Aspekte.

Notfallplanung setzt grundlegend eines voraus: Transparenz. Ohne Wissen über die wesentlichen Geschäftsprozesse und die beeinflussenden Faktoren bleibt eine Notfall-Planung Stückwerk und birgt für den „Fall der Fälle“ Risiken.

Daher wählen wir für den Ansatz einer Notfall-Planung immer die Geschäftsprozesse.

## **Schritt 1: Auflistung der (wichtigen Kern-) Prozesse im Unternehmen**

Die Prozessdokumentation ist in vielen Unternehmen aufgrund z. Bsp. einer ISO-Zertifizierung bereits vorhanden. Ansonsten ist die Erstellung elementar und nicht nur für eine Notfall-Planung verwendbar. Auch die EU Datenschutz-Grundverordnung bedingt eine entsprechende Dokumentation. Je nach Unternehmensgröße und einsetzbaren Mitteln (Mitarbeiter, Zeit) können die vermeintlich wichtigsten Prozesse zuerst betrachtet werden. Diese Einschätzung kann sich aber nach Betrachtung vorhandener Abhängigkeiten nochmals verändern.

# IT Notfall-Planung – Notwendigkeit und Nutzen

Sind die Prozesse aufgelistet, nehmen wir eine erste Bewertung vor.

## Schritt 2: Bewertung

Die dokumentierten Prozesse werden einer Bewertung unterzogen. Hierbei beantworten wir die Fragen:

- Wie wichtig ist der Prozess für das Unternehmen insgesamt?
- Wie lang darf der Prozess maximal ausfallen? (Wann kommt es zu ernststen Schwierigkeiten für das Unternehmen (-> Unmöglichkeit der Leistungserbringung -> Schadenersatzforderungen -> Kundenverlust -> Unternehmensuntergang etc.)

Weiterhin betrachten wir auch die für den Prozess benötigten Daten und Informationen:

- Welchen Datenverlust können wir maximal verkraften?
- Wie alt dürfen die nach einem Ausfall wiederhergestellten Daten maximal sein?

Hieraus ergibt sich eine erste Bewertungsmatrix der Prozesse (z.B. Wichtigkeit kritisch, hoch, normal, niedrig).

Nun bestimmen wir die jeden Prozess beeinflussenden Faktoren.

## Schritt 3: Dokumentation aller beeinflussenden Faktoren pro Prozess.

Neben den technischen Elementen (benötigte IT-Systeme etc.) beeinflussen auch andere Faktoren - insbesondere Menschen und Wissen - die Prozesse. Gibt es beispielsweise Spezialwissen, das nur ein oder wenige Mitarbeiter haben? Dieses Wissen muss (nicht nur zur Notfallplanung, sondern auch im allgemeinen Unternehmensinteresse) transparent und für alle Berechtigten zur Verfügung stehen.

Externe Einflüsse wie gesetzliche Bestimmungen und sonstige (branchenspezifische) Auflagen und Vorgaben können wesentlichen Einfluss auf die Bewertung und vor allem das spätere Handeln bei Eintritt eines Notfalls haben. Hier sei nochmals die EU-Datenschutz Grundverordnung (DSGVO) erwähnt, die entsprechende Informationspflichten z.B. bei unbefugten Datenzugriffen vorschreibt. Auch diese müssen wir zu jedem Prozess dokumentieren.

Kommen wir nun zu den möglichen Störungen.

## Schritt 4: Betrachtung der möglichen Gefährdungen und Ausfallszenarien

Die möglichen Gefährdungen sind sehr umfangreich. Um kein Szenario zu übersehen, können wir uns der Hilfe des Bundesamtes für Sicherheit in der Informationstechnik

# IT Notfall-Planung – Notwendigkeit und Nutzen

(BSI) bedienen. Im IT-Grundschutz-Kompendium listet das BSI 47 „Elementare Gefährdungen“ auf, die wir in unsere Überlegungen einbeziehen. Diese sind unter folgendem Link zu finden:

[https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/elementare\\_gefaehrungen/elementare\\_Gefaehrungen\\_Uebersicht\\_node.html](https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/elementare_gefaehrungen/elementare_Gefaehrungen_Uebersicht_node.html)

Jede dieser Gefährdungen bewerten wir daraufhin, ob sich für den betrachteten Prozess eine Handlungsnotwendigkeit ergibt. Jede potentielle Gefährdungssituation versehen wir mit einer Eintrittswahrscheinlichkeit.

Somit haben wir die Grundlage für die Notfall-Behandlung geschaffen. Auf Basis der nun vorliegenden Dokumentation erstellen wir Rollen für die Mitarbeiter, die diese bei Eintritt eines Ausfallszenarios einnehmen.

## **Schritt 5: Erstellen von Rollen für die Notfallbehandlung**

Da es in Notfällen unabdingbar ist, schnell und zielgerichtet zu handeln, beschreiben wir die notwendigen Aufgaben in Rollen. Diese werden von den dafür vorgesehenen Mitarbeitern eingenommen. Wir beschreiben Aufgaben und Befugnisse, damit Notfallteams schnell handeln können. Dabei orientieren wir uns an den unterschiedlichen Ausfallszenarien, gestaffelt nach Eintrittswahrscheinlichkeit.

Als Grundlage für künftiges Handeln dienen Notfall-Dokumente.

## **Schritt 6: Erfassung und Bereitstellung aller benötigten Dokumente und Informationen**

Notfälle gehören glücklicherweise nicht zum Tagesgeschäft und sind in der Regel immer Stresssituationen. Gerade deswegen ist es wichtig, den handelnden Personen alle notwendigen Dokumente und Informationen auf einfache Weise zur Verfügung zu stellen. Alle benötigten Informationen müssen zentral verzeichnet sein und in geeigneter Form bereitstehen. Es bietet sich an, diese digital erfasst in z.B. einem Wiki vorzuhalten. Zusätzlich müssen Vorkehrungen getroffen sein, falls genau dieses System nicht zur Verfügung steht. Eventuell vorgehaltene analoge Dokumente müssen regelmäßig aktualisiert werden. Zu den benötigten Dokumenten gehören Handlungsanweisungen, Ablaufpläne und Checklisten ebenso wie Systemhandbücher, Lage- bzw. Raumpläne und Lizenzinformationen sowie die Kontaktinformationen aller beteiligten Mitarbeiter, Dienstleister, Lieferanten und ggf. Behörden.

Erst zum Abschluss befassen wir uns mit den IT-Systemen.

# IT Notfall-Planung – Notwendigkeit und Nutzen

## Schritt 7: Zuordnung von IT-Systemen zu den betrachteten Prozessen

Vorausgesetzt, es existiert eine aktuelle IT-Dokumentation (Inventarisierung) ordnen wir nun die Prozesse den zu Grunde liegenden IT-Systemen (Server, Netzwerke, Sicherheitssysteme, CloudServices etc.) zu. Andernfalls ist die IT-Dokumentation zwingend zu erstellen. Hierdurch erkennen wir Abhängigkeiten und können auch einzelne IT-Systeme damit in Bezug auf Wichtigkeit, maximal tolerierbare Ausfallzeit etc. bewerten. Somit erkennen wir Handlungsbedarf, wenn entsprechende Systeme die Anforderungen nicht erfüllen können.

### Fazit

Die prozessorientierte Vorgehensweise stellt sicher, dass keine Lücken in der Notfallplanung „übersehen“ werden. Gleichzeitig gibt sie den Entscheidungsträgern im Unternehmen die Möglichkeit, bestehende Risiken zu erkennen und Entscheidungen entsprechend der Dringlichkeit zu steuern. Sie ermöglicht die aus IT-technischer Sicht notwendige Betrachtung als Serviceverbund. (= Summe aller notwendigen Systeme, um dem Anwender einen bestimmten Service oder ein bestimmte „App“ wie z.B. Mail oder CRM zur Verfügung zu stellen.)

Die erarbeiteten Anforderungen und die serviceorientierte Betrachtung bieten eine belastbare Grundlage für Ausschreibungen sowohl für eigene Investitionen und Eigenbetrieb von Systemen und Anlagen als auch für das Outsourcing einzelner Services bis hin zur kompletten IT.

Darüber hinaus wird eine IT Notfallplanung in nahezu allen Fällen auch von Wirtschaftsprüfern und Versicherungen gefordert, beeinflusst unter Umständen das Kreditranking einer Organisation und ist für Inhaber, Geschäftsführung bzw. Vorstand auch aus haftungstechnischen Fragen weit mehr als ein notwendiges Übel.



**Andreas Gradl** ist Gründungsgesellschafter bei GCT und als Geschäftsführer für Finanzen, Rechtliches und Organisation verantwortlich.

**GCT** ist seit 1989 Ihr professioneller IT-Dienstleister im Rhein-Main-Gebiet mit Sitz in Bad Homburg v.d.H. Als klassisches IT-Systemhaus betreuen wir Ihre IT im eigenen Haus, als Outsourcer bringen wir Ihre IT in eine private Cloud im GCT Rechenzentrum in Frankfurt am Main oder in die public Cloud namhafter Anbieter und als Managed Service Anbieter liefern wir Ihnen Anwendungen und Security „as a Service“.

# IT Notfall-Planung – Notwendigkeit und Nutzen

Warum der Blick auf die IT-Systeme nicht der richtige Startpunkt ist. Zum Erfolg in sieben Schritten.

Durch die immer größere Abhängigkeit aller Unternehmen von der Datenverarbeitung im Zuge der notwendigen Digitalisierung von Prozessen und ganzen Organisationen gewinnt auch die Notfall-Planung immer mehr an Gewicht. Gerade in KMU können Ausfälle sehr schnell unternehmenskritisch werden, da bereits die Nichtverfügbarkeit von Daten oder bestimmten Services für wenige Stunden oder Tage nicht zu kompensieren ist.

In diesem Whitepaper wollen wir die allgemeine Herangehensweise an das Thema betrachten, die unterschiedlichen Gefahrenbereiche ansprechen und erste Handlungshilfen geben. Die Erfahrung zeigt, dass gerade die „ersten Schritte“ die schwierigsten sind.

Instinktiv wählen viele, die sich an die Erstellung von Notfallplänen machen (müssen), den Ansatz über die physikalisch vorhandenen Systeme und beschränken sich auf die daraus entstehenden Ausfallszenarien. Mit dieser Herangehensweise werden jedoch z. Bsp. ausgelagerte Services nicht erfasst. Auch im eher konservativen Deutschland gibt es nur noch wenige Unternehmen, die sich „der Cloud“ komplett entziehen können. Letztendlich ist daher eine aktuelle IT-Dokumentation ein wichtiges Hilfsmittel zur Notfall-Planung, deckt aber nur Teile des gesamten Szenarios ab. Erst die vom Anwender ausgehende, serviceorientierte Betrachtungsweise ermöglicht die vollständige Behandlung aller für den Unternehmenserfolg wichtigen Aspekte.

Notfallplanung setzt grundlegend eines voraus: Transparenz. Ohne Wissen über die wesentlichen Geschäftsprozesse und die beeinflussenden Faktoren bleibt eine Notfall-Planung Stückwerk und birgt für den „Fall der Fälle“ Risiken.

Daher wählen wir für den Ansatz einer Notfall-Planung immer die Geschäftsprozesse.

## **Schritt 1: Auflistung der (wichtigen Kern-) Prozesse im Unternehmen**

Die Prozessdokumentation ist in vielen Unternehmen aufgrund z. Bsp. einer ISO-Zertifizierung bereits vorhanden. Ansonsten ist die Erstellung elementar und nicht nur für eine Notfall-Planung verwendbar. Auch die EU Datenschutz-Grundverordnung bedingt eine entsprechende Dokumentation. Je nach Unternehmensgröße und einsetzbaren Mitteln (Mitarbeiter, Zeit) können die vermeintlich wichtigsten Prozesse zuerst betrachtet werden. Diese Einschätzung kann sich aber nach Betrachtung vorhandener Abhängigkeiten nochmals verändern.

# IT Notfall-Planung – Notwendigkeit und Nutzen

Sind die Prozesse aufgelistet, nehmen wir eine erste Bewertung vor.

## Schritt 2: Bewertung

Die dokumentierten Prozesse werden einer Bewertung unterzogen. Hierbei beantworten wir die Fragen:

- Wie wichtig ist der Prozess für das Unternehmen insgesamt?
- Wie lang darf der Prozess maximal ausfallen? (Wann kommt es zu ernststen Schwierigkeiten für das Unternehmen (-> Unmöglichkeit der Leistungserbringung -> Schadenersatzforderungen -> Kundenverlust -> Unternehmensuntergang etc.)

Weiterhin betrachten wir auch die für den Prozess benötigten Daten und Informationen:

- Welchen Datenverlust können wir maximal verkraften?
- Wie alt dürfen die nach einem Ausfall wiederhergestellten Daten maximal sein?

Hieraus ergibt sich eine erste Bewertungsmatrix der Prozesse (z.B. Wichtigkeit kritisch, hoch, normal, niedrig).

Nun bestimmen wir die jeden Prozess beeinflussenden Faktoren.

## Schritt 3: Dokumentation aller beeinflussenden Faktoren pro Prozess.

Neben den technischen Elementen (benötigte IT-Systeme etc.) beeinflussen auch andere Faktoren - insbesondere Menschen und Wissen - die Prozesse. Gibt es beispielsweise Spezialwissen, das nur ein oder wenige Mitarbeiter haben? Dieses Wissen muss (nicht nur zur Notfallplanung, sondern auch im allgemeinen Unternehmensinteresse) transparent und für alle Berechtigten zur Verfügung stehen.

Externe Einflüsse wie gesetzliche Bestimmungen und sonstige (branchenspezifische) Auflagen und Vorgaben können wesentlichen Einfluss auf die Bewertung und vor allem das spätere Handeln bei Eintritt eines Notfalls haben. Hier sei nochmals die EU-Datenschutz Grundverordnung (DSGVO) erwähnt, die entsprechende Informationspflichten z.B. bei unbefugten Datenzugriffen vorschreibt. Auch diese müssen wir zu jedem Prozess dokumentieren.

Kommen wir nun zu den möglichen Störungen.

## Schritt 4: Betrachtung der möglichen Gefährdungen und Ausfallszenarien

Die möglichen Gefährdungen sind sehr umfangreich. Um kein Szenario zu übersehen, können wir uns der Hilfe des Bundesamtes für Sicherheit in der Informationstechnik

# IT Notfall-Planung – Notwendigkeit und Nutzen

(BSI) bedienen. Im IT-Grundschutz-Kompendium listet das BSI 47 „Elementare Gefährdungen“ auf, die wir in unsere Überlegungen einbeziehen. Diese sind unter folgendem Link zu finden:

[https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/elementare\\_gefaehrungen/elementare\\_Gefaehrungen\\_Uebersicht\\_node.html](https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/elementare_gefaehrungen/elementare_Gefaehrungen_Uebersicht_node.html)

Jede dieser Gefährdungen bewerten wir daraufhin, ob sich für den betrachteten Prozess eine Handlungsnotwendigkeit ergibt. Jede potentielle Gefährdungssituation versehen wir mit einer Eintrittswahrscheinlichkeit.

Somit haben wir die Grundlage für die Notfall-Behandlung geschaffen. Auf Basis der nun vorliegenden Dokumentation erstellen wir Rollen für die Mitarbeiter, die diese bei Eintritt eines Ausfallszenarios einnehmen.

## **Schritt 5: Erstellen von Rollen für die Notfallbehandlung**

Da es in Notfällen unabdingbar ist, schnell und zielgerichtet zu handeln, beschreiben wir die notwendigen Aufgaben in Rollen. Diese werden von den dafür vorgesehenen Mitarbeitern eingenommen. Wir beschreiben Aufgaben und Befugnisse, damit Notfallteams schnell handeln können. Dabei orientieren wir uns an den unterschiedlichen Ausfallszenarios, gestaffelt nach Eintrittswahrscheinlichkeit.

Als Grundlage für künftiges Handeln dienen Notfall-Dokumente.

## **Schritt 6: Erfassung und Bereitstellung aller benötigten Dokumente und Informationen**

Notfälle gehören glücklicherweise nicht zum Tagesgeschäft und sind in der Regel immer Stresssituationen. Gerade deswegen ist es wichtig, den handelnden Personen alle notwendigen Dokumente und Informationen auf einfache Weise zur Verfügung zu stellen. Alle benötigten Informationen müssen zentral verzeichnet sein und in geeigneter Form bereitstehen. Es bietet sich an, diese digital erfasst in z.B. einem Wiki vorzuhalten. Zusätzlich müssen Vorkehrungen getroffen sein, falls genau dieses System nicht zur Verfügung steht. Eventuell vorgehaltene analoge Dokumente müssen regelmäßig aktualisiert werden. Zu den benötigten Dokumenten gehören Handlungsanweisungen, Ablaufpläne und Checklisten ebenso wie Systemhandbücher, Lage- bzw. Raumpläne und Lizenzinformationen sowie die Kontaktinformationen aller beteiligten Mitarbeiter, Dienstleister, Lieferanten und ggf. Behörden.

Erst zum Abschluss befassen wir uns mit den IT-Systemen.

# IT Notfall-Planung – Notwendigkeit und Nutzen

## Schritt 7: Zuordnung von IT-Systemen zu den betrachteten Prozessen

Vorausgesetzt, es existiert eine aktuelle IT-Dokumentation (Inventarisierung) ordnen wir nun die Prozesse den zu Grunde liegenden IT-Systemen (Server, Netzwerke, Sicherheitssysteme, CloudServices etc.) zu. Andernfalls ist die IT-Dokumentation zwingend zu erstellen. Hierdurch erkennen wir Abhängigkeiten und können auch einzelne IT-Systeme damit in Bezug auf Wichtigkeit, maximal tolerierbare Ausfallzeit etc. bewerten. Somit erkennen wir Handlungsbedarf, wenn entsprechende Systeme die Anforderungen nicht erfüllen können.

### Fazit

Die prozessorientierte Vorgehensweise stellt sicher, dass keine Lücken in der Notfallplanung „übersehen“ werden. Gleichzeitig gibt sie den Entscheidungsträgern im Unternehmen die Möglichkeit, bestehende Risiken zu erkennen und Entscheidungen entsprechend der Dringlichkeit zu steuern. Sie ermöglicht die aus IT-technischer Sicht notwendige Betrachtung als Serviceverbund. (= Summe aller notwendigen Systeme, um dem Anwender einen bestimmten Service oder ein bestimmte „App“ wie z.B. Mail oder CRM zur Verfügung zu stellen.)

Die erarbeiteten Anforderungen und die serviceorientierte Betrachtung bieten eine belastbare Grundlage für Ausschreibungen sowohl für eigene Investitionen und Eigenbetrieb von Systemen und Anlagen als auch für das Outsourcing einzelner Services bis hin zur kompletten IT.

Darüber hinaus wird eine IT Notfallplanung in nahezu allen Fällen auch von Wirtschaftsprüfern und Versicherungen gefordert, beeinflusst unter Umständen das Kreditranking einer Organisation und ist für Inhaber, Geschäftsführung bzw. Vorstand auch aus haftungstechnischen Fragen weit mehr als ein notwendiges Übel.



**Andreas Gradl** ist Gründungsgesellschafter bei GCT und als Geschäftsführer für Finanzen, Rechtliches und Organisation verantwortlich.

**GCT** ist seit 1989 Ihr professioneller IT-Dienstleister im Rhein-Main-Gebiet mit Sitz in Bad Homburg v.d.H. Als klassisches IT-Systemhaus betreuen wir Ihre IT im eigenen Haus, als Outsourcer bringen wir Ihre IT in eine private Cloud im GCT Rechenzentrum in Frankfurt am Main oder in die public Cloud namhafter Anbieter und als Managed Service Anbieter liefern wir Ihnen Anwendungen und Security „as a Service“.



# IT Notfall-Planung – Notwendigkeit und Nutzen

Warum der Blick auf die IT-Systeme nicht der richtige Startpunkt ist. Zum Erfolg in sieben Schritten.

Durch die immer größere Abhängigkeit aller Unternehmen von der Datenverarbeitung im Zuge der notwendigen Digitalisierung von Prozessen und ganzen Organisationen gewinnt auch die Notfall-Planung immer mehr an Gewicht. Gerade in KMU können Ausfälle sehr schnell unternehmenskritisch werden, da bereits die Nichtverfügbarkeit von Daten oder bestimmten Services für wenige Stunden oder Tage nicht zu kompensieren ist.

In diesem Whitepaper wollen wir die allgemeine Herangehensweise an das Thema betrachten, die unterschiedlichen Gefahrenbereiche ansprechen und erste Handlungshilfen geben. Die Erfahrung zeigt, dass gerade die „ersten Schritte“ die schwierigsten sind.

Instinktiv wählen viele, die sich an die Erstellung von Notfallplänen machen (müssen), den Ansatz über die physikalisch vorhandenen Systeme und beschränken sich auf die daraus entstehenden Ausfallszenarien. Mit dieser Herangehensweise werden jedoch z. Bsp. ausgelagerte Services nicht erfasst. Auch im eher konservativen Deutschland gibt es nur noch wenige Unternehmen, die sich „der Cloud“ komplett entziehen können. Letztendlich ist daher eine aktuelle IT-Dokumentation ein wichtiges Hilfsmittel zur Notfall-Planung, deckt aber nur Teile des gesamten Szenarios ab. Erst die vom Anwender ausgehende, serviceorientierte Betrachtungsweise ermöglicht die vollständige Behandlung aller für den Unternehmenserfolg wichtigen Aspekte.

Notfallplanung setzt grundlegend eines voraus: Transparenz. Ohne Wissen über die wesentlichen Geschäftsprozesse und die beeinflussenden Faktoren bleibt eine Notfall-Planung Stückwerk und birgt für den „Fall der Fälle“ Risiken.

Daher wählen wir für den Ansatz einer Notfall-Planung immer die Geschäftsprozesse.

## **Schritt 1: Auflistung der (wichtigen Kern-) Prozesse im Unternehmen**

Die Prozessdokumentation ist in vielen Unternehmen aufgrund z. Bsp. einer ISO-Zertifizierung bereits vorhanden. Ansonsten ist die Erstellung elementar und nicht nur für eine Notfall-Planung verwendbar. Auch die EU Datenschutz-Grundverordnung bedingt eine entsprechende Dokumentation. Je nach Unternehmensgröße und einsetzbaren Mitteln (Mitarbeiter, Zeit) können die vermeintlich wichtigsten Prozesse zuerst betrachtet werden. Diese Einschätzung kann sich aber nach Betrachtung vorhandener Abhängigkeiten nochmals verändern.

# IT Notfall-Planung – Notwendigkeit und Nutzen

Sind die Prozesse aufgelistet, nehmen wir eine erste Bewertung vor.

## Schritt 2: Bewertung

Die dokumentierten Prozesse werden einer Bewertung unterzogen. Hierbei beantworten wir die Fragen:

- Wie wichtig ist der Prozess für das Unternehmen insgesamt?
- Wie lang darf der Prozess maximal ausfallen? (Wann kommt es zu ernststen Schwierigkeiten für das Unternehmen (-> Unmöglichkeit der Leistungserbringung -> Schadenersatzforderungen -> Kundenverlust -> Unternehmensuntergang etc.)

Weiterhin betrachten wir auch die für den Prozess benötigten Daten und Informationen:

- Welchen Datenverlust können wir maximal verkraften?
- Wie alt dürfen die nach einem Ausfall wiederhergestellten Daten maximal sein?

Hieraus ergibt sich eine erste Bewertungsmatrix der Prozesse (z.B. Wichtigkeit kritisch, hoch, normal, niedrig).

Nun bestimmen wir die jeden Prozess beeinflussenden Faktoren.

## Schritt 3: Dokumentation aller beeinflussenden Faktoren pro Prozess.

Neben den technischen Elementen (benötigte IT-Systeme etc.) beeinflussen auch andere Faktoren - insbesondere Menschen und Wissen - die Prozesse. Gibt es beispielsweise Spezialwissen, das nur ein oder wenige Mitarbeiter haben? Dieses Wissen muss (nicht nur zur Notfallplanung, sondern auch im allgemeinen Unternehmensinteresse) transparent und für alle Berechtigten zur Verfügung stehen.

Externe Einflüsse wie gesetzliche Bestimmungen und sonstige (branchenspezifische) Auflagen und Vorgaben können wesentlichen Einfluss auf die Bewertung und vor allem das spätere Handeln bei Eintritt eines Notfalls haben. Hier sei nochmals die EU-Datenschutz Grundverordnung (DSGVO) erwähnt, die entsprechende Informationspflichten z.B. bei unbefugten Datenzugriffen vorschreibt. Auch diese müssen wir zu jedem Prozess dokumentieren.

Kommen wir nun zu den möglichen Störungen.

## Schritt 4: Betrachtung der möglichen Gefährdungen und Ausfallszenarien

Die möglichen Gefährdungen sind sehr umfangreich. Um kein Szenario zu übersehen, können wir uns der Hilfe des Bundesamtes für Sicherheit in der Informationstechnik

# IT Notfall-Planung – Notwendigkeit und Nutzen

(BSI) bedienen. Im IT-Grundschutz-Kompendium listet das BSI 47 „Elementare Gefährdungen“ auf, die wir in unsere Überlegungen einbeziehen. Diese sind unter folgendem Link zu finden:

[https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/elementare\\_gefaehrungen/elementare\\_Gefaehrungen\\_Uebersicht\\_node.html](https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/elementare_gefaehrungen/elementare_Gefaehrungen_Uebersicht_node.html)

Jede dieser Gefährdungen bewerten wir daraufhin, ob sich für den betrachteten Prozess eine Handlungsnotwendigkeit ergibt. Jede potentielle Gefährdungssituation versehen wir mit einer Eintrittswahrscheinlichkeit.

Somit haben wir die Grundlage für die Notfall-Behandlung geschaffen. Auf Basis der nun vorliegenden Dokumentation erstellen wir Rollen für die Mitarbeiter, die diese bei Eintritt eines Ausfallszenarios einnehmen.

## **Schritt 5: Erstellen von Rollen für die Notfallbehandlung**

Da es in Notfällen unabdingbar ist, schnell und zielgerichtet zu handeln, beschreiben wir die notwendigen Aufgaben in Rollen. Diese werden von den dafür vorgesehenen Mitarbeitern eingenommen. Wir beschreiben Aufgaben und Befugnisse, damit Notfallteams schnell handeln können. Dabei orientieren wir uns an den unterschiedlichen Ausfallszenarios, gestaffelt nach Eintrittswahrscheinlichkeit.

Als Grundlage für künftiges Handeln dienen Notfall-Dokumente.

## **Schritt 6: Erfassung und Bereitstellung aller benötigten Dokumente und Informationen**

Notfälle gehören glücklicherweise nicht zum Tagesgeschäft und sind in der Regel immer Stresssituationen. Gerade deswegen ist es wichtig, den handelnden Personen alle notwendigen Dokumente und Informationen auf einfache Weise zur Verfügung zu stellen. Alle benötigten Informationen müssen zentral verzeichnet sein und in geeigneter Form bereitstehen. Es bietet sich an, diese digital erfasst in z.B. einem Wiki vorzuhalten. Zusätzlich müssen Vorkehrungen getroffen sein, falls genau dieses System nicht zur Verfügung steht. Eventuell vorgehaltene analoge Dokumente müssen regelmäßig aktualisiert werden. Zu den benötigten Dokumenten gehören Handlungsanweisungen, Ablaufpläne und Checklisten ebenso wie Systemhandbücher, Lage- bzw. Raumpläne und Lizenzinformationen sowie die Kontaktinformationen aller beteiligten Mitarbeiter, Dienstleister, Lieferanten und ggf. Behörden.

Erst zum Abschluss befassen wir uns mit den IT-Systemen.

# IT Notfall-Planung – Notwendigkeit und Nutzen

## Schritt 7: Zuordnung von IT-Systemen zu den betrachteten Prozessen

Vorausgesetzt, es existiert eine aktuelle IT-Dokumentation (Inventarisierung) ordnen wir nun die Prozesse den zu Grunde liegenden IT-Systemen (Server, Netzwerke, Sicherheitssysteme, CloudServices etc.) zu. Andernfalls ist die IT-Dokumentation zwingend zu erstellen. Hierdurch erkennen wir Abhängigkeiten und können auch einzelne IT-Systeme damit in Bezug auf Wichtigkeit, maximal tolerierbare Ausfallzeit etc. bewerten. Somit erkennen wir Handlungsbedarf, wenn entsprechende Systeme die Anforderungen nicht erfüllen können.

### Fazit

Die prozessorientierte Vorgehensweise stellt sicher, dass keine Lücken in der Notfallplanung „übersehen“ werden. Gleichzeitig gibt sie den Entscheidungsträgern im Unternehmen die Möglichkeit, bestehende Risiken zu erkennen und Entscheidungen entsprechend der Dringlichkeit zu steuern. Sie ermöglicht die aus IT-technischer Sicht notwendige Betrachtung als Serviceverbund. (= Summe aller notwendigen Systeme, um dem Anwender einen bestimmten Service oder ein bestimmte „App“ wie z.B. Mail oder CRM zur Verfügung zu stellen.)

Die erarbeiteten Anforderungen und die serviceorientierte Betrachtung bieten eine belastbare Grundlage für Ausschreibungen sowohl für eigene Investitionen und Eigenbetrieb von Systemen und Anlagen als auch für das Outsourcing einzelner Services bis hin zur kompletten IT.

Darüber hinaus wird eine IT Notfallplanung in nahezu allen Fällen auch von Wirtschaftsprüfern und Versicherungen gefordert, beeinflusst unter Umständen das Kreditranking einer Organisation und ist für Inhaber, Geschäftsführung bzw. Vorstand auch aus haftungstechnischen Fragen weit mehr als ein notwendiges Übel.



**Andreas Gradl** ist Gründungsgesellschafter bei GCT und als Geschäftsführer für Finanzen, Rechtliches und Organisation verantwortlich.

**GCT** ist seit 1989 Ihr professioneller IT-Dienstleister im Rhein-Main-Gebiet mit Sitz in Bad Homburg v.d.H. Als klassisches IT-Systemhaus betreuen wir Ihre IT im eigenen Haus, als Outsourcer bringen wir Ihre IT in eine private Cloud im GCT Rechenzentrum in Frankfurt am Main oder in die public Cloud namhafter Anbieter und als Managed Service Anbieter liefern wir Ihnen Anwendungen und Security „as a Service“.

# IT Notfall-Planung – Notwendigkeit und Nutzen

Warum der Blick auf die IT-Systeme nicht der richtige Startpunkt ist. Zum Erfolg in sieben Schritten.

Durch die immer größere Abhängigkeit aller Unternehmen von der Datenverarbeitung im Zuge der notwendigen Digitalisierung von Prozessen und ganzen Organisationen gewinnt auch die Notfall-Planung immer mehr an Gewicht. Gerade in KMU können Ausfälle sehr schnell unternehmenskritisch werden, da bereits die Nichtverfügbarkeit von Daten oder bestimmten Services für wenige Stunden oder Tage nicht zu kompensieren ist.

In diesem Whitepaper wollen wir die allgemeine Herangehensweise an das Thema betrachten, die unterschiedlichen Gefahrenbereiche ansprechen und erste Handlungshilfen geben. Die Erfahrung zeigt, dass gerade die „ersten Schritte“ die schwierigsten sind.

Instinktiv wählen viele, die sich an die Erstellung von Notfallplänen machen (müssen), den Ansatz über die physikalisch vorhandenen Systeme und beschränken sich auf die daraus entstehenden Ausfallszenarien. Mit dieser Herangehensweise werden jedoch z. Bsp. ausgelagerte Services nicht erfasst. Auch im eher konservativen Deutschland gibt es nur noch wenige Unternehmen, die sich „der Cloud“ komplett entziehen können. Letztendlich ist daher eine aktuelle IT-Dokumentation ein wichtiges Hilfsmittel zur Notfall-Planung, deckt aber nur Teile des gesamten Szenarios ab. Erst die vom Anwender ausgehende, serviceorientierte Betrachtungsweise ermöglicht die vollständige Behandlung aller für den Unternehmenserfolg wichtigen Aspekte.

Notfallplanung setzt grundlegend eines voraus: Transparenz. Ohne Wissen über die wesentlichen Geschäftsprozesse und die beeinflussenden Faktoren bleibt eine Notfall-Planung Stückwerk und birgt für den „Fall der Fälle“ Risiken.

Daher wählen wir für den Ansatz einer Notfall-Planung immer die Geschäftsprozesse.

## **Schritt 1: Auflistung der (wichtigen Kern-) Prozesse im Unternehmen**

Die Prozessdokumentation ist in vielen Unternehmen aufgrund z. Bsp. einer ISO-Zertifizierung bereits vorhanden. Ansonsten ist die Erstellung elementar und nicht nur für eine Notfall-Planung verwendbar. Auch die EU Datenschutz-Grundverordnung bedingt eine entsprechende Dokumentation. Je nach Unternehmensgröße und einsetzbaren Mitteln (Mitarbeiter, Zeit) können die vermeintlich wichtigsten Prozesse zuerst betrachtet werden. Diese Einschätzung kann sich aber nach Betrachtung vorhandener Abhängigkeiten nochmals verändern.

# IT Notfall-Planung – Notwendigkeit und Nutzen

Sind die Prozesse aufgelistet, nehmen wir eine erste Bewertung vor.

## Schritt 2: Bewertung

Die dokumentierten Prozesse werden einer Bewertung unterzogen. Hierbei beantworten wir die Fragen:

- Wie wichtig ist der Prozess für das Unternehmen insgesamt?
- Wie lang darf der Prozess maximal ausfallen? (Wann kommt es zu ernststen Schwierigkeiten für das Unternehmen (-> Unmöglichkeit der Leistungserbringung -> Schadenersatzforderungen -> Kundenverlust -> Unternehmensuntergang etc.)

Weiterhin betrachten wir auch die für den Prozess benötigten Daten und Informationen:

- Welchen Datenverlust können wir maximal verkraften?
- Wie alt dürfen die nach einem Ausfall wiederhergestellten Daten maximal sein?

Hieraus ergibt sich eine erste Bewertungsmatrix der Prozesse (z.B. Wichtigkeit kritisch, hoch, normal, niedrig).

Nun bestimmen wir die jeden Prozess beeinflussenden Faktoren.

## Schritt 3: Dokumentation aller beeinflussenden Faktoren pro Prozess.

Neben den technischen Elementen (benötigte IT-Systeme etc.) beeinflussen auch andere Faktoren - insbesondere Menschen und Wissen - die Prozesse. Gibt es beispielsweise Spezialwissen, das nur ein oder wenige Mitarbeiter haben? Dieses Wissen muss (nicht nur zur Notfallplanung, sondern auch im allgemeinen Unternehmensinteresse) transparent und für alle Berechtigten zur Verfügung stehen.

Externe Einflüsse wie gesetzliche Bestimmungen und sonstige (branchenspezifische) Auflagen und Vorgaben können wesentlichen Einfluss auf die Bewertung und vor allem das spätere Handeln bei Eintritt eines Notfalls haben. Hier sei nochmals die EU-Datenschutz Grundverordnung (DSGVO) erwähnt, die entsprechende Informationspflichten z.B. bei unbefugten Datenzugriffen vorschreibt. Auch diese müssen wir zu jedem Prozess dokumentieren.

Kommen wir nun zu den möglichen Störungen.

## Schritt 4: Betrachtung der möglichen Gefährdungen und Ausfallszenarien

Die möglichen Gefährdungen sind sehr umfangreich. Um kein Szenario zu übersehen, können wir uns der Hilfe des Bundesamtes für Sicherheit in der Informationstechnik

# IT Notfall-Planung – Notwendigkeit und Nutzen

(BSI) bedienen. Im IT-Grundschutz-Kompendium listet das BSI 47 „Elementare Gefährdungen“ auf, die wir in unsere Überlegungen einbeziehen. Diese sind unter folgendem Link zu finden:

[https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/elementare\\_gefaehrungen/elementare\\_Gefaehrungen\\_Uebersicht\\_node.html](https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/elementare_gefaehrungen/elementare_Gefaehrungen_Uebersicht_node.html)

Jede dieser Gefährdungen bewerten wir daraufhin, ob sich für den betrachteten Prozess eine Handlungsnotwendigkeit ergibt. Jede potentielle Gefährdungssituation versehen wir mit einer Eintrittswahrscheinlichkeit.

Somit haben wir die Grundlage für die Notfall-Behandlung geschaffen. Auf Basis der nun vorliegenden Dokumentation erstellen wir Rollen für die Mitarbeiter, die diese bei Eintritt eines Ausfallszenarios einnehmen.

## **Schritt 5: Erstellen von Rollen für die Notfallbehandlung**

Da es in Notfällen unabdingbar ist, schnell und zielgerichtet zu handeln, beschreiben wir die notwendigen Aufgaben in Rollen. Diese werden von den dafür vorgesehenen Mitarbeitern eingenommen. Wir beschreiben Aufgaben und Befugnisse, damit Notfallteams schnell handeln können. Dabei orientieren wir uns an den unterschiedlichen Ausfallszenarios, gestaffelt nach Eintrittswahrscheinlichkeit.

Als Grundlage für künftiges Handeln dienen Notfall-Dokumente.

## **Schritt 6: Erfassung und Bereitstellung aller benötigten Dokumente und Informationen**

Notfälle gehören glücklicherweise nicht zum Tagesgeschäft und sind in der Regel immer Stresssituationen. Gerade deswegen ist es wichtig, den handelnden Personen alle notwendigen Dokumente und Informationen auf einfache Weise zur Verfügung zu stellen. Alle benötigten Informationen müssen zentral verzeichnet sein und in geeigneter Form bereitstehen. Es bietet sich an, diese digital erfasst in z.B. einem Wiki vorzuhalten. Zusätzlich müssen Vorkehrungen getroffen sein, falls genau dieses System nicht zur Verfügung steht. Eventuell vorgehaltene analoge Dokumente müssen regelmäßig aktualisiert werden. Zu den benötigten Dokumenten gehören Handlungsanweisungen, Ablaufpläne und Checklisten ebenso wie Systemhandbücher, Lage- bzw. Raumpläne und Lizenzinformationen sowie die Kontaktinformationen aller beteiligten Mitarbeiter, Dienstleister, Lieferanten und ggf. Behörden.

Erst zum Abschluss befassen wir uns mit den IT-Systemen.

# IT Notfall-Planung – Notwendigkeit und Nutzen

## Schritt 7: Zuordnung von IT-Systemen zu den betrachteten Prozessen

Vorausgesetzt, es existiert eine aktuelle IT-Dokumentation (Inventarisierung) ordnen wir nun die Prozesse den zu Grunde liegenden IT-Systemen (Server, Netzwerke, Sicherheitssysteme, CloudServices etc.) zu. Andernfalls ist die IT-Dokumentation zwingend zu erstellen. Hierdurch erkennen wir Abhängigkeiten und können auch einzelne IT-Systeme damit in Bezug auf Wichtigkeit, maximal tolerierbare Ausfallzeit etc. bewerten. Somit erkennen wir Handlungsbedarf, wenn entsprechende Systeme die Anforderungen nicht erfüllen können.

### Fazit

Die prozessorientierte Vorgehensweise stellt sicher, dass keine Lücken in der Notfallplanung „übersehen“ werden. Gleichzeitig gibt sie den Entscheidungsträgern im Unternehmen die Möglichkeit, bestehende Risiken zu erkennen und Entscheidungen entsprechend der Dringlichkeit zu steuern. Sie ermöglicht die aus IT-technischer Sicht notwendige Betrachtung als Serviceverbund. (= Summe aller notwendigen Systeme, um dem Anwender einen bestimmten Service oder ein bestimmte „App“ wie z.B. Mail oder CRM zur Verfügung zu stellen.)

Die erarbeiteten Anforderungen und die serviceorientierte Betrachtung bieten eine belastbare Grundlage für Ausschreibungen sowohl für eigene Investitionen und Eigenbetrieb von Systemen und Anlagen als auch für das Outsourcing einzelner Services bis hin zur kompletten IT.

Darüber hinaus wird eine IT Notfallplanung in nahezu allen Fällen auch von Wirtschaftsprüfern und Versicherungen gefordert, beeinflusst unter Umständen das Kreditranking einer Organisation und ist für Inhaber, Geschäftsführung bzw. Vorstand auch aus haftungstechnischen Fragen weit mehr als ein notwendiges Übel.



**Andreas Gradl** ist Gründungsgesellschafter bei GCT und als Geschäftsführer für Finanzen, Rechtliches und Organisation verantwortlich.

**GCT** ist seit 1989 Ihr professioneller IT-Dienstleister im Rhein-Main-Gebiet mit Sitz in Bad Homburg v.d.H. Als klassisches IT-Systemhaus betreuen wir Ihre IT im eigenen Haus, als Outsourcer bringen wir Ihre IT in eine private Cloud im GCT Rechenzentrum in Frankfurt am Main oder in die public Cloud namhafter Anbieter und als Managed Service Anbieter liefern wir Ihnen Anwendungen und Security „as a Service“.



# IT Notfall-Planung – Notwendigkeit und Nutzen

Warum der Blick auf die IT-Systeme nicht der richtige Startpunkt ist. Zum Erfolg in sieben Schritten.

Durch die immer größere Abhängigkeit aller Unternehmen von der Datenverarbeitung im Zuge der notwendigen Digitalisierung von Prozessen und ganzen Organisationen gewinnt auch die Notfall-Planung immer mehr an Gewicht. Gerade in KMU können Ausfälle sehr schnell unternehmenskritisch werden, da bereits die Nichtverfügbarkeit von Daten oder bestimmten Services für wenige Stunden oder Tage nicht zu kompensieren ist.

In diesem Whitepaper wollen wir die allgemeine Herangehensweise an das Thema betrachten, die unterschiedlichen Gefahrenbereiche ansprechen und erste Handlungshilfen geben. Die Erfahrung zeigt, dass gerade die „ersten Schritte“ die schwierigsten sind.

Instinktiv wählen viele, die sich an die Erstellung von Notfallplänen machen (müssen), den Ansatz über die physikalisch vorhandenen Systeme und beschränken sich auf die daraus entstehenden Ausfallszenarien. Mit dieser Herangehensweise werden jedoch z. Bsp. ausgelagerte Services nicht erfasst. Auch im eher konservativen Deutschland gibt es nur noch wenige Unternehmen, die sich „der Cloud“ komplett entziehen können. Letztendlich ist daher eine aktuelle IT-Dokumentation ein wichtiges Hilfsmittel zur Notfall-Planung, deckt aber nur Teile des gesamten Szenarios ab. Erst die vom Anwender ausgehende, serviceorientierte Betrachtungsweise ermöglicht die vollständige Behandlung aller für den Unternehmenserfolg wichtigen Aspekte.

Notfallplanung setzt grundlegend eines voraus: Transparenz. Ohne Wissen über die wesentlichen Geschäftsprozesse und die beeinflussenden Faktoren bleibt eine Notfall-Planung Stückwerk und birgt für den „Fall der Fälle“ Risiken.

Daher wählen wir für den Ansatz einer Notfall-Planung immer die Geschäftsprozesse.

## **Schritt 1: Auflistung der (wichtigen Kern-) Prozesse im Unternehmen**

Die Prozessdokumentation ist in vielen Unternehmen aufgrund z. Bsp. einer ISO-Zertifizierung bereits vorhanden. Ansonsten ist die Erstellung elementar und nicht nur für eine Notfall-Planung verwendbar. Auch die EU Datenschutz-Grundverordnung bedingt eine entsprechende Dokumentation. Je nach Unternehmensgröße und einsetzbaren Mitteln (Mitarbeiter, Zeit) können die vermeintlich wichtigsten Prozesse zuerst betrachtet werden. Diese Einschätzung kann sich aber nach Betrachtung vorhandener Abhängigkeiten nochmals verändern.

# IT Notfall-Planung – Notwendigkeit und Nutzen

Sind die Prozesse aufgelistet, nehmen wir eine erste Bewertung vor.

## Schritt 2: Bewertung

Die dokumentierten Prozesse werden einer Bewertung unterzogen. Hierbei beantworten wir die Fragen:

- Wie wichtig ist der Prozess für das Unternehmen insgesamt?
- Wie lang darf der Prozess maximal ausfallen? (Wann kommt es zu ernststen Schwierigkeiten für das Unternehmen (-> Unmöglichkeit der Leistungserbringung -> Schadenersatzforderungen -> Kundenverlust -> Unternehmensuntergang etc.)

Weiterhin betrachten wir auch die für den Prozess benötigten Daten und Informationen:

- Welchen Datenverlust können wir maximal verkraften?
- Wie alt dürfen die nach einem Ausfall wiederhergestellten Daten maximal sein?

Hieraus ergibt sich eine erste Bewertungsmatrix der Prozesse (z.B. Wichtigkeit kritisch, hoch, normal, niedrig).

Nun bestimmen wir die jeden Prozess beeinflussenden Faktoren.

## Schritt 3: Dokumentation aller beeinflussenden Faktoren pro Prozess.

Neben den technischen Elementen (benötigte IT-Systeme etc.) beeinflussen auch andere Faktoren - insbesondere Menschen und Wissen - die Prozesse. Gibt es beispielsweise Spezialwissen, das nur ein oder wenige Mitarbeiter haben? Dieses Wissen muss (nicht nur zur Notfallplanung, sondern auch im allgemeinen Unternehmensinteresse) transparent und für alle Berechtigten zur Verfügung stehen.

Externe Einflüsse wie gesetzliche Bestimmungen und sonstige (branchenspezifische) Auflagen und Vorgaben können wesentlichen Einfluss auf die Bewertung und vor allem das spätere Handeln bei Eintritt eines Notfalls haben. Hier sei nochmals die EU-Datenschutz Grundverordnung (DSGVO) erwähnt, die entsprechende Informationspflichten z.B. bei unbefugten Datenzugriffen vorschreibt. Auch diese müssen wir zu jedem Prozess dokumentieren.

Kommen wir nun zu den möglichen Störungen.

## Schritt 4: Betrachtung der möglichen Gefährdungen und Ausfallszenarien

Die möglichen Gefährdungen sind sehr umfangreich. Um kein Szenario zu übersehen, können wir uns der Hilfe des Bundesamtes für Sicherheit in der Informationstechnik

# IT Notfall-Planung – Notwendigkeit und Nutzen

(BSI) bedienen. Im IT-Grundschutz-Kompendium listet das BSI 47 „Elementare Gefährdungen“ auf, die wir in unsere Überlegungen einbeziehen. Diese sind unter folgendem Link zu finden:

[https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/elementare\\_gefaehrungen/elementare\\_Gefaehrungen\\_Uebersicht\\_node.html](https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/elementare_gefaehrungen/elementare_Gefaehrungen_Uebersicht_node.html)

Jede dieser Gefährdungen bewerten wir daraufhin, ob sich für den betrachteten Prozess eine Handlungsnotwendigkeit ergibt. Jede potentielle Gefährdungssituation versehen wir mit einer Eintrittswahrscheinlichkeit.

Somit haben wir die Grundlage für die Notfall-Behandlung geschaffen. Auf Basis der nun vorliegenden Dokumentation erstellen wir Rollen für die Mitarbeiter, die diese bei Eintritt eines Ausfallszenarios einnehmen.

## **Schritt 5: Erstellen von Rollen für die Notfallbehandlung**

Da es in Notfällen unabdingbar ist, schnell und zielgerichtet zu handeln, beschreiben wir die notwendigen Aufgaben in Rollen. Diese werden von den dafür vorgesehenen Mitarbeitern eingenommen. Wir beschreiben Aufgaben und Befugnisse, damit Notfallteams schnell handeln können. Dabei orientieren wir uns an den unterschiedlichen Ausfallszenarios, gestaffelt nach Eintrittswahrscheinlichkeit.

Als Grundlage für künftiges Handeln dienen Notfall-Dokumente.

## **Schritt 6: Erfassung und Bereitstellung aller benötigten Dokumente und Informationen**

Notfälle gehören glücklicherweise nicht zum Tagesgeschäft und sind in der Regel immer Stresssituationen. Gerade deswegen ist es wichtig, den handelnden Personen alle notwendigen Dokumente und Informationen auf einfache Weise zur Verfügung zu stellen. Alle benötigten Informationen müssen zentral verzeichnet sein und in geeigneter Form bereitstehen. Es bietet sich an, diese digital erfasst in z.B. einem Wiki vorzuhalten. Zusätzlich müssen Vorkehrungen getroffen sein, falls genau dieses System nicht zur Verfügung steht. Eventuell vorgehaltene analoge Dokumente müssen regelmäßig aktualisiert werden. Zu den benötigten Dokumenten gehören Handlungsanweisungen, Ablaufpläne und Checklisten ebenso wie Systemhandbücher, Lage- bzw. Raumpläne und Lizenzinformationen sowie die Kontaktinformationen aller beteiligten Mitarbeiter, Dienstleister, Lieferanten und ggf. Behörden.

Erst zum Abschluss befassen wir uns mit den IT-Systemen.

# IT Notfall-Planung – Notwendigkeit und Nutzen

## Schritt 7: Zuordnung von IT-Systemen zu den betrachteten Prozessen

Vorausgesetzt, es existiert eine aktuelle IT-Dokumentation (Inventarisierung) ordnen wir nun die Prozesse den zu Grunde liegenden IT-Systemen (Server, Netzwerke, Sicherheitssysteme, CloudServices etc.) zu. Andernfalls ist die IT-Dokumentation zwingend zu erstellen. Hierdurch erkennen wir Abhängigkeiten und können auch einzelne IT-Systeme damit in Bezug auf Wichtigkeit, maximal tolerierbare Ausfallzeit etc. bewerten. Somit erkennen wir Handlungsbedarf, wenn entsprechende Systeme die Anforderungen nicht erfüllen können.

### Fazit

Die prozessorientierte Vorgehensweise stellt sicher, dass keine Lücken in der Notfallplanung „übersehen“ werden. Gleichzeitig gibt sie den Entscheidungsträgern im Unternehmen die Möglichkeit, bestehende Risiken zu erkennen und Entscheidungen entsprechend der Dringlichkeit zu steuern. Sie ermöglicht die aus IT-technischer Sicht notwendige Betrachtung als Serviceverbund. (= Summe aller notwendigen Systeme, um dem Anwender einen bestimmten Service oder ein bestimmte „App“ wie z.B. Mail oder CRM zur Verfügung zu stellen.)

Die erarbeiteten Anforderungen und die serviceorientierte Betrachtung bieten eine belastbare Grundlage für Ausschreibungen sowohl für eigene Investitionen und Eigenbetrieb von Systemen und Anlagen als auch für das Outsourcing einzelner Services bis hin zur kompletten IT.

Darüber hinaus wird eine IT Notfallplanung in nahezu allen Fällen auch von Wirtschaftsprüfern und Versicherungen gefordert, beeinflusst unter Umständen das Kreditranking einer Organisation und ist für Inhaber, Geschäftsführung bzw. Vorstand auch aus haftungstechnischen Fragen weit mehr als ein notwendiges Übel.



**Andreas Gradl** ist Gründungsgesellschafter bei GCT und als Geschäftsführer für Finanzen, Rechtliches und Organisation verantwortlich.

**GCT** ist seit 1989 Ihr professioneller IT-Dienstleister im Rhein-Main-Gebiet mit Sitz in Bad Homburg v.d.H. Als klassisches IT-Systemhaus betreuen wir Ihre IT im eigenen Haus, als Outsourcer bringen wir Ihre IT in eine private Cloud im GCT Rechenzentrum in Frankfurt am Main oder in die public Cloud namhafter Anbieter und als Managed Service Anbieter liefern wir Ihnen Anwendungen und Security „as a Service“.

# IT Notfall-Planung – Notwendigkeit und Nutzen

Warum der Blick auf die IT-Systeme nicht der richtige Startpunkt ist. Zum Erfolg in sieben Schritten.

Durch die immer größere Abhängigkeit aller Unternehmen von der Datenverarbeitung im Zuge der notwendigen Digitalisierung von Prozessen und ganzen Organisationen gewinnt auch die Notfall-Planung immer mehr an Gewicht. Gerade in KMU können Ausfälle sehr schnell unternehmenskritisch werden, da bereits die Nichtverfügbarkeit von Daten oder bestimmten Services für wenige Stunden oder Tage nicht zu kompensieren ist.

In diesem Whitepaper wollen wir die allgemeine Herangehensweise an das Thema betrachten, die unterschiedlichen Gefahrenbereiche ansprechen und erste Handlungshilfen geben. Die Erfahrung zeigt, dass gerade die „ersten Schritte“ die schwierigsten sind.

Instinktiv wählen viele, die sich an die Erstellung von Notfallplänen machen (müssen), den Ansatz über die physikalisch vorhandenen Systeme und beschränken sich auf die daraus entstehenden Ausfallszenarien. Mit dieser Herangehensweise werden jedoch z. Bsp. ausgelagerte Services nicht erfasst. Auch im eher konservativen Deutschland gibt es nur noch wenige Unternehmen, die sich „der Cloud“ komplett entziehen können. Letztendlich ist daher eine aktuelle IT-Dokumentation ein wichtiges Hilfsmittel zur Notfall-Planung, deckt aber nur Teile des gesamten Szenarios ab. Erst die vom Anwender ausgehende, serviceorientierte Betrachtungsweise ermöglicht die vollständige Behandlung aller für den Unternehmenserfolg wichtigen Aspekte.

Notfallplanung setzt grundlegend eines voraus: Transparenz. Ohne Wissen über die wesentlichen Geschäftsprozesse und die beeinflussenden Faktoren bleibt eine Notfall-Planung Stückwerk und birgt für den „Fall der Fälle“ Risiken.

Daher wählen wir für den Ansatz einer Notfall-Planung immer die Geschäftsprozesse.

## **Schritt 1: Auflistung der (wichtigen Kern-) Prozesse im Unternehmen**

Die Prozessdokumentation ist in vielen Unternehmen aufgrund z. Bsp. einer ISO-Zertifizierung bereits vorhanden. Ansonsten ist die Erstellung elementar und nicht nur für eine Notfall-Planung verwendbar. Auch die EU Datenschutz-Grundverordnung bedingt eine entsprechende Dokumentation. Je nach Unternehmensgröße und einsetzbaren Mitteln (Mitarbeiter, Zeit) können die vermeintlich wichtigsten Prozesse zuerst betrachtet werden. Diese Einschätzung kann sich aber nach Betrachtung vorhandener Abhängigkeiten nochmals verändern.

# IT Notfall-Planung – Notwendigkeit und Nutzen

Sind die Prozesse aufgelistet, nehmen wir eine erste Bewertung vor.

## Schritt 2: Bewertung

Die dokumentierten Prozesse werden einer Bewertung unterzogen. Hierbei beantworten wir die Fragen:

- Wie wichtig ist der Prozess für das Unternehmen insgesamt?
- Wie lang darf der Prozess maximal ausfallen? (Wann kommt es zu ernststen Schwierigkeiten für das Unternehmen (-> Unmöglichkeit der Leistungserbringung -> Schadenersatzforderungen -> Kundenverlust -> Unternehmensuntergang etc.)

Weiterhin betrachten wir auch die für den Prozess benötigten Daten und Informationen:

- Welchen Datenverlust können wir maximal verkraften?
- Wie alt dürfen die nach einem Ausfall wiederhergestellten Daten maximal sein?

Hieraus ergibt sich eine erste Bewertungsmatrix der Prozesse (z.B. Wichtigkeit kritisch, hoch, normal, niedrig).

Nun bestimmen wir die jeden Prozess beeinflussenden Faktoren.

## Schritt 3: Dokumentation aller beeinflussenden Faktoren pro Prozess.

Neben den technischen Elementen (benötigte IT-Systeme etc.) beeinflussen auch andere Faktoren - insbesondere Menschen und Wissen - die Prozesse. Gibt es beispielsweise Spezialwissen, das nur ein oder wenige Mitarbeiter haben? Dieses Wissen muss (nicht nur zur Notfallplanung, sondern auch im allgemeinen Unternehmensinteresse) transparent und für alle Berechtigten zur Verfügung stehen.

Externe Einflüsse wie gesetzliche Bestimmungen und sonstige (branchenspezifische) Auflagen und Vorgaben können wesentlichen Einfluss auf die Bewertung und vor allem das spätere Handeln bei Eintritt eines Notfalls haben. Hier sei nochmals die EU-Datenschutz Grundverordnung (DSGVO) erwähnt, die entsprechende Informationspflichten z.B. bei unbefugten Datenzugriffen vorschreibt. Auch diese müssen wir zu jedem Prozess dokumentieren.

Kommen wir nun zu den möglichen Störungen.

## Schritt 4: Betrachtung der möglichen Gefährdungen und Ausfallszenarien

Die möglichen Gefährdungen sind sehr umfangreich. Um kein Szenario zu übersehen, können wir uns der Hilfe des Bundesamtes für Sicherheit in der Informationstechnik

# IT Notfall-Planung – Notwendigkeit und Nutzen

(BSI) bedienen. Im IT-Grundschutz-Kompendium listet das BSI 47 „Elementare Gefährdungen“ auf, die wir in unsere Überlegungen einbeziehen. Diese sind unter folgendem Link zu finden:

[https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/elementare\\_gefaehrungen/elementare\\_Gefaehrungen\\_Uebersicht\\_node.html](https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/elementare_gefaehrungen/elementare_Gefaehrungen_Uebersicht_node.html)

Jede dieser Gefährdungen bewerten wir daraufhin, ob sich für den betrachteten Prozess eine Handlungsnotwendigkeit ergibt. Jede potentielle Gefährdungssituation versehen wir mit einer Eintrittswahrscheinlichkeit.

Somit haben wir die Grundlage für die Notfall-Behandlung geschaffen. Auf Basis der nun vorliegenden Dokumentation erstellen wir Rollen für die Mitarbeiter, die diese bei Eintritt eines Ausfallszenarios einnehmen.

## **Schritt 5: Erstellen von Rollen für die Notfallbehandlung**

Da es in Notfällen unabdingbar ist, schnell und zielgerichtet zu handeln, beschreiben wir die notwendigen Aufgaben in Rollen. Diese werden von den dafür vorgesehenen Mitarbeitern eingenommen. Wir beschreiben Aufgaben und Befugnisse, damit Notfallteams schnell handeln können. Dabei orientieren wir uns an den unterschiedlichen Ausfallszenarios, gestaffelt nach Eintrittswahrscheinlichkeit.

Als Grundlage für künftiges Handeln dienen Notfall-Dokumente.

## **Schritt 6: Erfassung und Bereitstellung aller benötigten Dokumente und Informationen**

Notfälle gehören glücklicherweise nicht zum Tagesgeschäft und sind in der Regel immer Stresssituationen. Gerade deswegen ist es wichtig, den handelnden Personen alle notwendigen Dokumente und Informationen auf einfache Weise zur Verfügung zu stellen. Alle benötigten Informationen müssen zentral verzeichnet sein und in geeigneter Form bereitstehen. Es bietet sich an, diese digital erfasst in z.B. einem Wiki vorzuhalten. Zusätzlich müssen Vorkehrungen getroffen sein, falls genau dieses System nicht zur Verfügung steht. Eventuell vorgehaltene analoge Dokumente müssen regelmäßig aktualisiert werden. Zu den benötigten Dokumenten gehören Handlungsanweisungen, Ablaufpläne und Checklisten ebenso wie Systemhandbücher, Lage- bzw. Raumpläne und Lizenzinformationen sowie die Kontaktinformationen aller beteiligten Mitarbeiter, Dienstleister, Lieferanten und ggf. Behörden.

Erst zum Abschluss befassen wir uns mit den IT-Systemen.

# IT Notfall-Planung – Notwendigkeit und Nutzen

## Schritt 7: Zuordnung von IT-Systemen zu den betrachteten Prozessen

Vorausgesetzt, es existiert eine aktuelle IT-Dokumentation (Inventarisierung) ordnen wir nun die Prozesse den zu Grunde liegenden IT-Systemen (Server, Netzwerke, Sicherheitssysteme, CloudServices etc.) zu. Andernfalls ist die IT-Dokumentation zwingend zu erstellen. Hierdurch erkennen wir Abhängigkeiten und können auch einzelne IT-Systeme damit in Bezug auf Wichtigkeit, maximal tolerierbare Ausfallzeit etc. bewerten. Somit erkennen wir Handlungsbedarf, wenn entsprechende Systeme die Anforderungen nicht erfüllen können.

### Fazit

Die prozessorientierte Vorgehensweise stellt sicher, dass keine Lücken in der Notfallplanung „übersehen“ werden. Gleichzeitig gibt sie den Entscheidungsträgern im Unternehmen die Möglichkeit, bestehende Risiken zu erkennen und Entscheidungen entsprechend der Dringlichkeit zu steuern. Sie ermöglicht die aus IT-technischer Sicht notwendige Betrachtung als Serviceverbund. (= Summe aller notwendigen Systeme, um dem Anwender einen bestimmten Service oder ein bestimmte „App“ wie z.B. Mail oder CRM zur Verfügung zu stellen.)

Die erarbeiteten Anforderungen und die serviceorientierte Betrachtung bieten eine belastbare Grundlage für Ausschreibungen sowohl für eigene Investitionen und Eigenbetrieb von Systemen und Anlagen als auch für das Outsourcing einzelner Services bis hin zur kompletten IT.

Darüber hinaus wird eine IT Notfallplanung in nahezu allen Fällen auch von Wirtschaftsprüfern und Versicherungen gefordert, beeinflusst unter Umständen das Kreditranking einer Organisation und ist für Inhaber, Geschäftsführung bzw. Vorstand auch aus haftungstechnischen Fragen weit mehr als ein notwendiges Übel.



**Andreas Gradl** ist Gründungsgesellschafter bei GCT und als Geschäftsführer für Finanzen, Rechtliches und Organisation verantwortlich.

**GCT** ist seit 1989 Ihr professioneller IT-Dienstleister im Rhein-Main-Gebiet mit Sitz in Bad Homburg v.d.H. Als klassisches IT-Systemhaus betreuen wir Ihre IT im eigenen Haus, als Outsourcer bringen wir Ihre IT in eine private Cloud im GCT Rechenzentrum in Frankfurt am Main oder in die public Cloud namhafter Anbieter und als Managed Service Anbieter liefern wir Ihnen Anwendungen und Security „as a Service“.