IT-Notfallplan

Version: <x.x>

Datum: <tt.mm.jjjj>

Version	Datum	Bearbeiter	Änderungen

Diese Word-Vorlage enthält das Gerüst für einen IT-Notfallplan, orientiert an den Bedürfnissen von kleinen und mittleren Unternehmen (KMU). Die Vorlage wurde Ihnen bereitgestellt von KonBriefing.com

Sie können die Vorlage für Ihre innerbetrieblichen Zwecke kostenfrei nutzen.

KonBriefing.com übernimmt keine Gewährleistung für die Vollständigkeit und Korrektheit dieser Vorlage und auch nicht dafür, ob die Vorlage für den beabsichtigten Zweck geeignet ist. Mit Ausnahme der gesetzlichen Haftung für Vorsatz ist jede Haftung von KonBriefing.com im Zusammenhang mit der Verwendung dieser Vorlage und ihrer Inhalte ausgeschlossen.

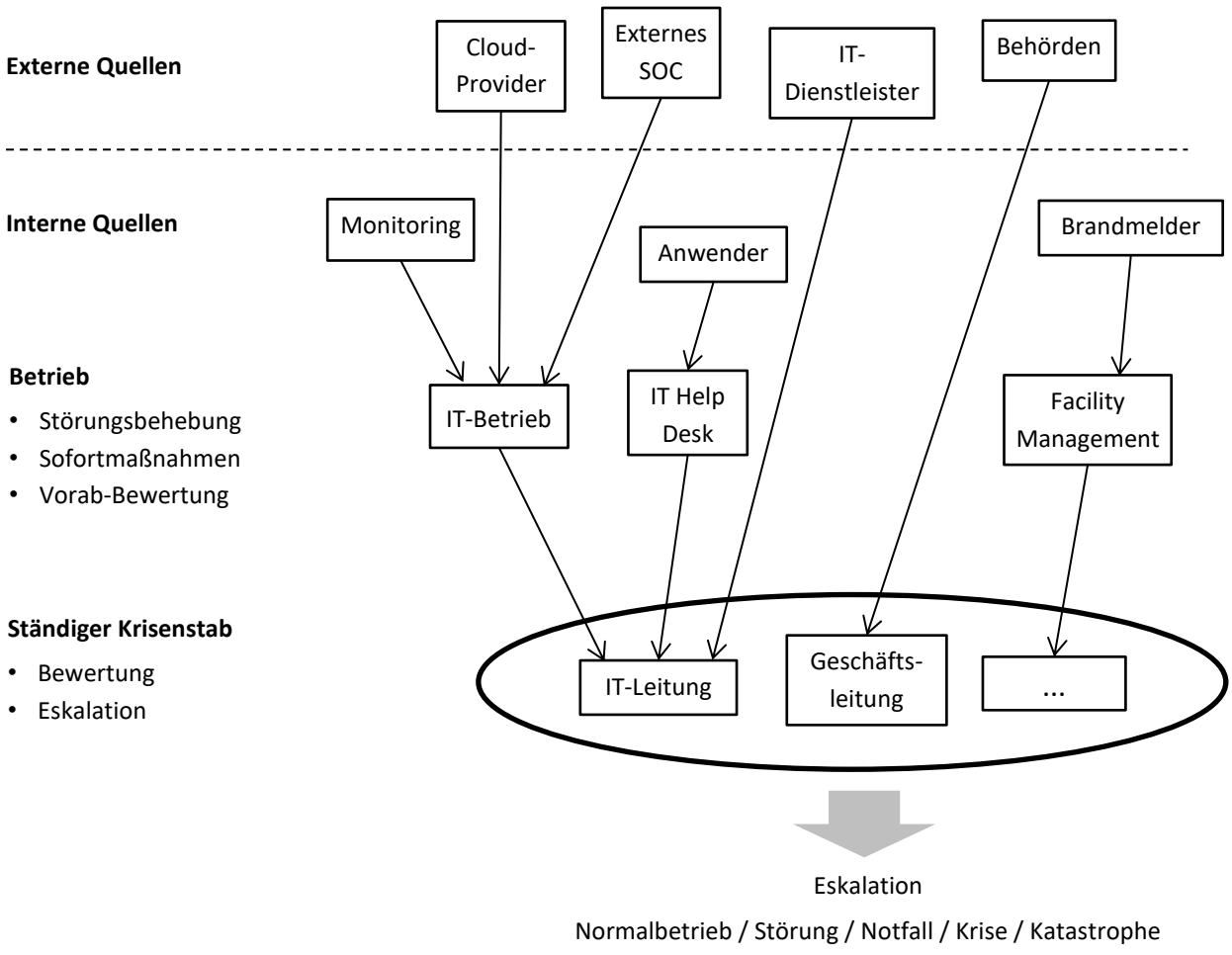
Hinweise, Verbesserungsvorschläge, Ergänzungen usw. sind jederzeit willkommen!

Inhalt

1 Störungen und IT-relevante Ereignisse

1.1 Aktivierung des Notfallplans

1.1.1 Meldewege für Störungen und Ereignisse



Hinweise zur Nutzung:

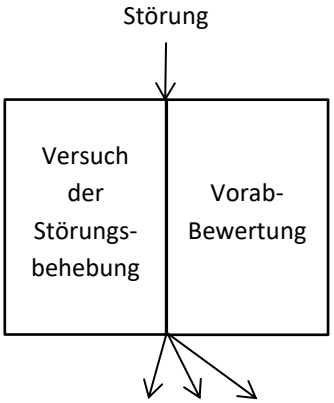
- Störungen und Ereignisse laufen in der Regel bei den Betriebsbereichen auf.
- Bei Störungen wird der Prozess zur Behebung der Störung bzw. zur Wiederherstellung der Arbeitsfähigkeit begonnen. Sobald sinnvoll möglich wird eine Vorab-Bewertung der Störung durchgeführt, um die notwendige Eskalationsstufe einzuschätzen.
- Bei Ereignissen werden zunächst die festgelegten Sofortmaßnahmen durchgeführt. Danach wird die Vorab-Bewertung vorgenommen.
- Diese Vorab-Bewertung wird an den ständigen Krisenstab gegeben.
- Der ständige Krisenstab bewertet die Gesamtsituation und entscheidet über die Eskalationsstufe.

- Die Bewertungen durch die Betriebsbereiche und durch den Krisenstab sind zu wiederholen, sobald neue relevante Informationen vorliegen.

1.1.2 Bewertungsschema für Störungen und Ereignisse

Störung

Beispiel: Ausfall einer Server-Komponente



Vorab-Bewertung/ Bewertung

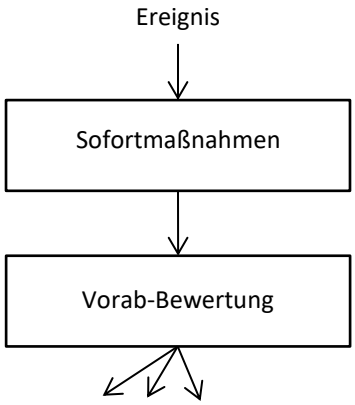
Welche Anwendungen und Geschäftsprozesse sind betroffen?

↓

Behebung oder Workaround innerhalb der akzeptablen Zeit möglich?

Ereignis

Beispiel: Feuer im Server-Raum, Ransomware



Behoben	Behebung in akzeptabler Zeit erwartet	Behebung dauert länger als die akzeptable Zeit oder Unklarheit, in welcher Zeit die Störung behoben werden kann		
Eskalationsstufe 0: Normalbetrieb	**Eskalationsstufe 1: Störung** Merkmale: • Geringe Beeinträchtigung der Geschäftstätigkeit • Störung kann sehr wahrscheinlich innerhalb der akzeptablen Zeit behoben werden.	**Eskalationsstufe 2: Notfall** Merkmale: • Beeinträchtigung der Geschäftstätigkeit • Ein primärer Prozess oder mehrere unterstützende Prozesse betroffen	**Eskalationsstufe 3: Krise** Merkmale: • Erhebliche Beeinträchtigung der Geschäftstätigkeit • Mehrere primäre Prozesse betroffen • Erheblicher finanzieller Schaden erwartet	**Eskalationsstufe 4: Katastrophe** Merkmale: • Unterbrechung wesentlicher Teile der Geschäfts-tätigkeit • Zahlreiche primäre Prozesse betroffen • Existenzgefährdend, hoher finanzieller Schaden erwartet • Behebung übersteigt weit die normalen Möglichkeiten

Hinweise zur Nutzung:

- Die Betriebsbereiche nutzen dieses Schema, um Störungen und Ereignisse vorab zu bewerten.
- Der ständige Krisenstab nutzt dieses Schema, um aus Sicht des gesamten Unternehmens die Eskalationsstufe zu ermitteln.
- Es soll die Eskalationsstufe gewählt werden, die der Situation im Hinblick auf die Auswirkungen am besten entspricht. Dabei müssen nicht alle genannten Merkmale zutreffen.
- Zur Definition der Prozesse siehe ...

Hinweise zur Erstellung:

- *Die Eskalationsstufen können abhängig vom Bedarf der Organisation frei definiert werden.*
- *Die Merkmale können auf die spezifische Situation hin angepasst werden.*
- *Primäre Prozesse meint die Prozesse der Haupt-Wertschöpfung, z.B. "Produktion" oder "Webshop". Unterstützende Prozesse sind z.B. "Personal" oder "Marketing" (sofern es keine Personalvermittlung oder Marketing-Agentur ist)*
- *Statt der Unterscheidung in primäre und unterstützende Prozesse kann auch eine andere Unterteilung genutzt werden oder es können spezifische Prozesse aufgeführt werden.*

1.1.3 Eskalation und Ausrufen von Notfall / Krise / Katastrophe

1.1.3.1 Reguläre Auslösung

Jedes Mitglied des ständigen Krisenstabs ist berechtigt, alleine einen Vorfall zu eskalieren, Notfall/Krise/Katastrophe auszurufen und die entsprechenden Maßnahmen einzuleiten.

1.1.3.2 Auslösung im Notstand

Bei Nichterreichbarkeit der Mitglieder des IT-Krisenstabs kann die Eskalation bzw. das Ausrufen von Notfall/Krise/Katastrophe auch von Mitgliedern der folgenden Gruppen durchgeführt werden:

- IT Help Desk bzw. allgemein von IT-Personal
- Facility Management
- ...

Das gilt insbesondere in Situationen wie:

- Umfangreiche Zerstörung von wichtiger IT-Infrastruktur, z.B. Feuer im Serverraum
- Ausfall kritischer IT-Komponenten, die eine hohe Auswirkung auf wichtige Geschäftsprozesse vermuten lassen, siehe Kapitel ...

1.1.3.3 Pflicht zur Durchführung der Sofortmaßnahmen

Die Mitglieder der Betriebsbereiche sind verpflichtet, bei Ereignissen die hier dokumentierten Sofortmaßnahmen ohne Rücksprache mit dem Krisenstab sofort einzuleiten.

1.2 Geschäftsprozesse

1.2.1 Wichtige Geschäftsprozesse

Listen Sie die Geschäftsprozesse in Ihrem Unternehmen auf. Die Priorität (bzw. Kritikalität) beschreibt die Wichtigkeit des Prozesses für den Geschäftsbetrieb und damit für den Erfolg bzw. die Existenz des Unternehmens. Die Priorität hilft bei der Definition der Einschätzung, für welche Prozesse ein Notbetrieb eingerichtet werden muss, in welcher Reihenfolge IT-Systeme wiederhergestellt werden müssen usw.

Prozess	Tätigkeiten	Maximal tolerierbare Ausfallzeit	Besondere Anforderungen an die Verfügbarkeit	Prio	Genutzte IT-Anwendungen
Primäre Prozesse					
Vertrieb	• Kundenbetreuung • Anfragen beantworten • Angebote erstellen und versenden • Aufträge empfangen • Aufträge erfassen	4 Stunden	Weihnachtsgeschäft im 4. Quartal	1	• Mail • Excel • ERP-System
Produktions-planung	• ...	8 Stunden		2	• ERP-System
Auftrags-abwicklung	•	8 Stunden		2	• ERP-System
Sekundäre Prozesse					
Buchhaltung	• ...	...	Steuervoraus-zahlungen	3	• Cloud-Service
Lohnbuch-haltung			Gehalt am 20. jeden Monats	2	

Beispiel

Anmerkungen:

...

(Erfassen Sie hier zusätzlich alle wichtigen Überlegungen, die Sie beim Ausfällen der Tabelle gemacht hatten und die beim späteren Verständnis der Tabelle nützlich sein können)

1.2.2 Kritische Services / Anwendungen

Beschreiben Sie die bei Ihnen genutzten Anwendungen und klassifizieren Sie sie danach, welche Relevanz sie für die wichtigen Geschäftsprozesse haben:

Anwendung	Maximal tolerierbare Ausfallzeit	Genutzte IT-Komponenten
Mail	4 Stunden	• Mail-Provider • Internet-Verbindung • lokaler Mail-Server • Arbeitsplatz-Rechner

Office		
ERP-System		
Auftragsabwicklung		
Buchhaltung		
Webpage		
Online-Shop		
Maschinensteuerung		

1.3 Notfall-Szenarien

1.3.1 Allgemeine Struktur

Leiten Sie aus der Kombination von

Die Szenarien sind nach der folgenden Struktur aufgebaut, die nach Bedarf erweitert oder gekürzt werden kann. Einzelne Punkte sind beispielhaft ausgefüllt, sie sollten jedoch nicht blind übernommen werden, sondern immer an die spezifischen Bedürfnisse des Unternehmens angepasst werden. Erarbeiten Sie die einzelnen Punkte in einer Zusammenarbeit zwischen Geschäftsführung, IT, Rechtsabteilung usw.

Beschreibung:

Beschreibung der Situation mit typischen Merkmalen.

Sofortmaßnahmen:

Was muss unmittelbar getan werden, ...

- um zu verhindern, dass der Schaden größer wird, z.B.
  - Rechner vom Netz abtrennen, um die Ausbreitung von Schadsoftware zu verhindern
- um Beweise zu sichern, z.B.
  - Bildschirmfotos machen
  - Bildschirm mit dem Smartphone abfotografieren
- um die Situation nachvollziehbar zu machen
  - Protokoll der Ereignisse mit Datum und Uhrzeit führen

Benachrichtigung:

Wer sollte über den Vorfall benachrichtigt werden, um weitere Maßnahmen zu ergreifen und Entscheidungen treffen zu können? Beispiele:

- Geschäftsleitung
- IT-Verantwortliche
- Leiter von betroffenen Abteilungen, die voraussichtlich nicht mehr arbeiten können.

Analyse und Bewertung:

Welche weiteren Maßnahmen kommen als Fortsetzung der Sofortmaßnahmen in Frage, um die Situation zu analysieren und das Ausmaß zu bewerten? Zum Beispiel ...

- Sicherung von Logdateien und anderer Hinweise und Beweise
- Hinzuziehen weiterer Spezialisten
- Beratung mit der Rechtsabteilung / mit dem Rechtsanwalt
- Anzeige bei der Polizei
- Abschätzung des Schadens

Kommunikation intern:

Bei einem Ausfall der IT sind in der Regel viele Mitarbeiter betroffen, daher ist eine entsprechende Kommunikation wichtig.

- Was ist passiert?
- Was wird aktuell unternommen?

- Was tun die vom Ausfall betroffenen Mitarbeiter? (Notbetrieb, Arbeitsplätze säubern, Akten sortieren, Urlaubsabbau usw.)
- Wie und wann erfolgt die weitere Kommunikation
- Bei Anfragen der Presse immer an den Pressesprecher verweisen. Schon im eigenen Interesse der Mitarbeiter, damit das Unternehmen durch eine konsistente Kommunikation einen Reputationsschaden vermeidet.

Da bei bestimmten Szenarien nicht auszuschließen ist, dass es einen Innentäter gibt, sollten bei der Mitarbeiter-Kommunikation nicht zu viele Details preisgegeben werden.

Kommunikation extern:

siehe oben

Wiederanlauf und Notbetrieb:

Wie kann ein Notbetrieb hergestellt werden, um den Geschäftsbetrieb trotz des Notfalls fortzuführen? In der Regel wird ein Notbetrieb eine geringere Leistungsfähigkeit haben, jedoch kann er im Idealfall die gravierendsten Auswirkungen abfangen, weil z.B. die wichtigsten Kundenaufträge weiterhin abgewickelt werden können.

- Welche alternativen Dienste können genutzt werden, z.B. Cloud-Dienste für Mail
- Kann kurzfristig ein Notstandort aufgebaut werden, z.B. durch Anmietung von Büros
- Welche Unternehmen können temporär bestimmte Fertigungsschritte übernehmen, wenn Teile der eigenen Produktion ausgefallen sind?

Wiederherstellung:

Welche weiteren Maßnahmen müssen ergriffen werden, um die betroffenen Systeme wieder in den Normalbetrieb zu bringen?

- Reihenfolge der Wiederherstellung entsprechend der Kritikalität der betroffenen Anwendungen
- Beschaffung von Ersatz-Servern bzw. Buchung zusätzlicher Cloud-Dienste
- Installation von Servern

Meldepflichten:

Abhängig von der Branche, in der Ihr Unternehmen tätig ist (z.B. Betrieb von kritischer Infrastruktur KRITIS) und von der Art des Vorfalls (z.B. Offenbarung von personenbezogenen Daten) können Meldepflichten mit Fristen bestehen. Lassen Sie sich von Ihrem Rechtsanwalt beraten!

1.3.2 Großflächiger Ausfall der IT

Beschreibung:

Weite Teile der Unternehmens-IT können nicht genutzt werden, entweder aus unbekanntem Grund oder weil die IT bewusst abgeschaltet wurde, um beispielsweise die Ausbreitung von Schadsoftware zu einzudämmen.

Sofortmaßnahmen:

Benachrichtigung:

Analyse und Bewertung:

Wiederanlauf und Notbetrieb:

Wiederherstellung:

Kommunikation intern:

Kommunikation extern:

Wiederherstellung:

Meldepflichten:

1.3.3 Physische Beschädigung zentraler IT-Komponenten

Beschreibung:

Verlust wichtiger IT-Dienste durch Brand im Rechenzentrum, Wasser im Serverraum usw.

Sofortmaßnahmen:

Benachrichtigung:

Analyse und Bewertung:

Wiederanlauf und Notbetrieb:

Wiederherstellung:

Kommunikation intern:

Kommunikation extern:

Wiederherstellung:

Meldepflichten:

1.3.4 Internet-Verbindung längere Zeit ausgefallen

Beschreibung:

Die Internet-Verbindung steht voraussichtlich eine längere Zeit nicht zur Verfügung.

- Wichtige Mails können nicht verschickt oder empfangen werden, z.B. um Kundenaufträge abzuwickeln. Es besteht die Gefahr, dass Aufträge verloren gehen oder nicht vertragsgerecht abgewickelt werden können.
- Wichtiger Datenverkehr kann nicht stattfinden, z.B. Buchungsdaten oder Steuermeldungen. Es besteht die Gefahr, dass Fristen versäumt werden
- Vom Unternehmen genutzte Cloud-Anwendungen können nicht genutzt werden.

Sofortmaßnahmen:

Benachrichtigung:

Analyse und Bewertung:

Wiederanlauf und Notbetrieb:

Wiederherstellung:

Kommunikation intern:

Kommunikation extern:

Meldepflichten:

1.3.5 Denial-of-Service-Attacke

Beschreibung:

Sofortmaßnahmen:

Benachrichtigung:

Analyse und Bewertung:

Wiederanlauf und Notbetrieb:

Wiederherstellung:

Kommunikation intern:

Kommunikation extern:

Meldepflichten:

1.3.6 Mail-Service ausgefallen

Beschreibung:

Sofortmaßnahmen:

Benachrichtigung:

Analyse und Bewertung:

Wiederanlauf und Notbetrieb:

Wiederherstellung:

Kommunikation intern:

Kommunikation extern:

Meldepflichten:

1.3.7 Mögliche Infektion mit Schadsoftware

Beschreibung:

Es wurde eine Handlung vorgenommen, die zu einer Infektion mit Schadsoftware geführt haben könnte. Es ist aber unklar, ob tatsächlich eine Infektion stattgefunden hat. Beispiele:

- In einer verdächtigen Mail wurde ein Link angeklickt.
- Es wurde ein Anhang aus einer verdächtigen Mail geöffnet

Das ist an sich noch kein Notfall, die Situation kann jedoch sofortiges Handeln erfordern.

Sofortmaßnahmen:

Benachrichtigung:

Analyse und Bewertung:

Wiederanlauf und Notbetrieb:

Wiederherstellung:

Kommunikation intern:

Kommunikation extern:

Meldepflichten:

1.3.8 Infektion mit Schadsoftware

Beschreibung:

Ein Befall mit Schadsoftware ist aufgetreten oder ist wahrscheinlich. Symptome:

- Virenscanner hat Schadsoftware gemeldet
- Auf dem Bildschirm erscheint eine Erpressungsforderung
- Dateien wurden verändert und sind nicht mehr lesbar
- Ungewöhnlich hohe Nutzung von Systemressourcen (CPU-Leistung, Speichernutzung usw.)

Sofortmaßnahmen:

Benachrichtigung:

Analyse und Bewertung:

Wiederanlauf und Notbetrieb:

Wiederherstellung:

Kommunikation intern:

Kommunikation extern:

Meldepflichten:

1.3.9 Unbefugter Zugriff auf Systeme

Beschreibung:

Es wurde festgestellt, dass Unbekannte großflächigen Zugriff auf Systeme haben.

Symptome:

- Es sind unbekannte Benutzer auf dem System eingerichtet oder aktiv
- Zugriffsrechte wurden verändert
- Ungewöhnliche Einträge in Logdateien

Sofortmaßnahmen:

Benachrichtigung:

Analyse und Bewertung:

Wiederanlauf und Notbetrieb:

Wiederherstellung:

Kommunikation intern:

Kommunikation extern:

Meldepflichten:

1.3.10 Die Website des Unternehmens wurde gehackt

Beschreibung:

Die Website des Unternehmens wurde gehackt und verändert oder wird zur Auslieferung von Schadsoftware genutzt. Sofern es nur die reine Webpräsenz betrifft (und nicht z.B. einen Onlineshop), hat es oft keine unmittelbare Auswirkung auf den Geschäftsbetrieb, durch die hohe Sichtbarkeit kann es jedoch die Reputation des Unternehmens beeinträchtigen.

Sofortmaßnahmen:

Benachrichtigung:

Analyse und Bewertung:

Wiederanlauf und Notbetrieb:

Wiederherstellung:

Kommunikation intern:

Kommunikation extern:

Meldepflichten:

2 Arbeit des Krisenstabs

2.1 Krisenstab für IT-Notfälle

2.1.1 Ständiger Krisenstab

Der ständige Krisenstab bewertet alle für die IT relevanten Störungen und Ereignisse und entscheidet über deren Eskalation zu Notfall/Krise/Katastrophe.

Der ständige Krisenstab besteht aus den folgenden Mitgliedern bzw. Rollen:

... (Geschäftsleitung)

... (IT-Leitung)

...

2.1.2 Erweiterter Krisenstab

Der erweiterte Krisenstab tritt nach einer Eskalation zu Notfall/Krise/Katastrophe zusammen, um die Situation über das gesamte Unternehmen zu steuern.

Der erweiterte Krisenstab besteht aus den folgenden Mitgliedern bzw. Rollen:

...

... (Recht)

... (Personal)

... (Öffentlichkeitsarbeit)

Anmerkung: Aufgrund der zentralen Rolle der IT haben IT-Notfälle in der Regel erhebliche Auswirkungen auf den gesamten Geschäftsbetrieb. In kurzer Zeit sind zahlreiche und z.T. gravierende Entscheidungen zu treffen und es ist eine abgestimmte Kommunikation zu verschiedensten Interessensgruppen zu führen. Deshalb ist der Krisenstab keine "IT-Angelegenheit", sondern ist so zu besetzen, dass er im Hinblick auf die gesamte Geschäftstätigkeit maximal entscheidungs- und handlungsfähig ist.

2.1.3 Arbeitsmodi

Abhängig von der Situation sind für den ständigen und für den erweiterten Krisenstab die folgenden Arbeitsweisen denkbar:

- Information / bei Bedarf: Die Mitglieder werden über eine Situation regelmäßig informiert, kommen aber nur bei besonderem Bedarf zusammen. Anwendbar zum Beispiel in Situationen mit niedriger Eskalationsstufe.
- Teilzeit: Die Mitglieder kommen regelmäßig zusammen, um eine Situation zu besprechen. Sie nehmen jedoch auch ihre andere Tätigkeiten wahr.
- Vollzeit: Die Mitglieder arbeiten ausschließlich an der Bewältigung der Situation. Das ist notwendig bei hohen Eskalationsstufen (Katastrophe), die komplex sind und eine hohe Arbeitslast generieren.

Vor allem bei Katastrophen kann es notwendig sein, viele Stunden pro Tag und auch am Wochenende zu arbeiten. Deshalb sollte in solchen Fällen auch an Vertretungsmöglichkeiten gedacht werden.

2.2 Alarmierung

2.2.1 Grundsätze

Sofern vorhanden sollten immer mehrere Kanäle parallel genutzt werden, z.B. Mail und Telefon oder Mail und Messenger-Dienste.

Der Ausfall der IT kann mit dem Ausfall der Telefonanlage verbunden sein, insbesondere wenn beide Systeme auf demselben Netz betrieben werden. Je nach Situation:

- Information der Führungskräfte über Mobiltelefon
- Einsatz von Meldern, die von Abteilung zu Abteilung laufen und Führungskräfte und Mitarbeiter über den Sachverhalt informieren.
    - Der Melder hat das Recht, interne Besprechungen zu unterbrechen
    - Bei Besprechungen mit externer Beteiligung bittet er die Führungskräfte hinaus, um ihnen den Sachverhalt zu erläutern.

2.2.2 Alarmierung des ständigen Krisenstabs

Die Mitglieder des ständigen Krisenstabs alarmieren sich nach folgendem Schema:

Während normaler Arbeitszeiten:

...

Während Feierabend / Urlaub / Feiertag:

...

2.2.3 Alarmierung des erweiterten Krisenstabs

Die Mitglieder des erweiterten Krisenstabs alarmieren sich nach folgendem Schema:

Während normaler Arbeitszeiten:

...

Während Feierabend / Urlaub / Feiertag:

...

2.2.4 Alarmierung der Führungskräfte des Unternehmens

2.2.4.1 Während der normalen Arbeitszeiten

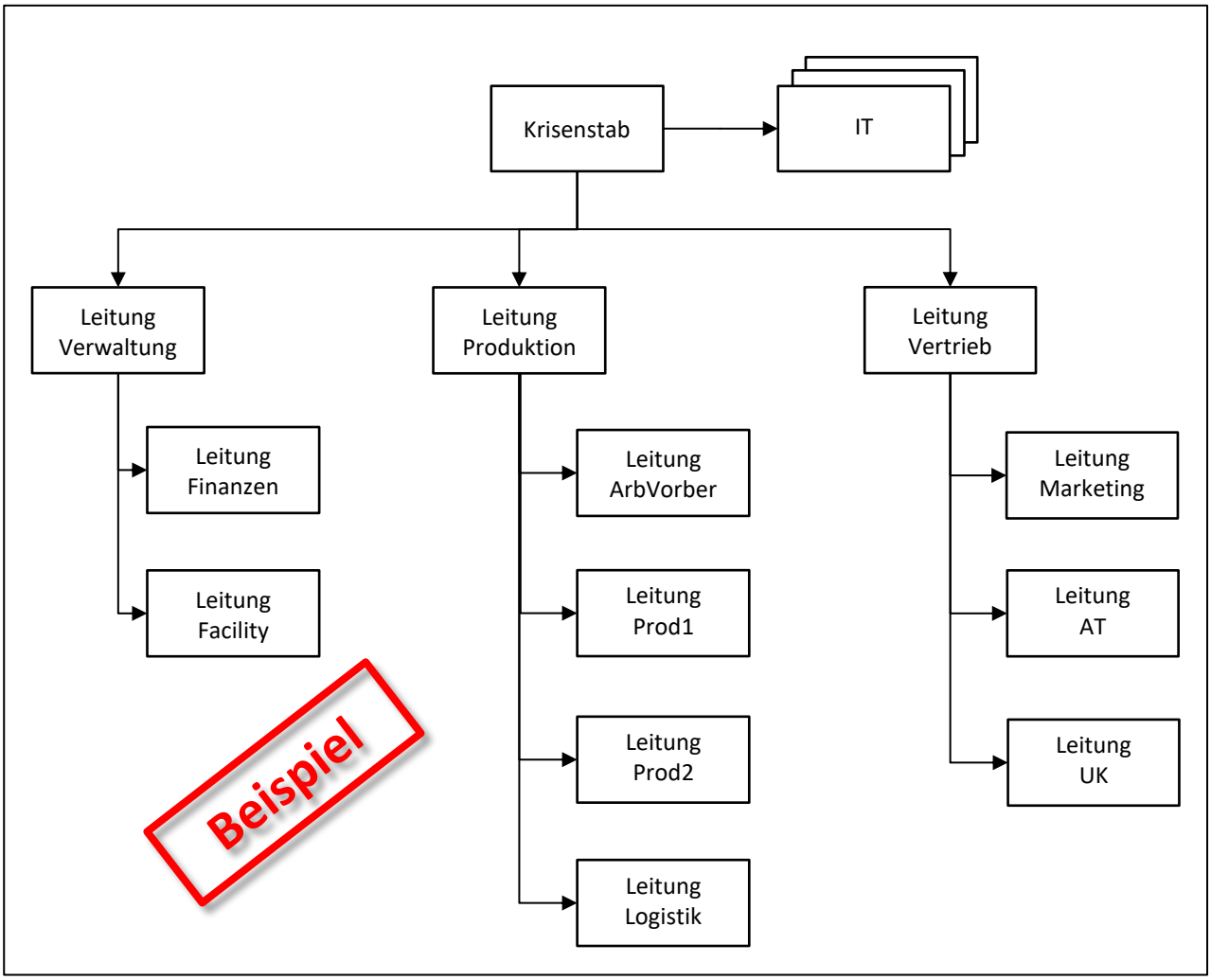
- Mail
- Telefon / Mobiltelefon, ggf. unter Anwendung des Meldebaums
- Bei Ausfall von Mail und Telefon: Melder, die von Abteilung zu Abteilung laufen.

2.2.4.2 Während Feierabend / Urlaub / Feiertag

Bei hohen Eskalationsstufen kann es notwendig sein, die Führungskräfte des Unternehmen (einer Niederlassung usw.) zu alarmieren. Bei Benachrichtigungen per Mail nach Feierabend bzw. im Urlaub besteht das Risiko, dass sie zunächst nicht gelesen werden. Da aber gerade bei hohen Eskalationsstufen ein schnelles Handeln erforderlich ist, sollte dann eine telefonische Benachrichtigung versucht werden.

2.2.4.3 Meldebaum

Um die Arbeitslast der Alarmierung aufzuteilen, wird der folgende Melde-Baum verwendet. Der Plan sollte bei den ausführenden Personen ausgedruckt sowohl am Arbeitsplatz als auch zu Hause vorliegen.



Standardisierte Meldung

Um die Information unverfälscht über den gesamten Meldebaum zu bringen, sollte sie standardisiert übermittelt werden. Personen, die Zwischenstation sind, sollten die Information bei telefonischem Empfang aufschreiben, um sicherzustellen, dass sie alle Inhalte an alle weiteren Personen weitergegeben werden.

Beispiel:

Stichwort: IT-Notfall

Schweregrad:	mittel / schwer
betroffene Bereiche:	z.B. Bürokommunikation, Produktion
Verbote:	z.B. Keine IT-Geräte einschalten oder mit dem Netz verbinden wegen Malware-Gefahr
Handlungen:	z.B. Zur Niederlassung kommen, mit dem Vorgesetzten in Kontakt treten, ...
Weitergabe:	Weitergabe dieser Information entsprechend Benachrichtigungsplan

2.2.5 Alarmierung der Mitarbeiter

2.2.5.1 Während der normalen Arbeitszeiten

- Mail
- Telefon / Mobiltelefon, ggf. unter Anwendung des Meldebaums
- Bei Ausfall von Mail und Telefon: Melder, die von Abteilung zu Abteilung laufen.

2.2.5.2 Während Feierabend / Urlaub / Feiertag

Verschlüsselungs-Trojaner werden häufig nach Feierabend oder zum Wochenende gestartet. Daher sollten sofort alle verfügbaren Kanäle genutzt werden, einschließlich privater Telefonnummern und E-Mails, um Mitarbeiter auch daheim davon abzuhalten, ihre IT-Geräte wieder mit dem Firmennetz zu verbinden.

2.3 Kommunikation

2.3.1 Interne Kommunikation zu Mitarbeitern

2.3.1.1 Mitarbeiter über die Situation informieren

Vorschlag zum Inhalt:

Status
Was ist vorgefallen? (Grober Sachverhalt, ohne in alle Details zu gehen)
Status (bei der Analyse, bei der Wiederherstellung usw.)
Haben externe Dienstleister zur Unterstützung geholt (optional)
Haben den Vorfall den Behörden gemeldet (optional)
Verhalten
Die Vorgesetzten werden die weitere Vorgehensweise mit den Mitarbeitern besprechen.
Gegenüber Kunden: Aktuell haben wir eine technische Störung.
Bitte: Den Vorfall nicht auf sozialen Medien zu veröffentlichen. Warum? Die in sozialen Medien sich schnell entwickelnden Unsachlichkeiten und Übertreibungen können dem Unternehmen weiteren Schaden zufügen - was nicht im Interesse der Mitarbeiter sein dürfte.
Bitte: Bei Anfragen von Pressevertretern keine Auskünfte geben, sondern auf den Pressesprecher des Unternehmens verweisen. Warum? Es ist kurzfristig sicher ein tolles Gefühl, in der Presse zu sein. Jedoch sollte man nicht davon ausgehen, korrekt zitiert zu werden. Stattdessen könnte man schnell zum Mittelpunkt einer verzerrten Darstellung und von Spekulationen werden, was sowohl dem Unternehmen als auch der Person selbst schaden kann.
Abschluss
Hoffen auf die Mitarbeit aller.
Werden informieren, sobald es Neuigkeiten gibt
Werden gemeinsam die schwierige Situation bewältigen.

2.3.2 Kommunikation mit Kunden

- Mail über Probleme und mögliche Verzögerungen
- Informationsbanner auf der Website oder im Online-Shop

2.3.3 Öffentlichkeitsarbeit

2.3.3.1 Übersicht

Notfälle haben eine erhebliche Auswirkung auf das Geschäft und sind damit in unterschiedlichen Graden auch außerhalb des Unternehmens wahrnehmbar, entweder nur für Geschäftspartner und Kunden oder sogar für die Allgemeinheit.

Entsprechend sollte informiert werden, damit auf der Gegenseite keine Unsicherheit entsteht, sondern das Vertrauen auch in der Krisensituation erhalten bleibt.

Zu Beeinträchtigungen kann es ebenfalls bei der Einhaltung gesetzlichen Pflichten kommen, wie z.B. der Steueranmeldung, beim Jahresabschluss oder der Bereitstellung von statistischen Daten. Auch mit diesen Institutionen muss Kontakt hergestellt werden.

Und es besteht immer die Möglichkeit, dass Informationen über größere oder spektakuläre Ausfälle an die Presse gelangen. Daher sollte im Vorfeld überlegt werden, ab wann und wie eine aktive Kommunikation nach außen betrieben wird, damit das Unternehmen dabei eine aktive Rolle behält und nicht von der Presse vor sich hergetrieben wird. Alle Informationen an die Presse sollten nur über einen dedizierten Pressesprecher laufen, um eine konsistente Kommunikation zu gewährleisten.

2.3.3.2 Pressesprecher

Es sollte eine Person zum Pressesprecher ernannt werden, der die gesamte Kommunikation mit der Presse und anderen externen Interessensvertretern betreibt. Der Pressesprecher sollte sich regelmäßig mit den internen Fachexperten beraten und hat die aktuelle Berichterstattung sowie deren Tenor zu verfolgen.

Instrumente:

- Pressemitteilungen
- Gespräche mit Pressevertretern
- ...

2.3.3.3 Textbausteine für Pressemitteilungen

Ransomware-Angriff

Einleitung:

Am <Datum> wurde die <Unternehmen> von einem schweren Cyber-Angriff getroffen.

Das führt zu <ernsthaften> Einschränkungen <in der Produktion, in der Auftragsabwicklung, ...>

an <den Standorten ..., an allen Standorten>

Geschehen:

Durch Ransomware wurden die Inhalte <mehrerer Server> verschlüsselt,

davon betroffen <ist die Bürokommunikation, ist die Produktion, sind größere Teile der IT-Infrastruktur>.

Maßnahmen:

Die <Unternehmen> arbeitet intensiv daran, die Auswirkungen auf Kunden und Mitarbeiter zu minimieren und die IT-Systeme wiederherzustellen.

Die zuständigen Behörden wurden über den Vorfall informiert.

Weitere Informationen:

Sobald weitere Informationen vorliegen, wird die <Unternehmen> darüber informieren.

Für weitere Fragen wenden Sie sich bitte an <Kontaktdaten Pressesprecher>.

2.3.4 Offizielle Kommunikation, z.B. mit Behörden

Insbesondere wenn es um wichtige Fristen geht, sollte die Kommunikation immer nachweisbar sein. Beispiel: Telefonate vor Zeugen führen, nachträglich Mails schreiben usw.

Wenn KRITIS-Betreiber:

- Meldung von Sicherheitsvorfällen

Bei Datenschutzverstößen:

- Meldung an die Datenschutzbehörde

Wenn öffentlich gehandelte Aktiengesellschaft:

- Je nach Umfang des Notfalls Herausgabe einer Adhoc-Meldung
- Bei großem Umfang ggf. Aussetzung des Handels

3 Verzeichnisse

3.1 Kontaktdaten

Tragen Sie hier die Kontaktdaten von allen Personen, Dienstleistern und Behörden zusammen, die bei der Bewältigung eines IT-Notfalls einbezogen werden müssen oder hilfreich sein könnten. Sollten Sie diese Adressen bereits in einem übergreifenden Unternehmens-Notfallhandbuch gesammelt haben, können Sie in diesem Kapitel auch einfach nur darauf verweisen.

3.1.1 Intern

3.1.1.1 Geschäftsführung, Betriebsleitung

Name

Telefon

Mail

Privat

3.1.1.2 IT-Verantwortliche

Name

Telefon

Mail

Privat

3.1.1.3 Facility Management, Hausmeister, Elektriker

Je nach Situation kann es notwendig sein, in unerwartet verschlossene Räume zu gelangen, eine Wasserleitung abzustellen oder provisorisch ein Kabel zu verlegen. Halten Sie hier alle Personen fest, die dabei vermutlich unterstützen können. Ggf. unterschieden nach verschiedenen Standorten

Facility Management

Name

Telefon

Mail

Privat

Hausmeister

Name

Telefon

Mail

Privat

Elektriker

Name

Telefon

Mail

Privat

3.1.2 Dienstleister

Ggf. unterschieden nach verschiedenen Standorten

3.1.2.1 IT- und andere Dienstleister

Tragen Sie hier die IT-Dienstleister ein, mit denen Sie zusammenarbeiten. Denken Sie daran, dass Sie eventuell ganz verschiedene IT-Systeme nutzen, die unterschiedliche Ansprechpartner haben. Beispiel: Die Steuerung einer Produktionsanlage hat einen anderen Dienstleister als ihre Büro-IT. Halten Sie deshalb unter „Themen" das Aufgabengebiet des Dienstleisters fest. Denken Sie auch daran, Alternativen zu planen, insbesondere wenn ihr IT-Dienstleister eine One-Man-Show ist, der auch mal im Urlaub sein kann, wenn Sie Unterstützung brauchen.

Themen sind z.B.:

- Netzwerk, Server, Büro-IT
- Klimaanlage Server-Raum
- Produktionssteuerung

Themen

Name

Telefon

Mail

Themen

Name

Telefon

Mail

3.1.2.2 Cloud-Provider

Kontaktdaten für die vom Unternehmen genutzten Cloud-Angebote (Plattformen, Software)

Name

Notruf

Telefon

Mail

Web

Name

Notruf

Telefon

Mail

Web

3.1.2.3 Telekommunikationsunternehmen

Name

Notruf

Telefon

Mail

Web

3.1.2.4 Rechtsanwalt des Unternehmens

Name

Telefon

Mail

3.1.2.5 Versorgungsunternehmen

Bestimmte IT-Notfälle können durch Probleme an Versorgungseinrichtungen ausgelöst worden sein (z.B. Wasserrohrbruch) oder lassen sich nur mit Schaltungen an Versorgungseinrichtungen beheben.

Strom

Name

Notruf

Telefon

Mail

Website

Wasser

Name

Notruf

Telefon

Mail

Abwasser

Name

Notruf

Telefon

Mail

Gas

Name

Notruf

Telefon

Mail

Website

Sonstige (z.B. technische Gase)

Name

Notruf

Telefon

Mail

Website

3.1.3 Behörden

Ggf. unterschieden nach verschiedenen Standorten

3.1.3.1 Polizei

Örtliche Polizei

...

Zentrale Ansprechstellen Cybercrime der Polizeien der Länder und des Bundes für die Wirtschaft

siehe https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Meldestelle/Polizeikontakt/ZACkontakt/zackontakt.html

3.1.3.2 Datenschutzbehörde

IT-Notfälle können mit Datenschutz-Vorfällen verbunden sein, die ggf. meldepflichtig sind.

Name

Telefon

Mail

Website

3.1.3.3 Umweltschutzbehörde

Name

Telefon

Mail

Website

3.1.3.4 Rathaus, Ordnungsamt

Name

Telefon

Mail

Website

3.1.4 Medien

Ggf. unterschieden nach verschiedenen Standorten

Örtliche Zeitung

Regionalfernsehen

3.2 IT-Umgebung

Dokumentieren Sie Ihre IT-Umgebung. Dies sollte so erfolgen, dass nicht nur Ihre eigene IT bzw. Ihre IT-Dienstleister damit arbeiten können. Vielmehr sollte es auch einem sachverständigen Dritten möglich sein, die Infrastruktur zu verstehen, da Sie bei einem umfassenden Notfall wahrscheinlich auch andere Dienstleister hinzuziehen werden.

3.2.1 Standorte / Niederlassungen

Beschreiben Sie jeden Ihrer Firmen-Standorte

3.2.1.1 Standort 1: ...

Anschrift:

Funktionen:	... (z.B. Verwaltung, Produktion)
Wichtige IT-Komponenten:	... (z.B. Rechenzentrum, Dateiserver)
Gebäudeplan:	→ Anhang
Plan Verkabelung:	→ Anhang
Plan Serverraum:	→ Anhang

3.2.1.2 Standort 2: ...

3.2.2 IT-Infrastruktur

3.2.2.1 Rechenzentrum / Server

Server

3.2.2.2 Cloud-Dienste

3.2.2.3 Netzwerk

Beschreiben Sie die wichtigen Aspekte Ihres Netzwerks. Fügen Sie einen Netzwerkplan im Anhang an.

3.2.2.4 Internet-Anbindung

Provider: ...

Verträge: → Anhang

3.2.3 Anwendungen und Services

3.3 Weitere Verzeichnisse

(als separate Dateien)

Für jeden Standort:

- Gebäudepläne der Standorte
- Verkabelungspläne
- Plan Serverraum