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.

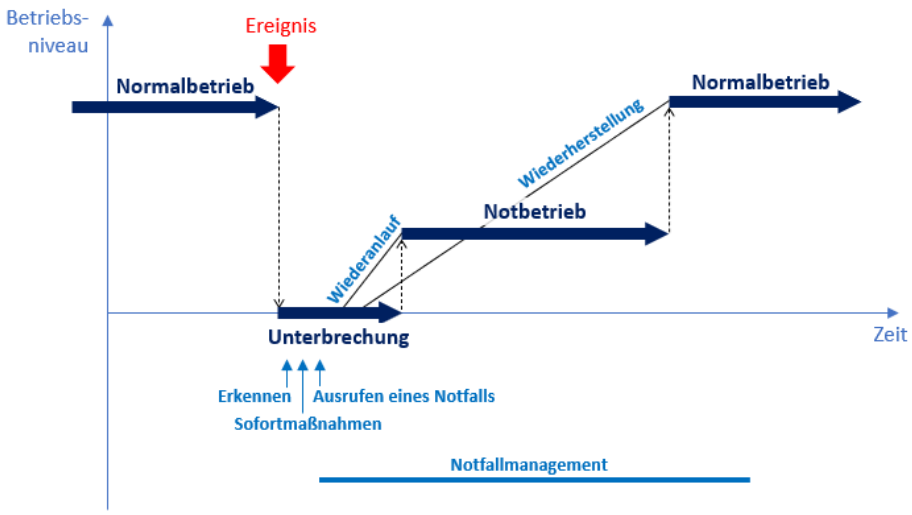
KonBriefing.com übernimmt keine Gewährleistung für die Vollständigkeit und Korrektheit dieser Vorlage und auch nicht dafür, ob die Vorlage für den beabsichtigten Zweck geeignet ist. Mit Ausnahme der gesetzlichen Haftung für Vorsatz ist jede Haftung von KonBriefing.com im Zusammenhang mit der Verwendung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

Hinweise, Verbesserungsvorschläge, Ergänzungen usw. sind jederzeit willkommen!

Inhalt

1 Einordnung des IT-Notfallplans

Der IT-Notfallplan ist ein Werkzeug zur Reaktion auf außergewöhnliche Ereignissen in der IT, die zum Ausfall von kritischen Geschäftsprozessen führen. Ein Notfall ist dann gegeben, wenn eine Störung nicht mehr im Rahmen des Normalbetriebs bewältigt werden kann.



In Anlehnung an den BSI-Standard 100-4

Der Notfallplan enthält die oben hellblau dargestellten Abschnitte:

- Erkennen und Melden von potenziellen Notfällen
- Sofortmaßnahmen
- Ausrufen des Notfalls durch eine diensthabende Person
- Notfallmanagement durch den Notfall-Stab
- Wiederanlauf zum Notbetrieb
- Wiederherstellung zum Normalbetrieb

Darüber hinaus enthält er eine Sammlung von Informationen, die in einem Notfall besonders hilfreich sind, wie z.B. Kontaktlisten, IT-Dokumentation u.a.

Vor allem das Erkennen und Melden von potenziellen Notfällen sowie die Sofortmaßnahmen müssen bei den entsprechenden Organisationseinheiten auch außerhalb des Notfallplans vorliegen und bekannt sein.

2 Erkennen und Melden potenzieller Notfälle

Informationen über potenzielle Notfälle können aus internen und externen Quellen kommen.

Beispiele für interne Quellen:

- Help Desk / Incident Management: großflächiger Ausfall, unklare Störungen
- Internes Monitoring / Security Operations Center (SOC): verdächtige Aktivitäten
- Anwender von kritischen Anwendungen
- Facility Management: Ausfall der Versorgung, Brände, Wasserschäden

Beispiele für externe Quellen:

- Meldungen von SaaS-/PaaS-/IaaS-Anbeitern
- Externes Security Operations Center
- Dienstleister
- Informationen von Behörden

2.1 Kriterien eines potenziellen IT-Notfalls

2.1.1 Für den IT-Betrieb

Eines der folgenden Kriterien ist erfüllt:

- ...

2.1.2 Für den IT Help Desk

Eines der folgenden Kriterien ist erfüllt:

- ...

2.1.3 Für Anwender kritischer IT-Services

Für kritische Anwendungen, die nicht von der IT betreut werden (z.B. SaaS) oder außerhalb der normalen IT-Sprechzeiten.

Eines der folgenden Kriterien ist erfüllt:

- Ausfall einer Anwendung, die unmittelbar für einen zeitkritischen Prozess benötigt wird
- Hinweise auf Schadsoftware, z.B. Erpressungsforderungen auf dem Bildschirm
- ...

2.1.4 Für das Facility Management

Eines der folgenden Kriterien ist erfüllt:

- Einwirkung oder die Gefahr der Einwirkung von Feuer, Wasser, Zerstörung etc. auf IT-Infrastruktur - (Rechenzentrum oder größere Zahl von Arbeitsplätzen)

2.1.5 Für den Empfang / für die Telefonzentrale

Eines der folgenden Kriterien ist erfüllt:

- Meldung von Dritten, Behörden usw., die auf eine schwere Störung der IT hindeuten können

2.2 Automatisierte Systeme

Die folgenden Systeme generieren Alarme, die einen IT-Notfall bedeuten können:

...

2.3 Melden potenzieller IT-Notfälle

2.3.1 Zu normalen Arbeitszeiten:

Mo - Fr von … bis ... Uhr

An den IT Help Desk

...

Weiterleitung vom Help Desk an die jeweils diensthabende Person für IT-Notfälle

...

2.3.2 Außerhalb der normalen Arbeitszeiten

Nachts, Wochenende, Feiertage direkt an die diensthabende Person für IT-Notfälle

...

2.4 Diensthabende Person für IT-Notfälle

Es ist die ständige Erreichbarkeit einer diensthabenden Person zu organisieren, die Meldungen über potenzielle IT-Notfälle entgegennimmt, bewertet und ggf. den IT-Notfall erklärt sowie weitere Maßnahmen initiiert.

3 IT-Sofortmaßnahmen

3.1 Allgemein

Je nach Situation zuerst immer die normalen Rettungsmaßnahmen ergreifen, z.B. Menschen aus der Gefahrenzone bringen, Löschversuch unternehmen, Rettungsdienste alarmieren.

IT-Sofortmaßnahmen:

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

Die Mitglieder der IT-Betriebsbereiche sind verpflichtet, bei Ereignissen die hier dokumentierten Sofortmaßnahmen ohne Rücksprache sofort einzuleiten.

3.2 Bei Schadsoftware

Maßnahmen

- Betroffene Systeme sofort isolieren
- ...
- Sofortige Anweisung an alle Mitarbeitenden

Berechtigt zur Durchführung:

- ...

3.3 Bei Feuer, Wasser

...

3.4 Umschwenken kritischer Anwendungen auf Ersatz-Infrastruktur

- Ersatz-Rechenzentrum
- Ersatz-Server
- Ersatz-Cloud

Berechtigt zur Durchführung:

- ...

4 Ausrufen eines IT-Notfalls

4.1.1 Reihenfolge

Zunächst sind je nach Situation die Sofortmaßnahmen zu ergreifen bzw. einzuleiten.

4.1.2 Kriterien für einen IT-Notfall

Ein IT-Notfall wird erklärt, wenn:

- Mindestens ein kritischer Geschäftsprozess ist unterbrochen oder erheblich eingeschränkt.
  Oder es ist zu vermuten, dass er unterbrochen oder erheblich eingeschränkt sein wird.
- Und
  - Die Wiederherstellung wird ungefähr gleich oder länger brauchen als die maximal zulässige Zeit.
    Oder die Zeit für eine Wiederherstellung kann nicht eingeschätzt werden.
  - Oder für die Wiederherstellung sind besondere Ressourcen erforderlich, z.B. regulär nicht geplante interne oder externe Ressourcen (Personal, Technik).

4.1.3 Wer ruft den Notfall aus?

Der Notfall wird im Normalfall durch die diensthabende Person für IT-Notfälle entsprechend ihrer Einschätzung ausgerufen.

Ist diese nicht erreichbar, so kann der IT-Notfall auch von folgenden anderen Beteiligten ausgerufen werden:

- Geschäftsleitung
- alle designierten Mitglieder des IT-Notfall-Stabs
- Leitung IT
- IT-Betrieb
- IT Help Desk
- ...

4.1.4 Unklare Situationen, Vorwarnung

Wurde aufgrund der in einem Moment vorliegenden Anhaltspunkte ein IT-Notfall ausgerufen und es stellt sich später heraus, dass kein Notfall vorliegt, so hat das für den ausrufenden Mitarbeiter (m/w/d) keine Folgen (Ausnahme: vorsätzliche Falschalarmierung).

Abhängig von der Entwicklung einer Situation kann der IT-Notfall auch zu einem späteren Zeitpunkt erklärt werden. Im Zweifelsfall sollte jedoch nicht zu lange gewartet werden, damit keine Zeit verloren geht.

Wurde in einer unklaren Situation noch kein Notfall ausgerufen, so sind die zu alarmierenden Personen trotzdem vorzuwarnen, insbesondere rechtzeitig vor Feierabend, Wochenenden, Betriebsferien.

4.2 Alarmierung

4.2.1 Grundsätze

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

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 (m/w/d), 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.

4.2.2 Alarmierung bei einem IT-Notfall

Bei Eintritt eines IT-Notfalls sind die folgenden Personen zu benachrichtigen:

IT-Notfall-Stab mit seinen Mitgliedern:

- ...

Geschäftsleitung, Administration

- Geschäftsleitung: ...
- Personal: ...
- Recht: ...
- Öffentlichkeitsarbeit: ...
- Betriebsrat: ...

Verantwortliche der Fachbereiche:

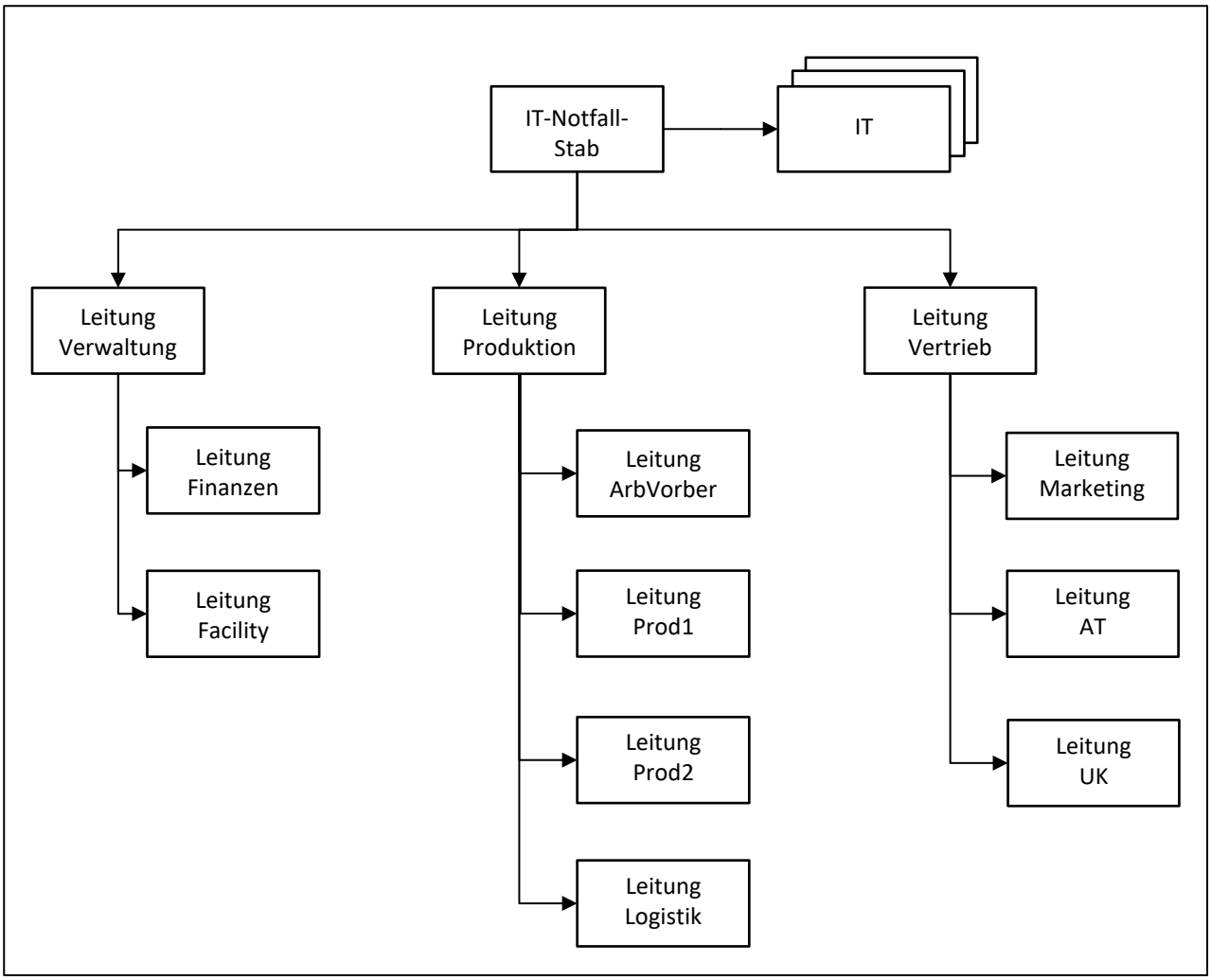
- ...

Je nach Situation bestimmte oder alle Mitarbeitenden - z.B. bei Malware-Befall

- ...
-

4.2.3 Meldebaum

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



4.2.4 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

5 Notfallmanagement durch den IT-Notfall-Stab

5.1 Allgemein

Die Verantwortung für die weitere Bearbeitung eines IT-Notfalls liegt beim IT-Notfall-Stab. Seine Mitglieder sind vorbestimmt und in ihre Aufgaben eingewiesen.

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 IT-Notfall-Stab keine "IT-Angelegenheit", sondern ist so zu besetzen, dass er im Hinblick auf die gesamte Geschäftstätigkeit maximal entscheidungs- und handlungsfähig ist.

5.2 Arbeitsräume für den IT-Notfall-Stab

Auf dem Firmengelände:

...

Ausweichräume außerhalb des Firmengeländes:

...

Virtuell:

...

5.3 Arbeitsmodi des Notfall-Stabs

Abhängig von der Situation sind für den Notfall-Stab die folgenden Arbeitsweisen denkbar:

- Information / bei Bedarf: Die Mitglieder werden über eine Situation regelmäßig informiert, kommen aber nur bei besonderem Bedarf zusammen. Beispielsweise anwendbar in einfachen Situationen, die längere Wartezeiten beinhalten (um z.B. Anwendungen neu zu konfigurieren).
- Teilzeit: Die Mitglieder kommen regelmäßig zusammen, um eine Situation zu besprechen. Sie nehmen jedoch auch ihre anderen Tätigkeiten wahr.
- Vollzeit: Die Mitglieder arbeiten ausschließlich an der Bewältigung der Situation. Das ist notwendig bei komplexen Situationen, die eine hohe Arbeitslast generieren, z.B. umfangreicher Malware-Befall.

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

5.4 Management von Wiederanlauf und Wiederherstellung

Die wichtigste Aufgabe ist der Wiederanlauf zu einem Notbetrieb sowie die Wiederherstellung des Normalbetriebs.

Siehe dazu die Kapitel

- Wiederanlauf und Wiederherstellung kritischer Geschäftsprozesse
- Wiederanlauf und Wiederherstellung der kritischen IT-Services

5.5 Meldepflichten

Bei einem IT-Notfall müssen u.U. innerhalb definierter Fristen Meldungen an Behörden und andere Institutionen gemacht werden.

Wenn KRITIS-Betreiber:

- Meldung von Sicherheitsvorfällen

Bei möglichen oder tatsächlichen 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

Die Meldungen sollten immer nachweisbar sein. Beispiel: schriftlich, Telefonate vor Zeugen führen, nachträglich Mails schreiben, Inhalt mit Datum und Uhrzeit dokumentieren usw.

Abhängig von der Situation sollte eine Anzeige bei der Polizei erwogen werden.

5.6 Dokumentation und Beweissicherung

5.6.1 Protokollierung der Ereignisse

Ein gravierender IT-Notfall mit längerer Unterbrechung kritischer Geschäftsprozesse kann später zu strafrechtlichen und zivilrechtlichen Konsequenzen für das Unternehmen und für Einzelpersonen führen. Daher ist eine fortlaufende Dokumentation aller Ereignisse sinnvoll. Jeder Eintrag sollte Datum und Uhrzeit beinhalten und mit so viel Kontextinformationen versehen werden, dass die Abläufe auch im Nachhinein noch gut nachvollzogen werden können.

5.6.2 Forensische Sicherung auf IT-Systemen

Je nach Situation sollten auf den relevanten IT-Systemen die Spuren forensisch gesichert werden (z.B. Logdateien). Dafür sollte ein Experte für Cyber-Sicherheit hinzugezogen werden.

5.7 Kommunikation

5.7.1 Interne Kommunikation

5.7.1.1 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.

5.7.2 Kommunikation mit Kunden

- Mail über Probleme und mögliche Verzögerungen.
- Informationen zu veränderten Erreichbarkeiten
- Informationsbanner auf der Website oder im Online-Shop

5.7.3 Kommunikation mit Behörden und Ämtern

Unabhängig von Meldepflichten (siehe unten) sollten je nach Situation mit Behörden und Ämtern Kontakt aufgenommen werden, um Schwierigkeiten durch Ordnungsgelder, Kontopfändungen usw. abzuwenden:

- Sich verzögernde Pflichtmeldungen an Finanzämter

- Sich verzögernde Zahlungen
- Sich verzögernde Bereitstellung statistischer Daten

5.8 Öffentlichkeitsarbeit

5.8.1.1 Übersicht

Notfälle haben eine erhebliche Auswirkung auf das Geschäft und sind damit in unterschiedlichen Graden auch außerhalb des Unternehmens wahrnehmbar, 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 dieser Situation erhalten bleibt.

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 bzw. die Organisation 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.

5.8.1.2 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
- ...

5.8.1.3 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>.

5.9 Alternative Organisation der Arbeit

In der Zeit der Unterbrechung bzw. während des Notbetriebs gibt es u.U. einen Überschuss an Mitarbeitenden, da Geschäftsprozesse unterbrochen sind, Infrastruktur nicht funktioniert, nicht genügend Arbeitsplätze zur Verfügung stehen u.a. Das sind Optionen, wie die Arbeit anders organisiert werden kann:

- Urlaub abbauen
- Kurzarbeit
- Arbeitsplätze aufräumen
- In mehreren Schichten arbeiten
- An Wochenenden arbeiten
- ...

6 Wiederanlauf und Wiederherstellung kritischer Geschäftsprozesse

Welche Geschäftsprozesse sind zeitkritisch und nutzen einen IT-Service, so dass eine Unterbrechung durch Ausfall dieser IT schwerwiegende Folgen für das Unternehmen hätte? Die Grundlage dafür liefert eine Business Impact-Analyse (BIA). Aus der maximal tolerierbaren Ausfallzeit abgeleitet ist die Reihenfolge beim Wiederanlauf in einen Notbetrieb.

6.1 Liste der kritischen Geschäftsprozesse

Reihen-folge beim Wieder-anlauf	Prozess	Tätigkeiten	Maximal tolerierbare Ausfallzeit	Besondere Anforderungen an die Verfügbarkeit	Genutzte IT-Services
	Primäre Prozesse				
1	Vertrieb	• Kundenbetreuung • Anfragen beantworten • Angebote erstellen und versenden • Aufträge empfangen • Aufträge erfassen	4 h	Weihnachts-geschäft im 4. Quartal	• Standard-Arbeitsplatz • Mail • Office • CRM-System
2	Produktions-planung	• ...	8 h		• Standard-Arbeitsplatz • ERP-System
2	Auftrags-abwicklung	•	8 h		• Standard-Arbeitsplatz • ERP-System
	Sekundäre Prozesse				
3	Buchhaltung	• ...	...	Steuervoraus-zahlungen	• Standard-Arbeitsplatz • Cloud-Service
3	Lohnbuchhalt ung			Gehalt am 20. jeden Monats	

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)

6.2 Geschäftsprozess: Vertrieb

Maximale Wiederanlaufzeit für Notbetrieb: 4 h

IT-Service	4 h	8 h	24 h	2 d	5 d
Standard-Arbeitsplatz	Notbetrieb, 2 Arbeitsplätze	Notbetrieb, 5 Arbeitsplätze	Notbetrieb, 10 Arbeitsplätze	Normalbetrieb	Normalbetrieb
Mail	Notbetrieb, nur Info@...	Notbetrieb, Ausweichsystem	Notbetrieb, Ausweichsystem	Normalbetrieb	Normalbetrieb
Office	Normalbetrieb, via Web	Normalbetrieb, via Web	Normalbetrieb	Normalbetrieb	Normalbetrieb
CRM-System	-	Notbetrieb, ohne Schnittstellen	Notbetrieb, nur Schnittstelle zum Online-Shop	Normalbetrieb	Normalbetrieb

6.3 Geschäftsprozess: Produktionsplanung

Maximale Wiederanlaufzeit für Notbetrieb: 8 h

IT-Service	4 h	8 h	24 h	2 d	5 d

6.4 Geschäftsprozess: Auftragsabwicklung

...

7 Wiederanlauf und Wiederherstellung der kritischen IT-Services

- Wie kann ein Notbetrieb hergestellt werden, so dass die kritischen Geschäftsprozesse wiederanlaufen können, wenn auch mit verringertem Durchsatz?
- Welche Maßnahmen müssen ergriffen werden, um den Normalbetrieb wiederzustellen?

7.1 Übergreifend

7.1.1 Mögliche Ersatz-Räumlichkeiten

Wo können kurzfristig Notstandorte aufgebaut werden?

Rechenzentrum

- Auf dem Gelände: ...
- Außerhalb des Geländes: ...

Aufbau von Arbeitsplätzen

- Auf dem Gelände: ...
- Außerhalb des Geländes: ...

7.1.2 Bedarf IT-Personal

Je nach Situation:

	Tag 1	Tag 2	Tag 3	Tag 4	Tag 5
Koordination					
Analyse der Situation					
Aufbau Ersatzinfrastruktur					
Aufsetzen neuer Arbeitsplatzrechner					
Aufsetzen neuer Server					
Installation und Konfiguration von Anwendungen					
...					

7.1.3 Dienstleister

Dienstleister frühzeitig benachrichtigen und Unterstützung anfordern

- IT-Infrastruktur
- Anbieter der genutzten Software bzw. Cloud-Anwendungen
- Telekommunikationsdienstleister
- Experten für Cyber-Sicherheit

7.1.4 IT-Infrastruktur

7.1.4.1 Kabel, Router, Switches

Bedarfe:

...

Möglichkeiten zur kurzfristigen Bereitstellung / Beschaffung von Kabeln, Router, Switches:

...

7.1.4.2 Server

Bedarfe:

...

Möglichkeiten zur kurzfristigen Bereitstellung / Beschaffung von Ersatz-Servern:

...

7.1.4.3 Cloud-Anbieter

Bedarfe:

...

7.1.4.4 Arbeitsplatz-Rechner

Bedarf an funktionierenden und virenfreien Arbeitsplatz-Rechnern für die kritischen Geschäftsprozesse:

	Tag 1	Tag 2	Tag 3	Tag 4	Tag 5

Möglichkeiten zur kurzfristigen Bereitstellung / Beschaffung von Arbeitsplatz-Rechnern:

...

7.1.5 Produktion

Welche Unternehmensteile oder externe Unternehmen können bestimmte Fertigungsschritte übernehmen, wenn Teile der eigenen Produktion ausgefallen sind?

...

7.2 Wiederanlauf / Wiederherstellung IT-Service "Standard-Arbeitsplatz"

...

7.3 Wiederanlauf / Wiederherstellung IT-Service "..."

Voraussetzungen:

- Räumlichkeiten
- funktionierende IT-Infrastruktur bzw. Cloud-Umgebung

Wiederanlauf für Notbetrieb

Aufgabe	Personal	Skill	Aufwand
Server aufsetzen			
Anwendung installieren & konfigurieren			
Datensicherung einspielen			
Schnittstellen einrichten			

Wiederherstellung für Normalbetrieb

Aufgabe	Personal	Skill	Aufwand

8 Verzeichnisse

8.1 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.

8.1.1 Intern

8.1.1.1 Geschäftsführung, Betriebsleitung

Name

Telefon

Mail

Privat

8.1.1.2 IT-Verantwortliche

Name

Telefon

Mail

Privat

8.1.1.3 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

8.1.2 Dienstleister

Ggf. unterschieden nach verschiedenen Standorten

8.1.2.1 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
- Cyber-Sicherheit

Themen

Name

Telefon

Mail

Themen

Name

Telefon

Mail

8.1.2.2 Cloud-Provider

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

Name

Notruf

Telefon

Mail

Web

Name

Notruf

Telefon

Mail

Web

8.1.2.3 Telekommunikationsunternehmen

Name

Notruf

Telefon

Mail

Web

8.1.2.4 Rechtsanwalt des Unternehmens

Name

Telefon

Mail

8.1.2.5 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

8.1.3 Behörden

Ggf. unterschieden nach verschiedenen Standorten

8.1.3.1 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

8.1.3.2 Datenschutzbehörde

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

Name

Telefon

Mail

Website

8.1.3.3 Umweltschutzbehörde

Name

Telefon

Mail

Website

8.1.3.4 Rathaus, Ordnungsamt

Name

Telefon

Mail

Website

8.1.4 Medien

Ggf. unterschieden nach verschiedenen Standorten

Örtliche Zeitung

Regionalfernsehen

8.2 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.

8.2.1 Standorte / Niederlassungen

Beschreiben Sie jeden Ihrer Firmen-Standorte

8.2.1.1 Standort 1: ...

Anschrift:

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

8.2.1.2 Standort 2: ...

8.2.2 IT-Infrastruktur

8.2.2.1 Rechenzentrum / Server

Server

8.2.2.2 Cloud-Dienste

8.2.2.3 Netzwerk

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

8.2.2.4 Internet-Anbindung

Provider: ...

Verträge: → Anhang

8.2.3 Anwendungen und Services

8.3 Weitere Verzeichnisse

(als separate Dateien)

Für jeden Standort:

- Gebäudepläne der Standorte
- Verkabelungspläne
- Plan Serverraum