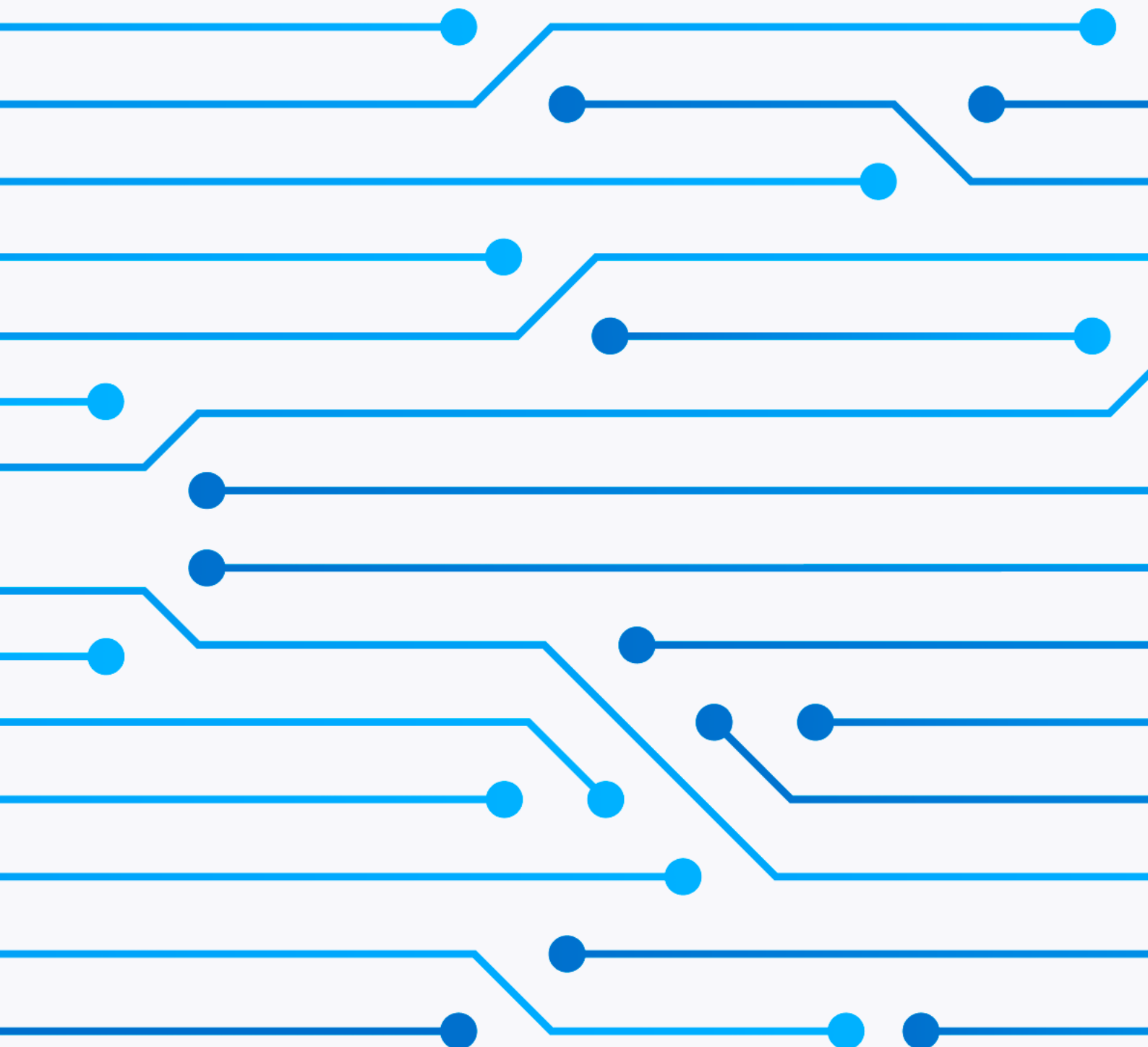


Notfallplan für den Cybersicherheitsvorfall

Schritt für Schritt auf den Notfall vorbereiten und reagieren



Inhalt

01 • Einleitung Seite 06

1.1 Wozu dient der Plan? Seite 06

1.2 Wie nutze ich diesen Plan? Seite 06

1.3 Exkurs: Wie lasse ich es erst gar nicht zu einem Notfall kommen? Seite 06

1.3.1 IT-Sicherheitsrichtlinien und IT-Sicherheitskonzept Seite 06

1.3.2 Einhaltung des Sicherheitskonzepts und der Richtlinien gewährleisten Seite 07

02 • Allgemeines Seite 07

2.1 Wer ist verantwortlich für den Notfallplan und dessen Umsetzung? Seite 07

2.2 Für welche Standorte und Abteilungen des Unternehmens gilt der Notfallplan? Seite 08

2.3 Gelten für meine Branche ggf. besondere Anforderungen an einen Notfallplan, z. B. kritische Infrastruktur, über die ich mich zusätzlich informieren sollte? Seite 08

03 • Vorbereitung auf den Notfall: Was muss ich im Vorfeld tun? Seite 09

3.1 Wie soll ein Cybersicherheitsvorfall beim ersten Auftreten gemeldet werden? Seite 09

3.1.1 Wem soll ein Vorfall gemeldet werden? Seite 09

3.1.2 Welche Informationen sollen dem Notfallkontakt gemeldet werden? Seite 09

3.2 Wie kann ich einschätzen, ob ein Cybersicherheitsvorfall einen Notfall für mein Unternehmen darstellt? Seite 10

3.2.1 Was gilt allgemein als Cybersicherheitsnotfall? Seite 11

3.2.2 Schritt 1: Wie definiert mein Unternehmen Kritikalität? Aufgabe: Definieren Sie gewünschte Reaktionszeiten für sich und Ihr Unternehmen. Seite 11

3.2.3 Schritt 2: Welche Informationen, die in meinem Unternehmen verarbeitet oder gespeichert werden, sind kritisch? Seite 12

Inhalt

3.2.4 Schritt 3: Welche Systeme und Software sind kritisch in meinem Unternehmen?	Seite 14
3.2.5 Schritt 4: Teilen andere Abteilungen und Experten meine Einschätzung?	Seite 16
3.3 Was könnten wahrscheinliche „Auslöser“ von Vorfällen in meinem Betrieb sein?	Seite 16
3.4 Wie ist die organisatorische Rollenverteilung im Notfall?	Seite 17
3.5 Welche Verhaltensregeln sollen im Notfall gelten?	Seite 19
3.6 Wie soll der Notfallprozess für Ihr Unternehmen aussehen?	Seite 20
3.7 Gibt es Prozesse für wahrscheinliche Szenarien, die Sie vordefinieren könnten?	Seite 21
a. E-Mail: Auf infizierten Link oder Anhang geklickt > Vorfall	Seite 22
b. E-Mail: Betrügerische Nachrichten von vermeintlichen Kunden/Partnern/Kollegen	Seite 22
c. Cyber-Erpressung: Information an GF	Seite 22
d. Exposition vertraulicher Daten	Seite 22
3.8 Wissen alle Mitarbeitenden, was im Notfall zu tun ist?	Seite 23
3.9 Sind der Notfallplan oder bereichsspezifische Notfallpläne für alle Mitarbeitenden verständlich dokumentiert und problemlos zugänglich (auch im Notfall)?	Seite 27
3.10 Gibt es einen Geschäftsführungsplan und einen Wiederherstellungs-/ Wiederanlaufplan?	Seite 27
3.10.1 Gibt es Ersatzsysteme und Sicherheitskopien, die im Notfall genutzt werden können?	Seite 27
3.10.2 Werden diese digital und räumlich getrennt von den üblichen Systemen aufbewahrt?	Seite 28
3.10.3 Werden diese regelmäßig auf ihre Funktion, Aktualität und Vollständigkeit getestet?	Seite 28
3.10.4 Wer ist zuständig, um den Wiederanlauf zu koordinieren?	Seite 29
3.10.5 Wie ist der Prozess bei der Inbetriebnahme und Wiederherstellung?	Seite 30

Inhalt

04 • Im Ernstfall: Umfangreicher Notfallplan für Notfallbeauftragte Seite 31

Notfallplan	Seite 31
A. Meine Verhaltensregeln	Seite 31
B. Allgemeiner Notfall-Prozess (ergänzen Sie ggf. um eigene Schritte)	Seite 31
C. Analyse der Meldung: Liegen Ihnen alle relevanten Informationen zum Vorfall vor?	Seite 32
D. Erste Beurteilung des Vorfalls: Liegt ein Notfall vor und wie kritisch ist dieser?	Seite 32
1. Welche Art von Vorfall wurde Ihnen gemeldet?	Seite 32
2. Welche Systeme und/oder Daten sind betroffen und finden sich kritische darunter? (Verfügbarkeit / Vertraulichkeit / Integrität)	Seite 33
Liste mit kritischen Systemen	Seite 33
Liste mit kritischen Daten	Seite 34
3. Welche Gefahren bestehen durch den Notfall?	Seite 34
4. Liegt ein Notfall vor?	Seite 34
5. Wie bewerte ich den Notfall?	Seite 34
E. Was kann die Ursache für diesen Notfall sein?	Seite 35
F. Welche ersten Maßnahmen könnten zur Behebung des Vorfalls getroffen werden?	Seite 35
G. Welche Beteiligte sollten informiert und als Unterstützung ins Boot geholt werden?	Seite 36
H. Welche ersten Maßnahmen könnten zum Wiederanlauf initiiert werden?	Seite 38
I. Wie kann ich den Vorfall nachbereiten? (inkl. Dokumentationspflichten)	Seite 39
1. Bewertung der Vorfall-Ursache	Seite 39
2. Bewertung der Behebung der Ursache	Seite 40
3. Bewertung der Sicherung/Wiederherstellung des Geschäftsbetriebs	Seite 40

Inhalt

4.	Bewertung des Kommunikationsprozesses	Seite 40
5.	Bewertung der Zusammenarbeit mit externen Beteiligten	Seite 40
6.	Schaden	Seite 40
7.	Dokumentation	Seite 40
05 .	Wie gewährleiste ich, dass der Plan aktuell bleibt?	Seite 41
	Anhang	Seite 42
1.	Liste mit allen bundesweit zuständigen Datenschutzaufsichtsbehörden	Seite 42
2.	Liste mit allen bundesweiten Ansprechpersonen der Polizei	Seite 43
	Quellen	Seite 44
	Impressum	Seite 45

01 | Einleitung

Jeder Notfall ist einzigartig und benötigt daher eine einzigartige Bewertung wie auch Vorgehensweise. Dieser Plan gibt ein grobes Gerüst vor und ist individuell für Ihr Unternehmen gestaltbar – unabhängig von bestimmter Hardware, Betriebssystemen, Protokollen oder Anwendungen.

1.1 Wozu dient der Plan?

Dieser Plan dient zur Vorbereitung auf den Notfall und als Handlungsorientierung im Notfall. Er soll das Notfallmanagement in Ihrem Unternehmen unterstützen: Notfälle definieren und beurteilen, Beteiligte identifizieren und Prozesse kreieren.

Der Notfallplan soll dabei unterstützen, weitere Schäden wie den Verlust von Betriebsgeheimnissen und Reputation zu vermeiden. Er soll dabei helfen, die Betriebsfähigkeit zu sichern oder wiederherzustellen und rechtliche Anforderungen zu erfüllen (IT-SicherheitsG, DSGVO).

1.2 Wie nutze ich diesen Plan?

Arbeiten Sie sich Schritt für Schritt durch unseren Plan. Wichtig ist, dass Sie im Vorfeld die Punkte unter „3. Vorbereitung auf den Notfall“ bearbeiten. Dadurch wird der allgemein gehaltene Plan individuell an die Bedürfnisse Ihres Unternehmens angepasst. Auf diese Weise haben Sie eine erste Übersicht der wichtigen Informationen im Notfall.

Bitte beachten sie, dass wir keine Gewähr für Vollständigkeit, Aktualität und Richtigkeit des Planes übernehmen.

1.3 Exkurs:

Wie lasse ich es erst gar nicht zu einem Notfall kommen?

Ebenso wichtig wie ein effektiver und verständlicher Notfallplan ist die Prävention. Indem Sie ein IT-Sicherheitskonzept mit verständlichen Richtlinien und regelmäßigen Übungen unternehmensweit etablieren, sorgen Sie dafür, dass ein Angriff auf Ihr Unternehmen so unwahrscheinlich wie möglich wird.

1.3.1 IT-Sicherheitsrichtlinien und IT-Sicherheitskonzept

Schaffen Sie ein umfassendes IT-Sicherheitskonzept für das gesamte Unternehmen (umfangreiche Informationen zum Thema „Notfallmanagement“ finden Sie im [BSI Standard 100-4](#)). Etablieren Sie in diesem Rahmen verständliche Richtlinien zu Themen wie der Nutzung privater Endgeräte, dem Umgang mit E-Mails, Passwort-Sicherheit, Arbeitsplatzsicherheit, sicherem Surfen im Netz, Home Office, Sicherheits-Updates, Patch-Management, Firewall – eine erste Orientierung finden Sie und Ihre Mitarbeitenden in unserem [Cybersicherheits-Training](#).

Hier ist Platz für Anmerkungen und um interne Richtlinien als Link o. ä. einzufügen.