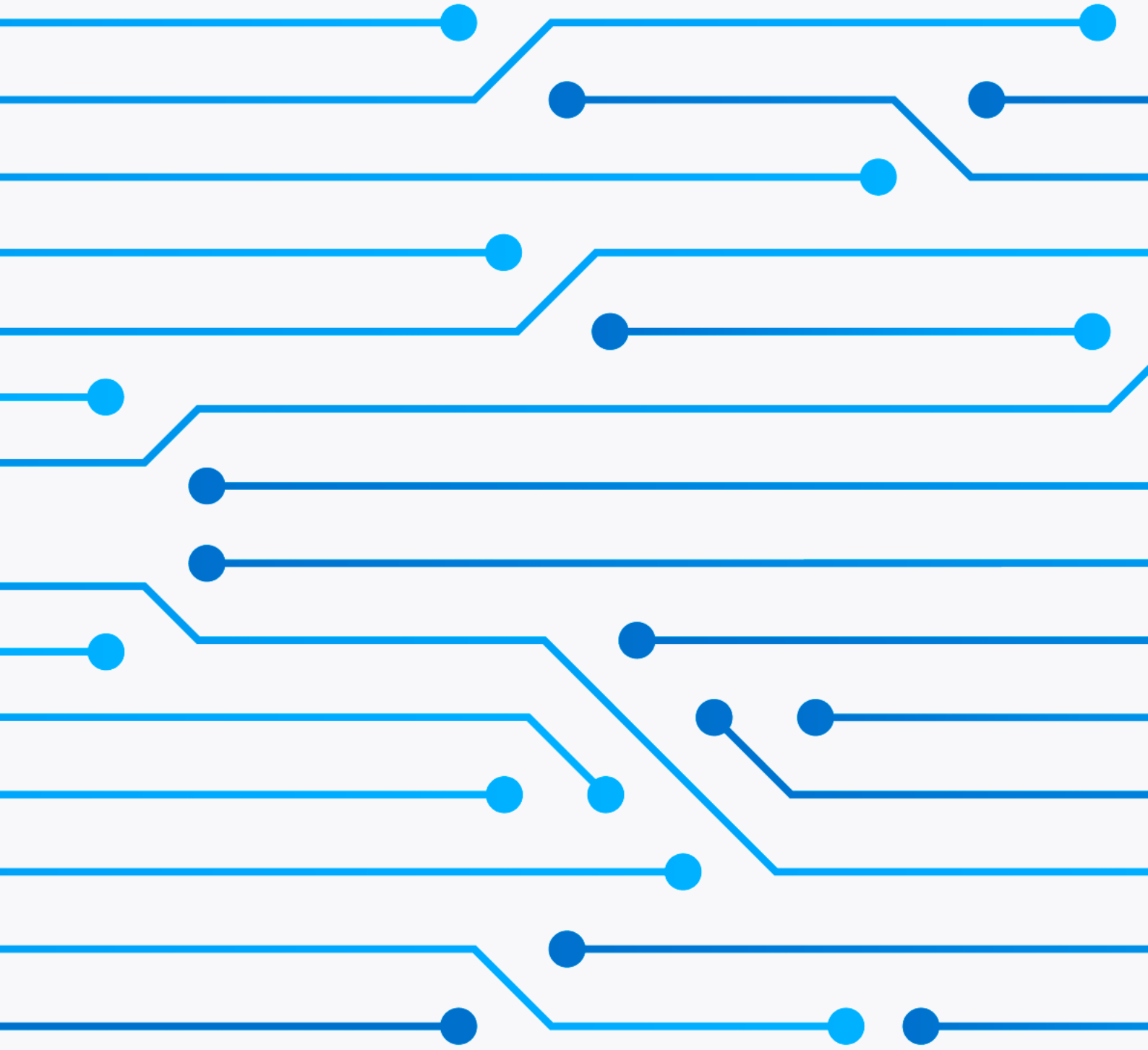
perseus.

Notfallplan für den Cybersicherheitsvorfall

Schritt für Schritt auf den Notfall vorbereiten und reagieren



Inhalt

Inhalt

Inhalt

Inhalt

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.

1.3.2 Einhaltung des Sicherheitskonzepts und der Richtlinien

Achten Sie darauf, dass das Sicherheitskonzept und die dazugehörigen Richtlinien umgesetzt werden.

- ☐ Sicherheit auf der Agenda in der gesamten Organisation
- ☐ Wiederholende Schulungen für Mitarbeitende
- ☐ Stichprobenartige Überprüfungen
- ☐ Regelmäßige Übungen zu cybersicherem Verhalten
- ☐ Kommunikationskonzept für Neuerungen
- ☐ Anreize für Einhaltung der Richtlinien

Hier ist Platz für Anmerkungen und um auf interne Routinen o.ä. zu verlinken.

02 | Allgemeines

2.1 Wer ist verantwortlich für den Notfallplan und dessen Umsetzung?

Vorname	
Nachname	
Position	
Abteilung	
Kontakt	

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

Standorte	Abteilungen

2.3 Gelten für meine Branche ggf. besondere Anforderungen an einen Notfallplan?

Aufgabe: Recherchieren Sie, ob an Ihre Branche spezielle Anforderungen im Sinne der IT-Sicherheit und des Datenschutzes im Notfall gelten und notieren Sie sich diese.

Hintergrund: Manche Branchen (z. B. kritische Infrastrukturen) sind dazu angehalten, besondere Sicherheitsanforderungen, Prozesse oder Meldepflichten im Notfall zu erfüllen. Dieser sollten Sie sich bereits im Vorfeld bewusst sein.

Hier ist Platz für Ihre Notizen.

03 | Vorbereitung auf den Notfall: Was muss ich im Vorfeld tun?

Sie sollten im Vorfeld relevante Informationen sammeln und notwendige Abläufe definieren, damit Sie im Notfall bereit sind, schnell und effektiv zu reagieren.

3.1 Wie soll ein Cybersicherheitsvorfall beim ersten Auftreten gemeldet werden?

3.1.1 Wem soll ein Vorfall gemeldet werden?

Aufgabe: Legen Sie eine zentrale erste Ansprechperson (Notfallkontakt) für alle Cybersicherheitsvorfälle fest. Benennen Sie außerdem eine Vertretung, so dass ein permanenter Kontaktpunkt gewährleistet ist. Sollte der Notfallkontakt nicht aus der IT stammen, sollte er regelmäßig geschult werden.

Hintergrund: Im Ernstfall ist es für die Mitarbeitenden hilfreich, nur eine erste Ansprechperson zu haben, die die Lage einschätzt, ggf. weitere Beteiligte informiert und über die nächsten Schritte entscheidet.

Orientierungshilfe:
Meist sind die IT-Verantwortlichen der erste Anlaufpunkt bei IT-Sicherheitsproblemen. Sie haben die beste Übersicht über Hard- und Software. Außderdem können sie deren Relevanz am besten einschätzen. Daher sind sie häufig eine gute Wahl als Notfallkontakt.

Rolle	Name, Vorname	Abteilung, Position	Telefon, E-Mail, Zimmer	Anmerkung
Notfallkontakt				
Vertretung				

3.1.2 Welche Informationen sollen dem Notfallkontakt gemeldet werden?

Aufgabe: Überlegen Sie sich, welche Informationen Sie von Erstmeldenden eines Vorfalls benötigen, um diesen effektiv, bewerten, kommunizieren und beheben zu können. Etablieren Sie eine „Better safe than sorry"-Kultur – lieber einmal unnötig Alarm schlagen, als einmal zu wenig.

Hintergrund: Indem Sie eine feste Struktur vorgeben, fällt es den Meldenden leichter, notwendige Informationen von irrelevanten zu unterscheiden. Auch Sie müssen nicht lange überlegen, welche Daten abzufragen sind. Nehmen Sie außerdem den Mitarbeitenden die Ängste, sich schnell bei Ihnen zu melden, erhalten Sie die Informationen hoffentlich schnellstmöglich – bevor ein größerer Schaden eintritt.

Orientierungshilfe:
Wie bei allen anderen Unfällen gelten die W-Fragen: Wo, wer, was, wie. Folgende Informationen halten wir für sinnvoll.

a. Wer meldet den Vorfall?
- Vorname, Nachname
- Department und Position des Meldenden
- Kontaktdaten

b. Wann und unter welchen Umständen ist der Vorfall zuerst aufgetreten?
- Erstbeobachtende identisch mit Meldenden? (falls nein, Name und Kontakt)
- Wann zuerst beobachtet?
- Datum und Uhrzeit des Vorfalls

c. Was für ein Vorfall liegt vor?
- Verlust der Vertraulichkeit
- Beeinträchtigung
- Störung
- Ausfall

d. Wie ist der Vorfall zu beschreiben?
- Langsamer Computer
- Kein Zugriff auf das System/Daten oder Teile davon
- Manipulation von Mitarbeitenden, z. B. unautorisierte Zahlungsaufforderungen
- Erpressungsversuch: Es wird eine Forderung für Zugriff auf System oder Daten gestellt. Es wird eine Forderung für das Unterlassen einer Handlung z. B. Veröffentlichung von sensiblen Daten gestellt.
- Hinweise von anderen, dass verdächtige Nachrichten von der eigenen Unternehmensdomain versendet werden
- Weitergeleitete Suche
- Daten im Internet
- Verdächtige Aktivitäten

e. Welche und wie viele Geräte, Programme und/oder Systeme sind betroffen?
f. Sind Daten betroffen? Wenn ja, welche? Wurden sie eingesehen, kopiert oder gelöscht?
g. Sind weitere Personen betroffen?
h. Wie kritisch erscheint der Vorfall?
i. Was wurde kurz vor dem Vorfall gemacht?
j. Welche Auswirkungen hat der Vorfall auf den Betrieb?

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

Als nächstes gilt es festzulegen, ab wann Ihr Unternehmen einen Cybervorfall tatsächlich als Notfall bewertet und welcher Reaktionsbedarf besteht. Dafür sind eine Reihe von Überlegungen und Entscheidungen vorzunehmen, durch die wir Sie Schritt für Schritt führen.

3.2.1 Was gilt allgemein als Cybersicherheitsnotfall?

Deutschlands Cybersicherheits-Behörde, das Bundesamt für Sicherheit in der Informationstechnik (BSI), definiert einen Cybersicherheitsnotfall als ein *„Schadensereignis, bei dem Prozesse oder Ressourcen einer Institution nicht wie vorgesehen funktionieren. Die Verfügbarkeit der entsprechenden Prozesse oder Ressourcen kann innerhalb einer geforderten Zeit nicht wiederhergestellt werden. Der Geschäftsbetrieb ist stark beeinträchtigt. Eventuell vorhandene SLAs (Service Level Agreements) können nicht eingehalten werden. Es entstehen hohe bis sehr hohe Schäden, die sich signifikant und in nicht akzeptablem Rahmen auf das Gesamtjahresergebnis eines Unternehmens oder die Aufgabenerfüllung einer Behörde auswirken. Notfälle können nicht mehr im allgemeinen Tagesgeschäft abgewickelt werden, sondern erfordern eine gesonderte Notfallbewältigungsorganisation."*
Kleinere Störungen wie ein defektes Gerät oder ein kurzfristiger Internetausfall sind beispielsweise Teil des Betriebsalltags. Sie sind einfach zu beheben und gelten nicht als Notfall.

Als Orientierung für mögliche Eskalationsstufen eines Vorfalls hat das BSI folgende Orientierung herausgegeben:

Eskalationsstufe			Beispiele
1	Grün	Normalbetrieb	–
2	Gelb	Störmeldungen	Ereignisse, die gemeldet, geprüft, dokumentiert und gegebenenfalls behoben werden müssen.
3	Orange	Voralarm	Ereignisse, die bereits erste Gefahren abwehrende oder Risiko reduzierende Maßnahmen erfordern, z. B. singuläre Brandlöschung.
4	Rot	Notfall	Ereignisse, die den Geschäftsbetrieb stark beeinträchtigen und nicht mehr innerhalb der geforderten Zeit behoben werden können.
5	Rot	Krise	Ereignisse mit Krisenpotential, die eine übergeordnete Koordinierung erfordern und die Existenz der Institution oder Leben gefährden.
6	Rot	Katastrophe	Großschadensereignisse, die nicht auf die Institution beschränkt sind.

Quelle: BSI -Standard 100-4

Um einen Notfall als solchen zu erkennen und richtig zu reagieren, sollten Sie sich im Vorfeld einen Überblick über die IT-Landschaft Ihres Unternehmens verschaffen und diese daraufhin überprüfen, wie kritisch ihr Ausfall/ihre Beeinträchtigung für Ihr Unternehmen ist. Auf diese Weise erhalten Sie eine Übersicht, die Sie im Ernstfall schnell zur Hand haben, um einen konkreten Vorfall und dessen Auswirkungen bewerten zu können.

3.2.2 Schritt 1: Wie definiert mein Unternehmen Kritikalität?

Aufgabe: Definieren Sie gewünschte Reaktionszeiten für sich und Ihr Unternehmen.

Hintergrund: „Kritisch" im Sinne des Notfallmanagements heißt „zeitkritisch". Je größer der drohende Schaden, umso schneller gilt es zu reagieren und eine Cybervorfall zu beheben. Umso wichtiger ist es, dass Sie Zeitfenster definieren, um ein vereinheitlichtes Verständnis zu haben, was die unterschiedlichen Stufen bedeuten.

Orientierungshilfe:
Mögliche Schäden, die bei der Bewertung zu berücksichtigen sind:
• Finanzieller Schaden
• Beeinträchtigung des Geschäftsbetriebs
• Verstoß gegen rechtliche Vorgaben z. B. DSGVO
• Verletzung von Vorschriften und Verträgen
• Negative Innen- und Außenwirkung (Reputationsschaden)
• Personenschaden
• Sonstige:

Kritikalitäts-kategorie	Wiederanlauf	Maximale tolerierbare Ausfallzeit	Gesamt-schaden nach x Stunden	Allgemein
„unkritisch“	> 720 Stunden	> 504 Stunden	„niedrig“	Ausfall hat keine oder nur minimale Auswirkungen.
„wenig kritisch“	≤ 720 Stunden	≤ 504 Stunden	„normal“	Ausfall hat Auswirkungen.
„kritisch“	≤ 168 Stunden	≤ 240 Stunden	„hoch“	Ausfall hat beträchtliche Auswirkungen.
„hoch kritisch“	≤ 4 Stunden	≤ 6 Stunden	„sehr hoch“	Ausfall oder Beeinträchtigung führen zu existen-tiell bedrohlichen Auswirkungen.

Quelle: BSI -Standard 100-4

So definiert mein Unternehmen Kritikalität:
• HOCH KRITISCH: Reaktion innerhalb von Stunde(n) einleiten, z. B. 1 Stunde.
• KRITISCH: Reaktion innerhalb von Stunde(n) einleiten, z. B. bis 2 Stunden.
• WENIG KRITISCH: Reaktion innerhalb von Stunde(n) einleiten, z. B. 24 Stunden.
• UNKRITISCH: Reaktion innerhalb von Stunde(n) einleiten, z. B. 72 Stunden.

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

Aufgabe: Dokumentieren Sie sämtliche Typen elektronischer Daten, die in Ihrer Organisation gespeichert und verarbeitet werden. Überlegen Sie, welche Auswirkungen ihr Ausfall, ihre Manipulation oder auch ein Verlust ihrer Vertraulichkeit hätte.

Hintergrund: Während eines Cybervorfalls ist oft wenig Zeit, um sich über die Relevanz betroffener Daten und die möglichen Konsequenzen eines Vorfalls in ihrem Zusammenhang klar zu werden. Solch eine im Vorfeld präparierte Liste gibt Ihnen im Notfall eine Orientierung, welche Daten betroffen sein könnten und wie kritisch ein Vorfall ist, der diese betrifft.

Orientierungshilfe:
Unterstützend könnten Sie beispielsweise das Verarbeitungsverzeichnis Ihres Unternehmens nutzen Darin sollten verarbeitete Daten je nach Schutzbedarf unterschiedlich klassifiziert werden. Meist gibt es drei Kategorien: öffentlich, intern und vertraulich. Öffentliche Daten sind häufig auch im Internet zu finden und es besteht keine Gefahr für das Unternehmen, wenn Fremde diese erhalten bspw. Adressdaten, Kundenservice-Telefon o.ä. Interne Daten sind nicht für die Öffentlichkeit gedacht. Ihre Veröffentlichung birgt eher ein geringes Risiko, aber es wirkt dennoch nicht professionell, z. B. Marktanalysen. Die Veröffentlichung von vertraulichen Daten birgt enorme Sicherheitsrisken für das Unternehmen, deren Angestellte oder deren Kundschaft und Partner. Darunter versteht man zum Beispiel sensible Informationen wie Geburtsdaten der Mitarbeitenden, Zahlungsinformation von Kundinnen und Kunden oder Betriebsgeheimnisse.

Mögliche Gefahre eines Cybervorfalls
- Manipulation: Daten und Systeme werden durch Unbefugte geändert.
- Verlust Vertraulichkeit: Daten und Systeme werden durch Unbefugte eingesehen.
- Störung: Daten und Systeme stehen nicht in voller Funktion für Befugte zur Verfügung.
- Ausfall: Daten und Systeme sind nicht für Befugte verfügbar.
- Löschung: Daten und Systeme werden komplett gelöscht.

Mögliche Schäden, die bei der Bewertung zu berücksichtigen sind:
- Finanzieller Schaden
- Beeinträchtigung des Geschäftsbetriebs
- Verstoß gegen rechtliche Vorgaben z. B. DSGVO
- Verletzung von Vorschriften und Verträgen
- Negative Innen- und Außenwirkung (Reputationsschaden)
- Personenschaden
- Sonstige:

1. Vorfall hat eine geringe, kaum spürbare Auswirkung (Bewertung: niedrig).
2. Vorfall hat spürbare Auswirkungen. („normal“)
3. Vorfall hat erhebliche Auswirkungen. („hoch“)
4. Vorfall oder Beeinträchtigung führen zu existentiell bedrohlichen Auswirkungen. („sehr hoch“)

Daten	Daten-klassifizierung	Auswirkungen	Anmerkungen
Daten der Mitarbeitenden			
Betriebs-geheimnisse			
Kontaktdaten Partner			
Kontaktdaten Kundschaft			
Sonstige			

3.2.4 Schritt 3: Welche Systeme und Software sind kritisch in meinem Unternehmen?

Aufgabe: Dokumentieren Sie sämtliche Hardware, Software und Systeme Ihrer Organisation. Überlegen Sie, welche Auswirkungen ein Ausfall, eine Störung, eine Sabotage oder auch ein Verlust der Vertraulichkeit auf diese hat. Überlegen Sie außerdem, welche der oben bestimmten sensiblen Daten mit Hilfe dieser verarbeitet oder gespeichert werden.

Hintergrund: Sobald Ihnen ein Cybervorfall und dazugehörige Details (wie das betroffene System) gemeldet werden, können Sie anhand einer präparierten Liste ablesen, welche Auswirkungen der Vorfall auf das betroffene System und somit auf den Betrieb haben könnte. Auf diese Weise haben sie einen Anhaltspunkt, um die Kritikalität des Vorfalls einzuschätzen, ihn ggf. als Notfall zu klassifizieren und die erforderlichen Maßnahmen in der gebotenen Zeit einzuleiten.

Orientierungshilfe: Überlegen Sie, **welche** Systeme im Unternehmen genutzt werden. Führen Sie sich vor Augen, **wie** diese verwendet werden und reflektieren Sie, welche negativen Auswirkungen ihr Ausfall oder ihre Beeinträchtigung für das Unternehmen haben könnten. Nehmen Sie die zuvor erarbeitete Liste zur Hand, um zu überlegen, welche Daten mithilfe des Systems verarbeitet oder gespeichert werden.

Mögliche Gefahre eines Cybervorfalls

- Manipulation: Daten und Systeme werden durch Unbefugte geändert.
- Verlust Vertraulichkeit: Daten und Systeme werden durch Unbefugte eingesehen.
- Störung: Daten und Systeme stehen nicht in voller Funktion für Befugte zur Verfügung.
- Ausfall: Daten und Systeme sind nicht für Befugte verfügbar.
- Löschung: Daten und Systeme werden komplett gelöscht.

Mögliche Schäden, die bei der Bewertung zu berücksichtigen sind:

- Finanzieller Schaden
- Beeinträchtigung des Geschäftsbetriebs
- Verstoß gegen rechtliche Vorgaben z. B. DSGVO
- Verletzung von Vorschriften und Verträgen
- Negative Innen- und Außenwirkung (Reputationsschaden)
- Personenschaden
- Sonstige:

System + Software	Betroffene Daten	Verlust Vertraulichkeit Auswirkung	Max. tolerierbare Ausfallzeit	Ausfall Auswirkung	Sabotage Auswirkung	Notizen: Abhängigkeiten mit anderen Systemen
Betriebssystem						
Server						
Telekommunikation						
E-Mail-Programm						
Kalender						
Design-Software						
E-Mail-Marketing-Tool						
HR-Tool						

System + Software	Betroffene Daten	Verlust Vertraulichkeit Auswirkung	Max. tolerierbare Ausfallzeit	Ausfall Auswirkung	Sabotage Auswirkung	Notizen: Abhängigkeiten mit anderen Systemen
Sonstige						

3.2.5 Schritt 4: Teilen andere Abteilungen und Experten meine Einschätzung?
Aufgabe: Holen Sie sich die Meinung relevanter Kolleginnen und Kollegen zu der Übersicht ein.

Hintergrund: Es ist schwierig, den Überblick über alle verwendeten Systeme und Softwares zu behalten. Auf diese Weise gehen Sie sicher, nichts vergessen und deren Rolle im Geschäftsbetrieb richtig eingeschätzt zu haben.

3.3 Was könnten wahrscheinliche „Auslöser" von Vorfällen in meinem Betrieb sein?

Aufgabe: Überlegen Sie, was mögliche und wahrscheinliche Auslöser für einen Cybersicherheitsvorfall sein könnten?

Hintergrund: Indem Sie im Vorfeld wahrscheinliche Ursachen eingrenzen, können Sie im Notfall diese als erstes prüfen und gewinnen wertvolle Zeit in der Behebung des Vorfalls. Des Weiteren können Sie präventiv geeignete Schutzmaßnahmen treffen.

Haken Sie je Ursache an.

Kritikalitäts-kategorie	Ja	Nein	Anmerkung
Falsche Systemkonfiguration	☐	☐	
Unbeabsichtigte Informationspreisgabe durch Mitarbeitende, z. B. Fotos auf Social Media, falsche Software-Konfiguration	☐	☐	
Fehlende System-/Software-Updates	☐	☐	
Denial-of-Service-Angriff	☐	☐	
Physischer Vandalismus	☐	☐	
Mängel Passwort- bzw. Zugangssicherheit	☐	☐	
Phishing	☐	☐	

Kritikalitäts-kategorie	Ja	Nein	Anmerkung
Weiteres Social Engineering	☐	☐	
Erpressung mittels Ransomware	☐	☐	
Elementarereignis (z. B. Sturm, Stromausfall…)	☐	☐	
Sonstiges Fehlverhalten von Mitarbeitenden	☐	☐	
Sonstige Virus-/Malware-Infektion	☐	☐	
Sonstiges Zufallsereignis	☐	☐	
Sonstiges	☐	☐	

3.4 Wie ist die organisatorische Rollenverteilung im Notfall?

Aufgabe: Überlegen Sie sich, welche internen als auch externen Beteiligten im Notfall informiert und involviert werden müssen. Notieren Sie zudem, welche Rolle diese im Notfall spielen könnten. Stimmen Sie Ihre Notizen mit den Betroffenen ab. Berücksichtigen Sie dabei auch andere Standorte.

Hintergrund: Im Notfall sollten Sie alle notwendigen Beteiligten schnellstmöglich identifizieren und kontaktieren können. Andersherum sollten diese wissen, dass Sie ihre Ansprechpersonen sind und welche Rolle sie im Notfall spielen.

Orientierungshilfe:
Eine Person kann auch mehrere Rollen erfüllen. Mögliche Rollen, die im Notfall übernommen werden könnten:
- Ansprechperson in der Abteilung
- Notfallbeauftragter und Vertretung
- Mitglied des Krisenstabs (Entscheidungen auf höherer Ebene)
- Mitglied des Notfallteams (operative Ebene zur Behebung des Notfalls)

Interne Beteiligte

Abteilung	Name	Kontakt (Tel. und E-Mail)	Rolle	Anmerkung z. B. Standort
IT				
Datenschutz + Rechtsabteilung				

Abteilung	Name	Kontakt (Tel. und E-Mail)	Rolle	Anmerkung z. B. Standort
Kommunikation/Presse				
Personal				
Geschäftsführung				
Produkt				
Kundenservice				
Operations				
Sonstige				

Externe Beteiligte

Dokumentieren Sie Einzelheiten des Vertrags, seine Abdeckung, wie sie Ihnen helfen können und zu welchem Zeitpunkt Sie mit ihnen in Kontakt treten müssen.

	Name (Firma und Ansprechpartner)	Kontakt (Tel. und E-Mail)	Vertrags-/ Kundennummer	Anmerkung
Externer IT-Dienstleister				
Incident Response-Anbieter	Perseus Technologies GmbH			24/7 erreichbar
Telekommunikationsanbieter				
Cyberversicherung	HDI	+49 511/3031 7000		Cyberversicherung umgehend informieren
Polizei				
Feuerwehr				

	Name (Firma und Ansprech-partner)	Kontakt (Tel. und E-Mail)	Vertrags-/ Kunden-nummer	Anmerkung
Datenschutz-aufsichtsbehör-de (siehe Liste im Anhang)				
Bundesamt für Sicherheit in der Informations-technik				
Wichtige Partner				
Wichtige Kunden				
Cloud-Service-Anbieter				
Stromanbieter				
Wasser-versorger				
Sonstige				

3.5 Welche Verhaltensregeln sollen im Notfall gelten?

Aufgabe: Überlegen Sie sich, welches Verhalten Sie sich im Notfall innerhalb Ihres Unternehmens wünschen, um optimal reagieren zu können. Schreiben Sie diese Verhaltensregeln nieder. Achten Sie darauf, dass es nicht zu viele sind.

Hintergrund: In einer Stresssituation kann es hilfreich sein, eine klare Erwartungshaltung zu definieren und gewisse Regeln vorzuformulieren, die Situation zu entspannen.

Orientierungshilfe: Wir haben vier allgemein akzeptierte Regeln für sie aufgelistet. Diese können Sie je nach Wunsch anpassen und ergänzen.

- Ruhe bewahren
- Notfallplan zur Hand nehmen
- Offene Kommunikation statt Schweigen
- Fokus auf Lösungen setzen, statt auf die Suche nach Schuldigen
- Dokumentieren, wo möglich

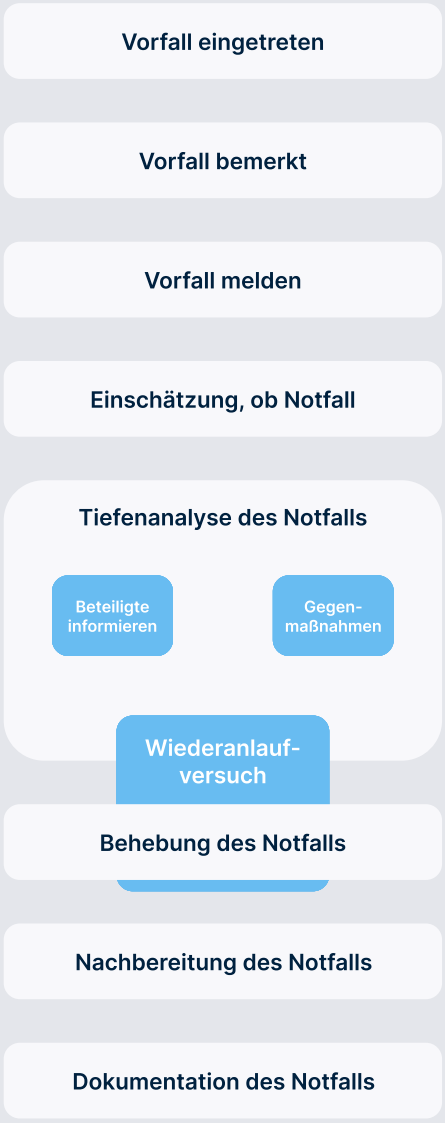
• Sonstiges:

3.6 Wie soll der Notfallprozess für Ihr Unternehmen aussehen?

Aufgabe: Überlegen Sie sich, wie ein übergreifender Notfallprozess in Ihrem Unternehmen gestaltet werden kann. Neben dem bloßen Prozess sollten Sie sich überlegen, welche Verhaltensregeln im Notfall gelten sollten. Skizzieren Sie diesen gerne mithilfe unserer Vorlage. Holen Sie sich das Feedback von dem Team ein, mit dem Sie im Notfall zusammenarbeiten.

Hintergrund: Bei einem Cybervorfall geht es oft etwas chaotisch zu. Wenn Sie im Vorfeld klare Prozesse kommuniziert und etabliert haben, sparen Sie wertvolle Zeit.

Orientierung:
So könnte ein grober Notfallprozess aussehen:



3.7 Gibt es Prozesse für wahrscheinliche Szenarien, die Sie vordefinieren könnten?

Aufgabe: Überlegen Sie, ob es wahrscheinliche Vorfalls-Szenarien gibt, für die Sie im Vorfeld genauere Verhaltensrichtlinien definieren können. Vielleicht gab es bereits einen oder mehrere Vorfälle, die ein Muster offenbarten. Vielleicht gab es schon Situationen, in denen Sie einen Vorfall noch abwenden konnten. Dokumentieren Sie diese Szenarien abstrakt und legen Sie Verhaltensrichtlinien fest, an denen die Mitarbeitenden sich orientieren können.

Hintergrund: Derartige Erstmaßnahmen helfen im Ernstfall Zeit zu sparen und den Schaden einzudämmen. Auf diese Weise kann eine tiefere Analyse erfolgen und weitere Maßnahmen getroffen werden.

Orientierung:
Folgende Erstmaßnahmen könnten je nach Fall empfehlenswert sein. Entscheiden Sie selbst, ob diese für Ihr Unternehmen zutreffen.

a. E-Mail: Auf infizierten Link oder Anhang geklickt > Vorfall
- **SOFORT:** PC vom Netzwerk trennen (LAN-Kabel ziehen)/evtl. direkt herunterfahren
- **SOFORT:** Notfallbeauftragte und Vertretung informieren > diese übernehmen die weitere Bearbeitung und Meldekette
- **Weitere Schritte**
  - IT-Verantwortliche/Dienstleister informieren
  - Weitere Schritte nach telefonischer Absprache
  - Information an Geschäftsführung
  - Mögliche Datenschutzverletzung prüfen

b. E-Mail: Betrügerische Nachrichten von vermeintlichen Kunden/Partnern/Kollegen:
- **SOFORT:** In keiner Form antworten
- **SOFORT:** Notfallbeauftragte und Vertretung informieren > diese übernehmen die weitere Bearbeitung und Meldekette
- **Weitere Schritte** (durch Notfallbeauftragte, wenn nicht erreichbar selbstständig):
  - IT-Verantwortliche/-Dienstleister informieren
  - Weitere Schritte nach telefonischer Absprache
  - Betreffende Personen telefonisch informieren, damit diese ihre Systeme prüfen können. (Nicht Tel.-Nummer aus Mail nehmen, sondern aus verifizierbarer Mail/früherem Kontakt/offizieller Website)
  - Information an Geschäftsführung und interne Kommunikation, so dass Kollegen ebenfalls gewarnt werden können
  - Anzeige bei der Polizei
  - Mögliche Datenschutzverletzung prüfen

c. Cyber-Erpressung: Information an GF
- **SOFORT:** In keiner Form antworten
- **SOFORT:** Notfallbeauftragte und Vertretung informieren > diese übernehmen die weitere Bearbeitung und Meldekette.
- **Weitere Schritte** (durch Notfallbeauftragte, wenn nicht erreichbar selbstständig):
  - IT-Verantwortliche/-Dienstleister informieren
  - GF informieren
  - Anzeige bei der Polizei
  - Mögliche Datenschutzverletzung prüfen

d. Offenlegung vertraulicher Daten
- **SOFORT:** Wenn möglich, unbefugten Zugriff auf sämtliche Daten unterbinden (z. B. Passwort ändern und Zwei-Faktor-Authentifizierung) oder veröffentlichte Daten löschen
- **SOFORT:** Notfallbeauftragte und Vertretung informieren > diese übernehmen die weitere Bearbeitung und Meldekette
- **Weitere Schritte** (durch Notfallbeauftragte, wenn nicht erreichbar selbstständig):
  - IT-Verantwortliche/-Dienstleister informieren
  - GF informieren
  - Mögliche Datenschutzverletzung prüfen und entsprechend handeln

3.8 Wissen alle Mitarbeitenden, was im Notfall zu tun ist?

Aufgabe: Informieren Sie die Belegschaft über die Existenz des Notfallplans, dessen Funktion und die Rolle jeder und jedes einzelnen. Setzen Sie eine Übung an, um den Ablauf und die Rolle jeder und jedes einzelnen zu trainieren. Werten Sie die Übung aus und kommunizieren Sie, was gut und was schlecht gelaufen ist. Dokumentieren Sie das Ganze.

Hintergrund: Alle Mitarbeitenden und alle Beteiligten Ihres Notfallteams sollten sich Ihrer Aufgaben im Notfall bewusst sein. Eine Übung des Ganzen ist erforderlich, um eine gewisse Sicherheit und um Routinen zu etablieren.

Orientierungshilfe: Nutzen Sie unsere Notfallkarte, um der Belegschaft eine grobe Orientierung zu geben, wie diese sich im Notfall verhalten soll. Sie können diese ausdrucken und an jedem Arbeitsplatz in Papierform zur Verfügung stellen.

Cyber-Notfallkarte – jetzt vorbereiten!

Wie erkenne ich einen Cyberangriff?	1. Veränderte Dateien oder Inhalte Achten Sie auf plötzlich veränderte **Symbole, Datei-Endungen** oder **Datei-Inhalte**. Dies könnten Anzeichen eines Cyberangriffs sein. 2. Verdächtige Meldungen Eine **Popup** Nachricht mit einer Zahlungsaufforderung ist ein sehr deutliches Zeichen für eine Cyberattacke. Des Weiteren können plötzlich auftretende **Systemfehlermeldungen** auf einen Virus hinweisen. Letzteres kann Ihr IT-Administrator für Sie prüfen. 3. "Automatisch" ausgelöste Aktionen Sollten Dateien **abrupt verschwinden** oder **automatisiert E-Mails** über Ihren Zugang verschickt werden, ist das ein klares Zeichen. Ebenso eindeutig ist es, wenn Ihr Browser **eigenständig unseriöse Webseiten** aufruft.
Wissen, wie Sie die Netzwerkverbindung trennen können.	Bei einem Angriff sollten Sie Ihren Rechner vom Internet und vom Firmennetzwerk trennen können. Vergewissern Sie sich, dass Sie die Funktionen bei Ihrem Rechner auch wirklich finden und bedienen können. Dazu können Sie am Rechner und auf Mobilgeräten den Empfang mobiler Daten ausschalten: • WLAN • mobiles Netz • Kabelverbindung mit dem Firmennetz
Notieren Sie Sich Ihre Daten.	**Benutzername:** **Rechnerkennung:**
Erstellen Sie regelmäßige Backups Ihrer Daten.	Programme lassen sich leicht neu installieren, aber Ihre Daten können bei einem Cyberangriff unwiederbringlich verloren gehen. Machen Sie unbedingt **regelmäßige Backups** Ihrer Dateien oder verwenden Sie **Cloud- oder Netzwerkspeicher**, die in der Regel automatisch Sicherheitskopien anfertigen und somit selbst gegen die meisten Verschlüsselungsangriffe genug Sicherheit bieten.
Notfallkarte ausdrucken und griffbereit legen.	Die "Cyber-Notfallkarte" sollte in **ausgedruckter** Form immer **griffbereit** liegen, so dass Sie bei einem evtl. Ausfall Ihres Rechners durch eine Cyberattacke darauf zugreifen können.

Richtiges Verhalten bei einem Cybersicherheits-Zwischenfall

Bewahren Sie Ruhe.	Nicht immer muss hinter verdächtigen Aktivitäten auf Ihrem Computer ein Cyberangriff stecken. Selbst wenn Sie angegriffen wurden, gilt: Ruhe bewahren, keine Kurzschlussreaktionen, der Notfallkarte folgen und umgehend Hilfe beim IT-Verantwortlichen suchen. **Arbeiten Sie auf keinen Fall weiter auf dem betroffenen Gerät!**
Informieren Sie Ihren IT-Administrator oder offiziellen IT-Notfallkontakt	Suchen Sie umgehend Hilfe bei Ihren IT-Verantwortlichen bzw. IT-Notfallkontakt. **Name:** **Telefonnummer:** Ihr erster Ansprechpartner sind IMMER die IT-Verantwortlichen bzw. Der offizielle Notfallkontakt Ihres Unternehmens. Nur diese können entscheiden, ob Sie eine Cyber-Notfallhilfe in Anspruch nehmen müssen.
Trennen Sie die Netzwerkverbindung.	Vielleicht versendet Ihr Rechner gerade geheime Firmendaten oder wird von einem Hacker heimlich im Hintergrund ferngesteuert. Durch die Trennung der Netzverbindung **schützen Sie Ihre Firmengeheimnisse** und verhindern eventuell, dass Ihr Rechner noch andere Rechner Ihrem Netzwerk infizieren kann.
Lassen Sie Ihren Computer angeschaltet.	Nachdem Sie die Internet- und Netzwerkverbindung getrennt haben, ist es in der Regel empfehlenswert, Ihren Rechner angeschaltet zu lassen, damit **Cybersicherheit-Experten** den Vorfall korrekt analysieren können.
Wenn Sie erpresst werden, folgen Sie auf keinen Fall den Anweisungen, sondern wenden Sie sich immer an Ihren IT-Verantwortlichen.	Eigentlich selbstverständlich: Wer andere erpresst, ist **auf keinen Fall vertrauenswürdig.** Wer an einen Cyber-Erpresser Geld überweist, bekommt deshalb noch lange nicht seine Daten zurück – egal was der Verbrecher vorab verspricht.
Warnen Sie Ihr Team.	Sollten Sie die Befürchtung haben, dass Kollegen ebenfalls Opfer des Angriffs werden könnten (z.B. wenn eine Phishing-E-Mail der Auslöser war,) dann warnen Sie Ihre Kollegen oder bitten einen Verantwortlichen (Gesch.ftsführer, IT-Administrator) darum.
Dokumentieren Sie den Vorfall.	Wenn möglich, **fotografieren** Sie Ihren Bildschirminhalt mit einem anderen Gerät (z.B. Handy). Alternativ können Sie den Vorfall selbstverständlich auch **schriftlich** festhalten.

Melden Sie alle bekannten Details des Vorfalls.

Folgende Informationen sind relevant:

a. Wer meldet den Vorfall?
- Vorname, Nachname
- Abteilung und Position des Meldenden
- Kontaktdaten

b. Wann und unter welchen Umständen ist der Vorfall zuerst aufgetreten?
- Erstbeobachtende identisch mit Meldenden? (falls nein, Name und Kontakt)
- Wann zuerst beobachtet? (Datum und Uhrzeit des Vorfalls)

c. Was für ein Vorfall liegt vor?
- Verlust der Vertraulichkeit
- Beeinträchtigung
- Störung
- Ausfall

d. Wie ist der Vorfall zu beschreiben?
- Langsamer Computer
- Kein Zugriff auf das System/Daten oder Teile davon
- Manipulation von Mitarbeitenden, z. B. unautorisierte Zahlungsaufforderungen
- Erpressungsversuch: Es wird eine Forderung für Zugriff auf System oder Daten gestellt. Es wird eine Forderung für das Unterlassen einer Handlung, z. B. Veröffentlichung von sensiblen Daten, gestellt.
- Hinweise von anderen, dass verdächtige Nachrichten von der eigenen Unternehmensdomain versendet werden
- Weitergeleitete Suche
- Daten im Internet
- Verdächtige Aktivitäten

e. Welche und wie viele Geräte, Programme und/oder Systeme sind betroffen?

f. Sind Daten betroffen? Wenn ja, welche? Wurden sie eingesehen, kopiert oder gelöscht?

g. Wie kritisch erscheint der Vorfall?

h. Was wurde kurz vor dem Vorfall gemacht?

i. Welche Auswirkungen hat der Vorfall auf den Betrieb?

3.9 Sind der Notfallplan oder bereichsspezifische Notfallpläne für alle Mitarbeitenden verständlich dokumentiert und problemlos zugänglich (auch im Notfall)?

Aufgabe: Hinterlegen Sie eine vereinfachte Form des Notfallplans und die ausführliche Form des Notfallplans in digitaler Form und in physischer Form. Weiter unten finden Sie beide Pläne, die entsprechend Ihren obigen Angaben vorausgefüllt wurden. Hinterlegen Sie die Pläne so, dass sie für alle umstandslos zugänglich sind. Kommunizieren Sie klar und auf mehreren Kanälen (E-Mail, Schulung, Kommunikation durch Supervisor), wo die Pläne zu finden sind.

Hintergrund: Da ggf. nicht alle Mitarbeitenden im Ernstfall den Notfallplan vor Augen haben, kann es hilfreich sein, dass sie wissen, wo er liegt und ihn ohne Umstände erreichen können. Da im Falle eines Cybernotfalls eventuell der digitale Zugriff unmöglich ist, sollte der Plan auch in Papierform hinterlegt sein.

Orientierungshilfe:
Hier können Sie notieren, wann, wo und wie die Pläne hinterlegt sind.

Form	Wo hinterlegt? (Link oder Beschreibung)	Wann kommuniziert?	Anmerkungen
Digitaler Plan			
Physischer Plan			

3.10 Gibt es einen Geschäftsfortführungsplan und einen Wiederherstellungs-/ Wiederanlaufplan?

Um die Funktionalität des betroffenen Systems wiederherzustellen und die Betriebsfähigkeit schnellstmöglich wieder aufzunehmen, ist es erforderlich, im Vorfeld gewisse organisatorische und technische Maßnahmen zu treffen:

3.10.1 Gibt es Ersatzsysteme und Sicherheitskopien, die im Notfall genutzt werden können?

Aufgabe: Prüfen Sie, ob es Ersatzsysteme und Sicherheitskopien aller relevanten Daten gibt. Ist dies nicht der Fall sollten Sie dies umgehend organisieren. Hinterlegen Sie eine Liste der gesicherten Systeme und Daten.

Hintergrund: Festplatten, Rechner, Server und ganze Systeme können durch technische Defekte oder aber durch Cyberangriffe, wie der Installation von Malware, unbrauchbar gemacht werden. Schlimmstenfalls, sind diese dann für immer verloren. Durch Backups erstellen Sie Sicherheitskopien Ihrer Daten. Durch diese können verlorene oder zerstörte Inhalte und sogar ganze Systeme wiederhergestellt werden. Dabei ist die Bandbreite der Arten von Backups groß:

Von automatisierten, laufwerksinternen Backups oder der Speicherung der Daten auf anderen Netzwerkbereichen, über externe Speichermedien wie Festplatten oder USB-Sticks, bis hin zur Nutzung einer Cloud, sind die Möglichkeiten sehr vielfältig. Durch die Wiederherstellung der kritischen Daten und Systeme ist auch der Wiederanlauf des Geschäftsbetriebs möglich.

Orientierungshilfe: Achten Sie bei der Erstellung von Backups auf Regelmäßigkeit und Quantität, da Ransomware auch auf dem Backup installiert werden kann und dieses verschlüssen kann. Sorgen Sie daher dafür, dass möglichst viele vorhergehende Backups gespeichert werden. Achten Sie darauf, Ihre Kopien im Modus „Read only" zu speichern. So können Ihre Backups im Nachhinein nicht mehr verändert werden – auch durch Ransomware nicht.

	Was genau wurde gesichert?	Wo werden die Backups aufbewahrt?	Anmerkungen
Daten			
Ersatzsysteme			

3.10.2 Werden diese digital und räumlich getrennt von den üblichen Systemen aufbewahrt?
Aufgabe: Stellen Sie sicher, dass sämtliche Sicherungskopien entsprechend der 3-2-1-Regel aufbewahrt werden. Und hinterlegen Sie die Aufbewahrungsorte in der obigen Tabelle.

Hintergrund: Bei einem erfolgreichen Cyberangriff, sind Ihre Sicherungskopien ggf. auch von dem Angriff betroffen und wurden gelöscht/sind nicht verfügbar. Auch bei physischen Vorfällen wie einem Brand geht man auf diesem Weg sicher, dass nicht sämtliche Kopien verloren gehen.

Orientierungshilfe:
Am häufigsten wird die 3-2-1-Backup-Strategie empfohlen:
- Legen Sie drei Sicherheitskopien wichtiger Daten an.
- Speichern Sie diese auf zwei unterschiedlichen Medientypen (z. B. externe Festplatte, Cloud etc.)
- Bewahren Sie eine Kopie extern auf – also räumlich getrennt und nicht mit dem Netzwerk verbunden, so dass beispielsweise auch nach einem Brand noch eine Kopie unversehrt ist.

3.10.3 Werden diese regelmäßig auf Funktion, Aktualität und Vollständigkeit getestet?
Aufgabe: Überlegen Sie sich einen Rhythmus zur Prüfung der Ersatzsysteme und Sicherungskopien auf Funktion, Aktualität und Vollständigkeit. Setzen Sie sich sich eine Erinnerung und halten Sie den Rhythmus fest.

Hintergrund: Auch wenn Ersatzsysteme und Sicherungskopien existieren, sollten diese regelmäßig überprüft werden. Auf diese Weise wird sichergestellt, dass sich über die Zeit keine Konfigurationsfehler/Inaktualitäten eingeschlichen haben. So wird sichergestellt, dass diese im Notfall effektiv und einsatzbereit sind.

Orientierungshilfe:
Bei den Test-Zyklen von Ersatzsystemen und Sicherungskopien werden verschiedenen Orientierungspunkte genannt:
• Wie kritisch sind diese?
• Um welche Form des Ersatzsystems und der Sicherungskopien handelt es sich?
• Wie schnell sind diese nicht mehr aktuell?

So könnte solch ein Testplan aussehen:

	niedrig	mittel	kritisch	hoch kritisch
z. B. Ersatzsysteme	z. B. jährlich	z. B. halbjährlich	z. B. vierteljährlich	z. B. alle zwei Monate

3.10.4 Wer ist zuständig, um den Wiederanlauf zu koordinieren?

Aufgabe: Identifizieren Sie alle notwendigen Beteiligten, um den Wiederanlauf des Betriebs schnell und erfolgreich umzusetzen. Informieren Sie diese und stimmen Sie die Rollenverteilung ab. Dokumentieren Sie die Ergebnisse.

Hintergrund: Normalerweise sind für einen Wiederanlauf unterschiedliche Personen/Abteilungen notwendig, um diesen erfolgreich zu starten. Diese Personen sollten sich ihrer Rolle bewusst sein, um notwendige Vorkehrungen zu treffen und im Ernstfall schnellstmöglich reagieren zu können.

Orientierungshilfe:

Abteilung	Name	Kontakt (Tel. und E-Mail)	Rolle	Anmerkung z. B. Standort
IT				
Datenschutz + Rechtsabteilung				
Kommunika-tion/Presse				
Personal				
Geschäftsfüh-rung				
Produkt				
Kundenservice				
Operations				
Sonstige				

3.10.5 Wie ist der Prozess bei der Inbetriebnahme und Wiederherstellung?

Aufgabe: Überlegen Sie sich einen Prozess für den Wiederanlauf. Welche Schritte sind in welcher Reihenfolge vorzunehmen? Diskutieren Sie diesen mit den relevanten Beteiligten.

Hintergrund: Wenn Sie erst im Ernstfall notwendige Schritte und deren Priorität überlegen, verlieren Sie wertvolle Zeit, um den Schaden einzudämmen und schnellstmöglich zum Normalbetrieb zurückzukehren.

Orientierungshilfe:

Hinterlegen Sie hier eine Kurzbeschreibung des Prozesses und den Link für weitere Dokumente.

04 | Im Ernstfall: Umfangreicher Notfallplan für Notfallbeauftragte

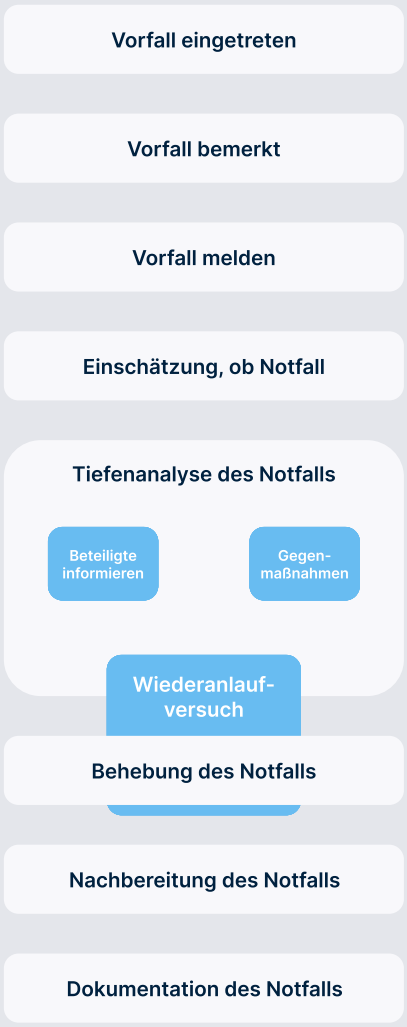
Notfallplan

Auch bei der besten Prävention und Vorsorge kann ein Vorfall nie ausgeschlossen werden. Da Sie für den Ernstfall vorbereitet sind, werden sich Ihre Vorbereitungen auszahlen. Erinnern Sie sich an die grundlegenden Verhaltensregeln, die identifizierten Prozesse und arbeiten Sie Ihren Notfallplan Schritt für Schritt ab:

A. Meine Verhaltensregeln

- Ruhe bewahren
- Notfallplan zur Hand nehmen
- Offene Kommunikation statt Schweigen
- Fokus auf Lösungen setzen, statt auf die Suche nach Schuldigen
- Dokumentieren, wo möglich
- Sonstiges

B. Allgemeinen Notfall-Prozess (ergänzen Sie ggf. um eigene Schritte)



C. Analyse der Meldung: Liegen Ihnen alle relevanten Informationen zum Vorfall vor?

Gehen Sie bestenfalls mit dem Erstmeldenden des Vorfalls alle Informationen auf Vollständigkeit und Verständnis durch:

a. Wer meldet den Vorfall?

- Vorname, Nachname
- Department und Position des Meldenden
- Kontaktdaten

b. Wann und unter welchen Umständen ist der Vorfall zuerst aufgetreten?

- Erstbeobachtende identisch mit Meldenden? (falls nein, Name und Kontakt)
- Wann zuerst beobachtet?
- Datum und Uhrzeit des Vorfalls

c. Was für ein Vorfall liegt vor?

- Verlust der Vertraulichkeit
- Beeinträchtigung
- Störung
- Ausfall

d. Wie ist der Vorfall zu beschreiben?

- Langsamer Computer
- Kein Zugriff auf das System/Daten oder Teile davon
- Manipulation von Mitarbeitenden, z. B. unautorisierte Zahlungsaufforderungen
- Erpressungsversuch: Es wird eine Forderung für Zugriff auf System oder Daten gestellt. Es wird eine Forderung für das Unterlassen einer Handlung z. B. Veröffentlichung von sensiblen Daten gestellt.
- Hinweise von anderen, dass verdächtige Nachrichten von der eigenen Unternehmensdomain versendet werden
- Weitergeleitete Suche
- Daten im Internet
- Verdächtige Aktivitäten

e. Welche und wie viele Geräte, Programme und/oder Systeme sind betroffen?

f. Sind Daten betroffen? Wenn ja, welche? Wurden sie eingesehen, kopiert oder gelöscht?

g. Wie kritisch erscheint der Vorfall?

h. Was wurde kurz vor dem Vorfall gemacht?

i. Welche Auswirkungen hat der Vorfall auf den Betrieb?

D. Erste Beurteilung des Vorfalls: Liegt ein Notfall vor und wie kritisch ist dieser?

Gehen Sie die Informationen der Meldung des Vorfalls Schritt für Schritt durch und versuchen Sie zu ergründen, ob ein Notfall vorliegt, wie kritisch dieser für Ihr Unternehmen ist und was die notwendigen nächsten Schritte sind. Achten Sie darauf, dass Ihnen alle relevanten Informationen zum Vorfallsgeschehen vorliegen. Ihre Vorbereitungen dienen als Orientierungshilfen.

1.Welche Art von Vorfall wurde Ihnen gemeldet?

- ☐ Störung
- ☐ Exposition
- ☐ Ausfall
- ☐ Sabotage
- ☐ Löschung

2. Welche Systeme und/oder Daten sind betroffen und befinden sich kritische darunter? (Verfügbarkeit / Vertraulichkeit / Integrität)

Liste mit kritischen Systemen

System + Software	Betroffene Daten	Verlust Vertraulichkeit Auswirkung	Max. tolerierbare Ausfallzeit	Ausfall Auswirkung	Sabotage Auswirkung	Notizen: Abhängigkeiten mit anderen Systemen
Betriebssystem						
Server						
Telekommunikation						
E-Mail-Programm						
Kalender						
Design-Software						
E-Mail-Marketing-Tool						
HR-Tool						
Sonstige						

Liste mit kritischen Daten

Daten	Daten-klassifizierung	Auswirkungen	Anmerkungen
Daten der Mitarbeitenden			
Betriebs-geheimnisse			
Kontaktdaten Partner			
Kontaktdaten Kundschaft			
Sonstige			

3. Welche Gefahren bestehen durch den Notfall?

- Finanzieller Schaden
- Beeinträchtigung des Geschäftsbetriebs
- Verstoß gegen rechtliche Vorgaben z. B. DSGVO
- Verletzung von Vorschriften und Verträgen
- Negative Innen- und Außenwirkung (Reputationsschaden)
- Personenschaden
- Sonstiges:

4. Liegt ein Notfall vor?

☐ Ja
☐ Nein

5. Wie bewerte ich den Notfall?

- HOCH KRITISCH: Reaktion innerhalb von Stunde(n) einleiten, z. B. 1 Stunde.
- KRITISCH: Reaktion innerhalb von Stunde(n) einleiten, z. B. bis 2 Stunden.
- WENIG KRITISCH: Reaktion innerhalb von Stunde(n) einleiten, z. B. 24 Stunden.
- UNKRITISCH: Reaktion innerhalb von Stunde(n) einleiten, z. B. 72 Stunden.

E. Was kann die Ursache für diesen Notfall sein?

Verdacht	Ursache
☐	**Falsche Systemkonfiguration**
☐	**Unbeabsichtigte Informationspreisgabe durch Mitarbeitende, z. B. Fotos auf Social Media, falsche Software-Konfiguration**
☐	**Fehlende System-/Software-Updates**
☐	**Denial-of-Service-Angriff**
☐	**Physischer Vandalismus**
☐	**Mängel Passwort- bzw. Zugangssicherheit**
☐	**Phishing**
☐	**Weiteres Social Engineering**
☐	**Erpressung mittels Ransomware**
☐	**Elementarereignis (z. B. Sturm, Stromausfall…)**
☐	**Sonstiges Fehlverhalten von Mitarbeitenden**
☐	**Sonstige Virus-/Malware-Infektion**
☐	**Sonstiges Zufallsereignis**
☐	**Sonstiges**

F. Welche ersten Maßnahmen könnten zur Behebung des Vorfalls getroffen werden?

a. E-Mail: Auf infizierten Link oder Anhang geklickt > Vorfall

- **SOFORT:** PC vom Netzwerk trennen (LAN-Kabel ziehen)/evtl. direkt herunterfahren
- **SOFORT:** Notfallbeauftragte und Vertretung informieren > diese übernehmen die weitere Bearbeitung und Meldekette
- **Weitere Schritte**
  - IT-Verantwortliche/Dienstleister informieren
  - Weitere Schritte nach telefonischer Absprache
  - Information an Geschäftsführung
  - Mögliche Datenschutzverletzung prüfen

b. E-Mail: Betrügerische Nachrichten von vermeintlichen Kunden/Partnern/Kollegen:

- **SOFORT:** In keiner Form antworten
- **SOFORT:** Notfallbeauftragte und Vertretung informieren > diese übernehmen die weitere Bearbeitung und Meldekette
- **Weitere Schritte** (durch Notfallbeauftragte, wenn nicht erreichbar selbstständig):
  - IT-Verantwortliche/-Dienstleister informieren

- Weitere Schritte nach telefonischer Absprache
- Betreffende Personen telefonisch informieren, damit diese ihre Systeme prüfen können. (Nicht Tel.-Nummer aus Mail nehmen, sondern aus verifizierbarer Mail/früherem Kontakt/offizieller Website)
- Information an Geschäftsführung und interne Kommunikation, so dass Kolleginnen und Kollegen ebenfalls gewarnt werden können.
- Anzeige bei der Polizei
- Mögliche Datenschutzverletzung prüfen

c. Cyber-Erpressung: Information an Geschäftsführung

- **SOFORT:** In keiner Form antworten
- **SOFORT:** Notfallbeauftragte und Vertretung informieren > diese übernehmen die weitere Bearbeitung und Meldekette
- **Weitere Schritte** (durch Notfallbeauftragte, wenn nicht erreichbar selbstständig):
  - IT-Verantwortliche/-Dienstleister informieren
  - Geschäftsführung informieren
  - Anzeige bei der Polizei
  - Mögliche Datenschutzverletzung prüfen

d. Offenlegung vertraulicher Daten

- **SOFORT:** Wenn möglich, unbefugten Zugriff auf sämtliche Daten unterbinden oder veröffentlichte Daten löschen
- **SOFORT:** Notfallbeauftragte und Vertretung informieren > diese übernehmen die weitere Bearbeitung und Meldekette
- **Weitere Schritte** (durch Notfallbeauftragte, wenn nicht erreichbar selbstständig):
  - IT-Verantwortliche/-Dienstleister informieren
  - Geschäftsführung informieren
  - Mögliche Datenschutzverletzung prüfen und entsprechend handeln

G. Welche Beteiligten sollten informiert und als Unterstützung ins Boot geholt werden?

Interne Beteiligte

Abteilung	Name	Kontakt (Tel. und E-Mail)	Rolle	Anmerkung z. B. Standort
IT				
Datenschutz + Rechtsabteilung				
Kommunikation/Presse				
Personal				
Geschäftsführung				

Abteilung	Name	Kontakt (Tel. und E-Mail)	Rolle	Anmerkung z. B. Standort
Produkt				
Kundenservice				
Operations				
Sonstige				

Externe Beteiligte

Dokumentieren Sie Einzelheiten des Vertrags, seine Abdeckung, wie sie Ihnen helfen können und zu welchem Zeitpunkt Sie mit ihnen in Kontakt treten müssen.

	Name (Firma und Ansprech-partner)	Kontakt (Tel. und E-Mail)	Vertrags-/ Kunden-nummer	Anmerkung
Externer IT-Dienstleister				
Incident Res-ponse-Anbieter	Perseus Technologies GmbH			24/7 erreichbar
Telekommuni-kationsanbieter				
Cyber-versicherung	HDI	+49 511/3031 7000		Cyberver-sicherung umgehend informieren
Polizei				
Feuerwehr				
Datenschutz-aufsichtsbehör-de (siehe Liste im Anhang)				
Bundesamt für Sicherheit in der Informations-technik				
Wichtige Partner				

	Name (Firma und Ansprech-partner)	Kontakt (Tel. und E-Mail)	Vertrags-/ Kunden-nummer	Anmerkung
Wichtige Kundschaft				
Cloud-Service-Anbieter				
Stromanbieter				
Wasser-versorger				
Sonstige				

H. Welche ersten Maßnahmen könnten zum Wiederanlauf initiiert werden?

Prüfung des Wiederanlaufsplans/-prozesses

Kurzbeschreibung des Prozesses und den Link für weitere Dokumente

Abstimmung mit Zuständigen, um den Wiederanlauf zu koordinieren

Abteilung	Name	Kontakt (Tel. und E-Mail)	Rolle	Anmerkung z. B. Standort
IT				
Datenschutz + Rechtsabteilung				
Kommunika-tion/Presse				
Personal				
Geschäftsfüh-rung				

Abteilung	Name	Kontakt (Tel. und E-Mail)	Rolle	Anmerkung z. B. Standort
Produkt				
Kundenservice				
Operations				
Sonstige				

Inbetriebnahme von Ersatzgeräten und Wiederherstellung von relevanten Daten und Systemen mit Hilfe von Sicherungskopien

	Was genau wurde gesichert?	Wo werden die Backups aufbewahrt?	Anmerkungen
Daten			
Ersatzsysteme			

I. Wie kann ich den Vorfall nachbereiten? (inkl. Dokumentationspflichten)

Aufgabe: Überlegen Sie für sich und mit sämtlichen Beteiligten, wie es zu dem Notfall kam und ob Sie mit dem Ablauf seiner Behebung zufrieden waren. Dokumentieren Sie Ihre Ergebnisse. Beachten Sie, dass es zwar darum geht, die Ursache zu ergründen, zukünftig Notfälle zu vermeiden bzw. effektiver zu beheben. Es geht aber nicht darum, die Fehler einzelner Personen hervorzuheben.

Hintergrund: Aus jedem Notfall können Sie für den nächsten Ernstfall lernen. Dafür ist es jedoch wichtig, das gesamte Geschehen aus allen Perspektiven zu bewerten. Damit dieses Wissen nicht verloren geht und gemeinsame Entscheidungen für die Zukunft festgehalten werden.

Orientierungshilfe:
Folgende Punkte könnten Sie in Ihrer Nachbereitung diskutieren:

1. Bewertung der Vorfall-Ursache
- Was war das Einstiegstor für den Notfall?
- Welches Gefahrenpotential bestand?

- Hätte man den Vorfall einfach vermeiden können?
- Waren Probleme im Vorfeld bekannt?
- Gibt es sonstigen Verbesserungsbedarf?

2. Bewertung der Behebung der Ursache
- Wurde die Ursache schnell identifiziert?
- Konnte der Notfall innerhalb der vorgegebenen Reaktionszeit gelöst werden? Falls nein, warum nicht?
- Wurden die Auswirkungen des Notfalls richtig eingeschätzt?
- Wurden die richtigen Maßnahmen getroffen?
- Hätte man weitere Maßnahmen treffen können?
- Gibt es sonstigen Verbesserungsbedarf?

3. Bewertung der Sicherung/Wiederherstellung des Geschäftsbetriebs
- Konnte auf notwendige Ersatzsysteme problemlos zugegriffen werden?
- Waren notwendige Ersatzsysteme funktionsfähig?
- Wie gut funktionierte der Zugriff auf Sicherheitskopien und Backup-Systeme?
- Reibungsloser Ablauf?
- Gibt es sonstigen Verbesserungsbedarf?

4. Bewertung des Kommunikationsprozesses
- Waren alle Beteiligten erreichbar?
- Haben sie schnell genug reagiert?
- Hat der Meldeprozess funktioniert?
- Welche Lücken gab es im Melde- und Kommunikationsprozess?
- Wurde die vorliegende Dokumentation zum Notfallprozess genutzt?
- Gibt es sonstigen Verbesserungsbedarf?

5. Bewertung der Zusammenarbeit mit externen Beteiligten
- Waren alle betroffenen externen Beteiligte erreichbar?
- Waren alle betroffenen externen Beteiligte hilfreich?
- Gibt es sonstigen Verbesserungsbedarf?

6. Schaden
- Welcher Schaden ist entstanden?
- Konnten weitere Schäden vermieden werden?
- Gibt es sonstigen Verbesserungsbedarf?

7. Dokumentation

05 | Wie gewährleiste ich, dass der Plan aktuell bleibt?

Aufgabe: Überlegen Sie sich Möglichkeiten, den Plan regelmäßig zu aktualisieren und ggf. Betroffene über die Änderungen zu informieren.

Hintergrund: Damit Ihr Notfallplan größtmögliche Effektivität gewährleistet, ist es notwendig, diesen aktuell zu halten und alle Beteiligten über Änderungen zu informieren.

Orientierungshilfe:
Folgende Maßnahmen können Sie umsetzen:

- Führen Sie regelmäßige Übungen durch und damit verbundene Audits, deren Ergebnisse in die Verbesserung des Plans einfließen.
- Halten sie regelmäßig Rücksprache mit allen Beteiligten.
- Regelmäßige Aufnahme des Ist-Zustandes aller relevanten Daten und Systeme sowie der getroffenen Sicherheits- und Wiederherstellungsmaßnahmen.
- Tragen Sie sich eine Erinnerung für eine regelmäßige Überarbeitung des Plans in Ihren Kalender ein.

Datum	Version	Autor	Abteilung

Anhang

1. Die Datenschutzaufsichtsbehörden der Bundesländer

In den meisten Fällen gilt: Zuständig ist die Datenschutzaufsichtsbehörde des Bundeslandes, in dem sich der Hauptsitz Ihres Unternehmens befindet. In den meisten Fällen gilt: Zuständig ist die Datenschutzaufsichtsbehörde des Bundeslandes, in dem sich der Hauptsitz Ihres Unternehmens befindet.

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit **Baden-Württemberg**	**0711 / 615541 - 0** www.baden-wuerttemberg.datenschutz.de
Landesamt für Datenschutzaufsicht **Bayern**	**09 81/18 00 93 – 0** www.lda.bayern.de
Berliner Beauftragte für Datenschutz und Informationsfreiheit	**030 / 13889 - 0** www.datenschutz-berlin.de
Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht **Brandenburg**	**033203 / 356 - 0** www.lda.brandenburg.de
Die Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt **Bremen**	**0421 / 361-2010** www.datenschutz-bremen.de
Der **Hamburgische** Beauftragte für Datenschutz und Informationsfreiheit	**040 /4 2854 - 4040** www.datenschutz-hamburg.de
Der **Hessische** Beauftragte für Datenschutz und Informationsfreiheit	**0611 / 1408 - 0** www.datenschutz.hessen.de
Der Landesbeauftragte für Datenschutz und Informationsfreiheit **Mecklenburg-Vorpommern**	**0385 / 59494 - 0** www.datenschutz-mv.de
Die Landesbeauftragte für den Datenschutz **Niedersachsen**	**0511 / 120 - 4500** www.lfd.niedersachsen.de
Landesbeauftragte für Datenschutz und Informationsfreiheit **Nordrhein-Westfalen**	**0211 / 38424 - 0** www.ldi.nrw.de
Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit **Rheinland-Pfalz**	**06131 / 8920 - 0** www.datenschutz.rlp.de
Unabhängiges Datenschutzzentrum **Saarland**	**0681 / 94781 - 0** www.datenschutz.saarland.de
Sächsischer Datenschutzbeauftragte	**0351 / 85471 - 101** www.datenschutz.sachsen.de
Landesbeauftragter für den Datenschutz **Sachsen-Anhalt**	**0391 / 81803 - 0** www.datenschutz.sachsen-anhalt.de
Unabhängiges Landeszentrum für Datenschutz **Schleswig-Holstein**	**0431 / 988 - 12 00** www.datenschutzzentrum.de
Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit	**0361 / 573 1129 - 00** www.tlfdi.de

Anhang

2. Liste mit allen bundesweiten Ansprechpartnern der Polizei

Bundeskriminalamt	0611 55-15037 | zac@cyber.bka.de
Baden-Württemberg	0711 5401-2444 | cybercrime@polizei.bwl.de
Bayern	089 1212-3300 | zac@polizei.bayern.de
Berlin	030 4664-924924 | zac@polizei.berlin.de
Brandenburg	03334 388-8686 | zac@polizei.brandenburg.de
Bremen	0421 362-19820 | cybercrime@polizei.bremen.de
Hamburg	040 4286-75455 | zac@polizei.hamburg.de
Hessen	0611 83-8377 | zac.hlka@polizei.hessen.de
M-V	03866 64-4545 | cybercrime.lka@polmv.de
Niedersachsen	0511 26262-3804 | zac@lka.polizei.niedersachsen.de
Nordrhein-Westfalen	0211 939-4040 | cybercrime.lka@polizei.nrw.de
Rheinland-Pfalz	06131 65-2565 | lka.cybercrime@polizei.rlp.de
Saarland	0681 962-2448 | cybercrime@polizei.slpol.de
Sachsen	0351 855 - 3226 | zac.lka@polizei.sachsen.de
Sachsen-Anhalt	0391 250-2244 | zac.lka@polizei.sachsen-anhalt.de
Schleswig-Holstein	0431 160-42727 | cybercrime@polizei.landsh.de
Thüringen	0361 57431-4545 | cybercrime.lka@polizei.thueringen.de

Quellen

- Unsere tägliche Erfahrung
- Bundesamt für Sicherheit in der Informationstechnik (2008): BSI-Standard 100-4: Notfallmanagement
- Allianz für Cybersicherheit zum Notfallmanagement (Stand: 2022): Informationen zum Notfallmanagement, https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Unternehmen-allgemein/IT-Notfallkarte/it-notfallkarte_node.html
- Britisches National Cyber Security Centre (2020): Cyber Security Response and Recovery. How to prepare for a cyber incident, from response through to recovery
- US-amerikanische National Institute of Standards and Technology (2012): Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technology

Impressum

Perseus Technologies GmbH | Hardenbergstraße 32 | 10623 Berlin
Telefon: +49 (30) 959998080 | E-Mail: info@perseus.de
Geschäftsführer: Kevin Püster

Handelsregister: Amtsgericht Charlottenburg HRB 180356 B
USt.-Ident-Nr.: DE308271739
Verantwortlicher gem. § 55 Abs. 2 RStV: Kevin Püster

An wen können Sie sich im Notfall wenden?
Unsere Notfallhilfe steht Perseus-Kunden je nach Vertrag in Verdachtsfällen zur Seite. Einfach einloggen und uns kontaktieren:
https://www.perseus.de/produkt/notfallhilfe/

Für Nicht-Kunden ist diese Notfall-Nummer rund um die Uhr erreichbar:
+49 30 233 2730 95