Muster IT-Notfallplan

Version	Datum	Bearbeiter	Änderungen	Vertraulichkeitsstatus
0….	10.10.2023	N.N.	Erstversion	• Vertraulich • Begleitende Dokumente, siehe jeweiliges Dokument

Rechtliche Hinweise zur Benutzung:

Bitte beachten Sie für die Verwendung des hier bereit gestellten Musters Folgendes:

- Das Muster wurde mit größter Sorgfalt erstellt, erhebt aber keinen Anspruch auf Vollständigkeit und Richtigkeit.
- Das Muster ist als Formulierungshilfen zu verstehen und soll nur eine Anregung bieten, wie die eigene Aktivität zur IT-Sicherheit sachgerecht gestaltet werden kann. Dies entbindet Sie jedoch nicht von der sorgfältigen eigenverantwortlichen Prüfung.
- Das Muster ist nur ein Vorschlag für eine mögliche Gestaltung. Sie können auch andere Formulierungen wählen. Vor einer Übernahme des unveränderten Inhaltes muss daher im eigenen Interesse genau überlegt werden, ob und in welchen Teilen gegebenenfalls eine Anpassung an die konkret zu gestaltende Situation erforderlich ist.
- Auf diesen Vorgang hat die Industrie- und Handelskammer keinen Einfluss und kann daher naturgemäß für die Auswirkungen auf keine Haftung übernehmen. Auch die Haftung für leichte Fahrlässigkeit ist grundsätzlich ausgeschlossen.

Um das Muster weiter zu verbessern sind wir für Anmerkungen und Verbesserungsvorschläge sehr dankbar. Bitte schicken Sie diese an Bernhard Kux, kux@muenchen.ihk.de

Muster eines IT-Notfallplanes:

In diesem Dokument wird, aus Gründen der besseren Lesbarkeit, ausschließlich das generische Maskulinum verwendet. Es bezieht sich auf Personen aller Geschlechter.

Zusätzlich zu diesem Dokument sind weitere Dokumente Teil des IT-Notfallplanes. Siehe hierzu „Dokumentenliste IT-Notfallplan“.
Insbesondere:

- IT-Notfallunterlagen:
  - Anwender-Notfallpläne: IT-Notfall aus Sicht der anwendenden Fachabteilung
  - Technische Notfallpläne: Übersicht über technische IT-Notfallsicht, i .d. R. mit Verweis auf Detaildokumentationen an anderer Stell
  - IT-Notfallsteckbriefe für einzelne Anwendungen

- Ergänzende-Dokumente: Regelmäßig zu aktualisierende Unterlagen
  - Interne Infos (Telefonlisten, Organigramme…)
  - Externe Infos (z. B. BSI-APT-Dienstleisterliste, Cyberversicherung…)

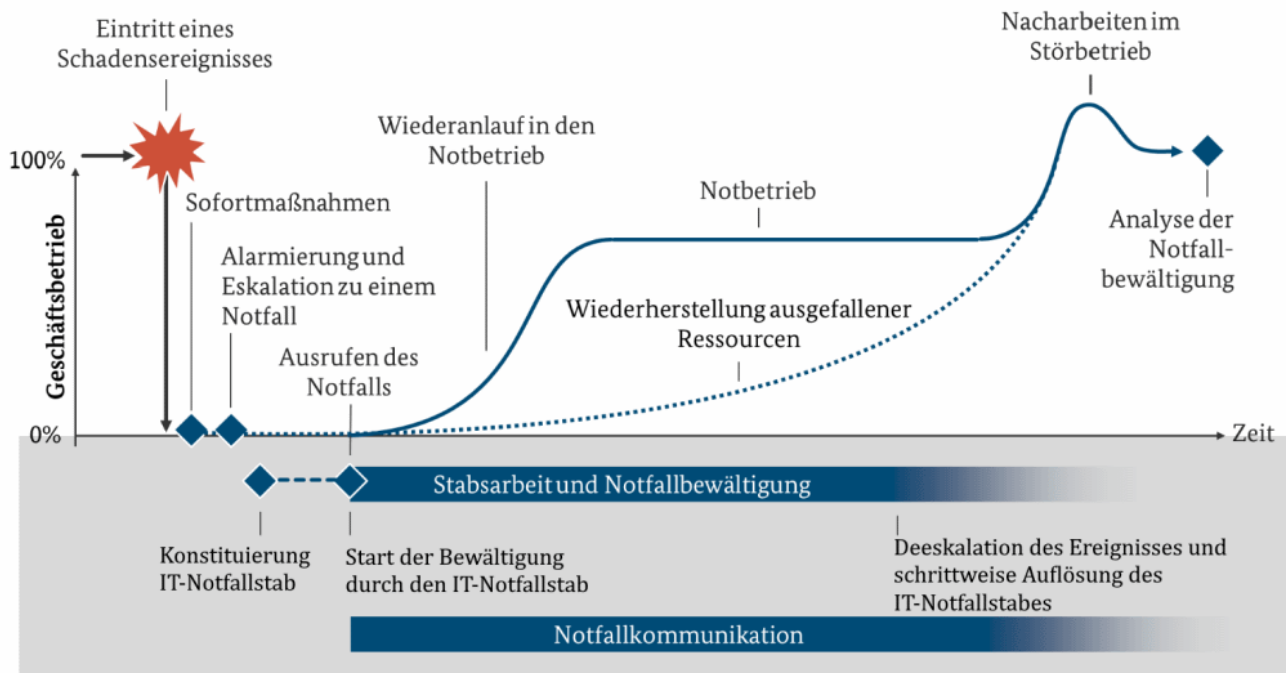
Inhalt

1 IT-Notfallplan: Ziel, Zuständigkeiten und Aktualität

Der IT-Notfallplan ist ein Werkzeug zur Reaktion auf außergewöhnliche Ereignisse in der IT, die zum Ausfall von insbesondere kritischen Geschäftsprozessen führen. Ziel ist die Aufrechterhaltung der Handlungsfähigkeit und die Wiederherstellung der IT-Prozesse.
Der IT-Notfallplan regelt die Vorgehensweise im Notfall, wenn IT oder IT-gesteuerte Prozesse betroffen sind.
Der IT-Sicherheitsbeauftragte kümmert sich um die Aktualität und Anwendbarkeit des IT-Notfallplanes. Alle Mitarbeiter tragen aktiv dazu bei und melden insbesondere proaktiv Aktualisierungen und benötigte Informationen.

2 IT-Notfall: Kurzübersicht

Ein Notfall ist dann gegeben, wenn eine Störung nicht mehr im Rahmen des Normalbetriebs bewältigt werden kann.



Quelle: BSI 200-4

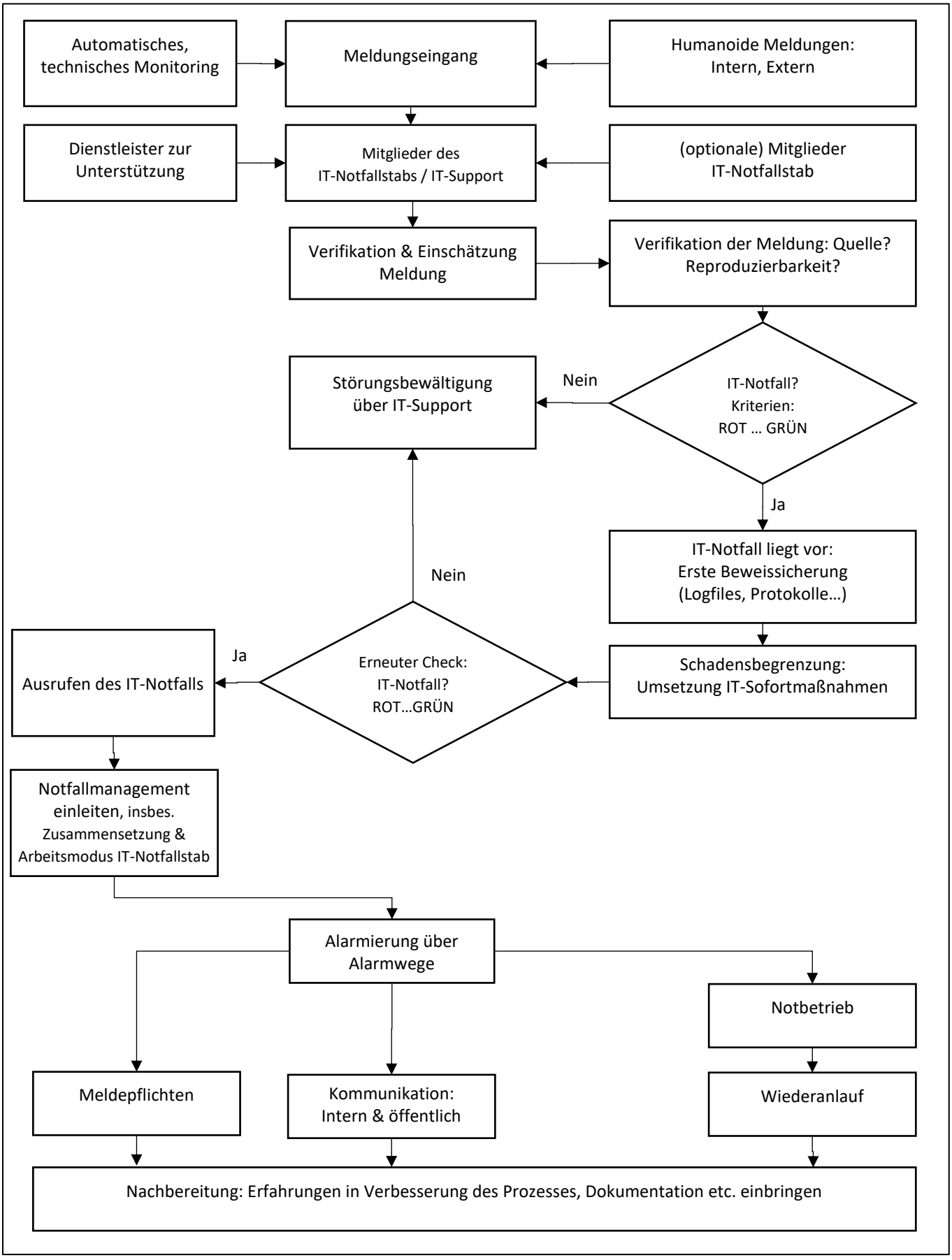
Der IT-Notfallplan enthält folgende Abschnitte:

1. Erkennen und Melden von potenziellen IT-Notfällen
2. Verifikation und Einschätzung der Meldung
3. IT-Sofortmaßnahmen
4. Ausrufen des Notfalls
5. Notfallmanagement durch den IT-Notfallstab: Meldepflichten, Dokumentation, Kommunikation
6. Wiederanlauf zum Notbetrieb, Wiederherstellung zum Normalbetrieb
7. Nachbereitung: Review des Notfalls

Darüber hinaus enthält der IT-Notfallplan eine Sammlung von Informationen, die in einem IT-Notfall hilfreich sind.

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

Vom Meldungseingang über die Einordnung und IT-Notfallmodus zur Nachbereitung (in Anlehnung BSI 200-4)



3 Melden, Erkennen, Verifizieren & Einschätzen von IT-Notfällen

Informationen über potenzielle Notfälle können aus internen und externen Quellen kommen, sowie vollautomatisch aus Monitoringsystemen oder durch Menschen. Meldungen werden eingeschätzt und ggf. Maßnahmen ergriffen.

3.1 Meldewege für potenzielle IT-Notfälle

3.1.1 Empfänger einer Meldung eines potenziellen IT-Notfalles

- Interne wie externe Meldequellen müssen mindestens ein Mitglied des IT-Notfallstabes erreichen. Die Erreichbarkeit mindestens eines Mitglieds des IT-Notfallstabes ist zu organisieren.
  - Innerhalb büroüblicher Arbeitszeiten:
    Im Internet sind die Kontaktdaten des IT-Notfallstabes veröffentlicht. Die Mitarbeiter sind über den internen Meldeweg informiert.
  - Außerhalb (Nachts, Wochenende, Feiertage): Fact24-Notfallbenachrichtigungen, siehe folgender Abschnitt
- Eine eintreffende IT-Notfallmeldung wird ggf. verifiziert, bewertet und ggf. weitere Maßnahmen initiiert.
  Oft wird die zu veranlassende Maßnahme an Dritte (z. B. Admins) weitergegeben, welche die operative Durchführung vollziehen.

3.1.2 Interne Meldewege und -quellen: Direkte Kontaktierung des IT-Notfallstabes

- Internes Monitoring:
  - [im oder für das Unternehmen ggf. eingesetzte Anwendungen zum Monitoring der Verfügbarkeit, Vertraulichkeit, Integrität]
    Im Fehlerfall erhalten Mitarbeiter (z. b. Product Owner) per [Mail/SMS/…] eine Benachrichtigung: Siehe Rolle „Alarmempfänger“ im Anhang Kontaktdaten.
- Product Owner (=Generalkümmerer) der jeweiligen IT-Anwendung (siehe Anhang Kontaktdaten)
  [Ggf.: Meldung über Ticketsystem, bei dringenden Fällen direkt an Dienstleister / IT-Admins Backend]
- [Ggf.: Über die Rufnummer …. können Mitarbeiter den IT-Notfallstab (Rolle fact24-Kontakt) erreichen].
- Mitarbeiter, die als Anwender von Anwendungen, über Dienstleister-Kontakte etc. auf ggf. vorhandene IT-Notfälle aufmerksam werden, können über ein IT-Ticketsystem Störungen, Datenschutzvorfälle und IT-Notfälle melden. Dabei können Sie die „Dringlichkeit aus Sicht des Nutzers“ sowie „Priorisierung ist mit „niedrig“ / „normal“ / „hoch“ angeben.
- Facility Management: Ausfall der Versorgung, Brände, Wasserschäden, Internet-Anbindung in Unternehmens-Gebäuden.

3.1.3 Externe Meldewege und -quellen

Kontaktierung von Mitarbeitern, die extern eingehende Meldungen in die passenden internen Meldewege kanalisieren.

- Bekannte Dienstleister:
  I.d.R. haben unsere Dienstleister Kollegen als Ansprechpartner → Interne Meldewege s. o.
- Externes Security Operations Center: Z. B. führt ein Dienstleister regelmäßig Schwachstellen- Scan für Websites durch.

- Externe Anwender von Anwendungen, BugBounty-Hacker:
  Über öffentlich zugängliche Mailadressen / Kontaktadressen → Interne Meldewege s. o.

3.1.4 Für Meldungen eingesetzte IKT

- Telefon-Notfallsystem mit Notfall-Rufnummer:
  - Infoblatt für Melder
  - Prozessbeschreibung
- Mail
- Festnetz-Telefon
- Mobilfunk (Sprache, SMS, Messenger) → siehe Anhang Kontaktdaten

3.2 Verifikation und erste Analyse der Meldung

3.2.1 Meldung verständlich und komplett?

Eine Notfallmeldung sollte folgende Mindestinformationen enthalten.

- Wer meldet?
- Kontaktinfos, z. B. für Rückruf
- Mit welchem IT-System wurde wie gearbeitet?
- Welches IT-System ist betroffen?
- Was haben Sie wann beobachtet?
- Wo befindet sich das betroffene IT-System? (Gebäude, Raum…)

Ggf. Rückfrage beim Melder:

- Fehlen Informationen bei der Meldung?
- Das in der Meldung geschilderte Problem ist nicht verständlich und kann nicht nachvollzogen werden.

3.2.2 Welche IKT-Ebene betrifft die Meldung?

Auf die IKT bezogen, hilft für die systematische Einordnung eingehender Meldungen ggf. das OSI-Schichtenmodell:
Geht man von Layer 1 bis 8 durch, kann das Problem oft eingegrenzt werden - bzw. Ursachen ausgeschlossen oder identifiziert werden.
Oft liegen **Meldungen zu Betriebsstörungen** auf der Anwendungsschicht oder im „Layer 8“ vor. Allerdings ist die grundsätzliche Annahme eines „Layer 8“-Problems oft nicht zielführend und beeinträchtigt die gemeinsame Suche nach Lösungen.
Gravierende IT-Notfälle sind zumeist in tiefer liegenden OSI-Schichten zu vermuten.

Layer-No	Layerbezeichnung	IKT	Beispielhafte Fehlerquellen
1	Physikalische Übertragung (Physical Layer)	Hardware: Netzverkabelung u. ä.	Hardwaredefekt, Verkabelung nicht vorhanden
2	Sicherungsschicht / Verbindungsebene (Data Link Layer)	Hardware: Bridges, Switches u. ä.	Hardwaredefekt
3	Vermittlungsschicht (Network Layer)	Hardware: Router u. ä. Protokolle: IP, ICMP u. ä.	Hardwaredefekt, Gesperrte Protokollverbindungen (IPs …)
4	Transportschicht (Transport Layer)	Sicherstellung der fehlerfreien Übertragung, Protokolle: TCP, UDP mit Ports u. ä.	Gesperrte Protokollverbindungen (Ports …)
5	Sitzungsschicht (Session Layer)	Software: Prozesskommunikation zwischen Systemen, Protokolle: RPC u. ä.	Gesperrte Protokollverbindungen, Fehler bei einem oder mehreren Systemen
6	Darstellungsschicht (Presentation Layer)	Software: Systemunabhängige Datendarstellung, Normen: Datenkompression, Verschlüsselung, ASCII, EBCDIC u. ä.	Unklare Datenformate, invalidierte Daten
7	Anwendungsschicht (Application Layer)	Software: Daten-Ein- und Ausgabe Anwendungen: Mailprogramme, Browser, Apps u. ä.	Admin-Konfigurationsfehler
8	Humanoide oder maschinelle Nutzer	Anwender: Relevanz bzw. IT-Sicherheit: Social Engineering, Programme zur Steigerung der IT-Sicherheits-Awareness	Bedienungsfehler, Fehlkonfigurationen

3.2.3 IT-Basisinfrastruktur: Wesentliche IT-Bereiche

Grundsätzliche Beschreibung der vom Unternehmen genutzten IT-Basisinfrastruktur: Ein IT-Notfall einer dieser IT-Basisinfrastruktur-Bereiche zieht unmittelbar die den IT-Notfall der darauf laufenden IT-Anwendungen nach sich. In Anhang „Notfallszenarien“ sind Ausfall- und IT-Notfallszenerien beschreiben.
Die Bereiche der Unternehmens IT-Basisinfrastruktur:

1. Cloud-Dienstleister / Cloud-Rechenzentrum für eigene Anwendungen
2. Rechenzentrum für (Co-)Hosting eigener Anwendungen
3. Rechenzentrum für Anwendungen bei zentralem IT-Dienstleister
4. Microsoft M365-Cloud
5. Externe Anwendungen, die unabhängig von der Unternehmens-Infrastruktur laufen. In Einzelfällen sind diese an Unternehmens-Berechtigungssysteme (LDAP, ActiveDirectory…) angeschlossen.
   Bei nicht an das Unternehmens-Berechtigungssysteme angebundenen Anwendungen werden Zugänge

& Mitarbeiter separat zur Information hinterlegt.
Beispiele:
- Reisebuchungssysteme z. B. bahn.de etc. (keine ActiveDirectory / LDAP-Anbindung)

3.2.4 Welche Orte sind betroffen?

Das Unternehmen setzt IKT an folgenden Orten ein. Welche sind betroffen?
Standortübersicht: www….

Standort. Kontakt	Standortfunktion	IT-Komponenten (IT-Relevanz, ggf. Hardware, Verkabelung…)
„Standort A" Adresse Kontaktdaten: Telefon, Mail…	Unternehmensstandort Kundenstandort: Weitere Firmen z. b. des Unternehmensverbundes	Produktionsstandort, Verwahrung von Backup-Tapes
„Standort B" Adresse Kontaktdaten: Telefon, Mail…	Unternehmensstandort	Bürostandort IT, Backup2Tapemaschine, Anwenderinfrastruktur (Arbeitsplätze, Drucker, Scanner…)
„Standort C" Adresse Kontaktdaten: Telefon, Mail…	Kundenstandort	Anwenderinfrastruktur (Arbeitsplätze, Drucker, Scanner…)
Mobiles Arbeiten	Mobiles Arbeiten im gesamten EU-Bereich (Homeoffice, ÖPNV, Coworking…). Kontakte ggf. über Personalabteilung	I.d.R. Nutzung privater / vom Unternehmen gestellter Hardware

3.3 Einschätzung der Meldung: Kriterien eines IT-Notfalls

3.3.1 Grundsätzliches zu „Betriebsstörung oder IT-Notfall?"

Unmittelbar nach einer Meldung ist oft nicht einschätzbar, ob es sich um eine „normale" Betriebsstörung oder um einen IT-Notfall handelt:

- Wird die Meldung als Betriebsstörung eingeschätzt, geht man davon aus, dass das Problem mit unmittelbar zur Verfügung stehenden Ressourcen schnell gelöst bzw. in den Griff bekommen werden kann.

- Wurde in einer unklaren Situation noch kein Notfall ausgerufen, so sind die zu alarmierenden Personen trotzdem vorzuwarnen, insbesondere rechtzeitig vor Feierabend, Wochenenden, Betriebsferien.
- Deutet die Einschätzung bzw. Ressourcen und Geschwindigkeit auf größere Probleme hin, muss auf die Behandlung als IT-Notfall geprüft werden. Mit diesem werden weitere Ressourcen aktiviert.
- 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 aufgrund der in einem Moment vorliegenden Anhaltspunkte ein IT-Notfall ausgerufen und es stellt sich später heraus, dass kein IT-Notfall („nur“ Betriebsstörung) vorliegt, so hat das für den ausrufenden Personen keine Folgen (Ausnahme: vorsätzliche Falschalarmierung).
- Wurde eine Meldung als Betriebsstörung eingeschätzt und stellt sich diese später als IT-Notfall heraus: Es ist zu prüfen, wie die Kriterien für die Einstufung verbessert werden können.

3.3.2 Hinzuziehen des IT-Supports sowie der fachlich bzw. technisch zuständigen Mitarbeiter

Bei der Einschätzung der Meldung können die fachlichen und technischen Verantwortlichen der betroffenen IKT mit einbezogen werden. Ein Kennzeichen eines IT-Notfalles ist es, dass der IT-Support die Fragestellungen nicht mehr mit den üblichen Supportlösungen lösen kann.

IKT-Anwendungen, die dem IT-Support zur Bearbeitung von Betriebsstörungen übergeben wurden sind in den organisatorisch-technischen Infopools des IT-Supports zu finden (z. B. Wiki, Jira…)

Daneben gibt es IKT-Anwendungen, die nicht an den Betrieb übergeben wurden. In diesen Fällen sind die jeweiligen fachlichen und technischen Ansprechpartner Anwendungsbezogen zu ermitteln. Beispiel: Unternehmens-SocialMedia-Kanäle wie LinkedIn, facebook etc..

3.3.3 Situationsanalyse: Verfügbarkeit, Vertraulichkeit, Integrität

Meldungen werden nach den drei Kriterien der IT-Sicherheit Verfügbarkeit, Vertraulichkeit und Integrität begutachtet.
Je nachdem wie der mögliche Schaden ausfallen kann (oder wie dies vermutet wird), sind geeignete Maßnahmen zu ergreifen.

- **Verfügbarkeit:**
  Es kann einen IT-Notfall darstellen, wenn absehbar ist, dass die Verfügbarkeit einer IT-Anwendung für voraussichtlich mehr als die maximal tolerierbare Zeit nicht gegeben ist. Ursachen sind z. B. außergewöhnliche Störungen, eine besonders gravierende Schwachstelle, die nicht schnell behoben werden kann, interne Sabotage (z. B. Missbrauch von Adminrechten) oder besondere externe Angriffe (z. B. DDos). Dadurch sind wesentliche Unternehmens-Geschäftsprozesse nicht mehr möglich (Beispiel: Ausfall E-Mail und Wiki für Wirtschaftshilfen).
  Auch sind Schadensereignisse wie Feuer, Wasser, Zerstörung etc. auf IT-Infrastruktur ggf. Ursachen für eine Einschränkung der Verfügbarkeit.
  Die in Art. 32 DSGVO genannte „Belastbarkeit“ stellt einen speziellen Aspekt der Verfügbarkeit dar und wird daher in das Kriterium „Verfügbarkeit“ integriert.
- **Vertraulichkeit:**
  Es kann einen IT-Notfall darstellen, wenn Unterlagen, die nicht für die Öffentlichkeit bestimmt sind (z. B. interne Dokumentationen, Strategiepapiere, Ausschreibungen, personenbezogene Daten etc.) für nicht berechtigte Personen einsehbar sind (z. B. über eine Unternehmens-Website wie Wikis). Oder

Erpresser mit der Veröffentlichung solcher Daten drohen. Dadurch kann dem Unternehmen ein maßgeblicher Imageverlust, finanzielle Nachteile oder Nachteile bei der Bearbeitung von Unternehmens-Aufgaben entstehen (z. B. Entscheidungseinschätzungen und interne Kommunikation bei den Wirtschaftshilfen).

- **Integrität:**
  Es kann einen IT-Notfall darstellen, wenn falsche Informationen im Namen des Unternehmens verbreitet werden. Wenn dies seitens des Unternehmens nicht oder spät bemerkt wird (z. B. falsche Informationen zu wesentlichen Angeboten des Unternehmens) und diese nicht oder spät korrigiert werden können sind für das Unternehmen gravierende Nachteile möglich.

3.3.4 Schadenskriterien: niedrig bis sehr hoch

Zu entscheiden ist, in welche Schadenskategorie die Meldung fällt. Dies erfolgt auf Basis der zu erwartenden Schäden.
Quelle: BSI 3.3.2 Schadenskategorien und -szenarien festlegen, BSI 200-4 Tabelle 10

Schadenskategorie	Schadensszenario	Definition
Niedriger Schaden	finanzielle Auswirkungen	Der mögliche finanzielle Schaden ist für das Unternehmen unerheblich.
	Verstoß gegen Gesetze, Vorschriften oder Verträge	Es drohen keine juristischen Konsequenzen oder Konventionalstrafen.
	Beeinträchtigung der Aufgabenerfüllung	Die Abläufe im Unternehmen werden allenfalls unerheblich beeinträchtigt.
	negative Innen- und Außenwirkung	Es droht kein Ansehensverlust bei Kunden und Geschäftspartnern.
Mittlerer Schaden	finanzielle Auswirkungen	Der mögliche finanzielle Schaden ist für das Unternehmen tolerabel.
	Verstoß gegen Gesetze, Vorschriften oder Verträge	Es drohen nur geringfügige juristische Konsequenzen oder Konventionalstrafen.
	Beeinträchtigung der Aufgabenerfüllung	Die Abläufe werden allenfalls unerheblich beeinträchtigt.
	negative Innen- und Außenwirkung	Es droht ein Ansehensverlust nur bei wenigen Kunden und Geschäftspartnern.
Hoher Schaden	finanzielle Auswirkungen	Der mögliche finanzielle Schaden ist für das Unternehmen erheblich und nachhaltig spürbar.

	Verstoß gegen Gesetze, Vorschriften oder Verträge	Es drohen schwerwiegende juristische Konsequenzen oder Konventionalstrafen.
	Beeinträchtigung der Aufgabenerfüllung	Die Abläufe werden erheblich beeinträchtigt.
	negative Innen- und Außenwirkung	Das Ansehen des Unternehmens bei Kunden und Geschäftspartnern wird erheblich beeinträchtigt.
Sehr hoher Schaden	finanzielle Auswirkungen	Der mögliche finanzielle Schaden hat existenzbedrohende Ausmaße.
	Verstoß gegen Gesetze, Vorschriften oder Verträge	Die juristischen Konsequenzen oder Konventionalstrafen sind existenz-gefährdend.
	Beeinträchtigung der Aufgabenerfüllung	Die Abläufe werden so stark beeinträchtigt, dass Ausfallzeiten nicht toleriert werden können.
	negative Innen- und Außenwirkung	Das Ansehen des Unternehmens bei Kunden und Geschäftspartnern wird grundlegend und nachhaltig beschädigt.

3.3.5 Einstufungskriterien: „Betriebsstörung oder IT-Notfall?“

Die Einstufung als IT-Notfall ergibt sich aus

- Möglicher Schaden: Einstufung des Schadensszenarios
- Nötige Reaktionsgeschwindigkeit (in Abhängigkeit vom Schaden, Ressourcen…)
- Aufwand für Maßnahmen: Die für den Notbetrieb und die Wiederherstellung des Normalbetriebs nötigen Ressourcen (personell, finanziell …)

Einstufung in fünf Szenarien:

Einstufung	Denkbarer Schaden für das Unternehmen	Reaktions-geschwindigkeit	Nötige Ressourcen	Beispiel
ROT: Schwerer IT-Notfall	Sehr hoher Schaden	Sofortige Handlungs-notwendigkeit	Umfangreiche und ungeplante Ressourcen sind nötig, eine zeitnahe Lösung NICHT erwartbar	- Absehbar längerfristiger Ausfall eines IT-Bereiches - Siehe Anhang IT-Notfallszenarien wie z. B. „längerer Ausfall von Kronjuwelen-Anwendungen“, „Ransomware-Erpressung“, „Drohung der Veröffentlichung sensibler Daten/Unterlagen“
ORANGE: IT-Notfall	Hoher Schaden	Schnelle Handlungs-notwendigkeit	Ungeplante Ressourcen sind nötig, eine zeitnahe Lösung NICHT erwartbar	- Defacement einer Website - Sicherheitslücke auf einer Website wird aktiv ausgenutzt - Schwere Sicherheitslücke wird bekannt, Updates müssen schnell eingespielt werden oder Anwendung abgeschaltet werden
GELB: Schwere Betriebs-störung	Mittlerer Schaden	Schnelle Handlungs-notwendigkeit	vorhandene, wenngleich nicht dafür eingeplante, Ressourcen sind ausreichend für eine zeitnahe Lösung	- Längerer Ausfall der VDI-Umgebung - Längerer Ausfall der Mails
HELLGRÜN: Betriebs-störung	Niedriger Schaden	Zeitnahe Handlungs-notwendigkeit	Vorhandene, eingeplante Ressourcen sind ausreichend für eine, sehr zeitnahe Lösung	- Ausfall bestimmt der Datenbanken, z. B. Veranstaltungsdatenbank - Website offline, Restart schnell möglich
GRÜN: Fehlalarm	Kein bis vernach-lässigbarer Schaden	Keine Handlungs-notwendigkeit	Entfällt	- Sehr kurze Störung - Fehlalarm

Darüber hinaus kennt der BSI 200-4 den Begriff „Krise“: Wenn für die Situation keine Notfallpläne vorhanden sind oder die bestehenden Notfallpläne nur bedingt angewendet werden können, handelt es sich um eine Krise, die im situativ behandelt werden muss.

3.3.6 Konkrete IT-Notfallszenarien, Kronjuwelen

Im Anhang „Notfallszenarien“ sind Notfallszenarien gelistet. Erst aus dem denkbaren resultierenden Schaden, Ressourcennotwendigkeit und nötiger Reaktionsgeschwindigkeit ergibt sich für eine Anwendung bzw. dessen Problemsituation eine Bewertung von grün bis rot.
Für bestimmte „Kronjuwelen“-Anwendungen müssen besondere Maßstäbe angesetzt werden, die diese für die

Geschäftstätigkeit des Unternehmens eine besondere Bedeutung haben (bzw. der denkbare Schaden besonders gravierend ausfallen könnte).

4 IT-Sofortmaßnahmen

Die Meldung wurde als IT-Notfall eingeschätzt („orange“ bzw. „rot“). Im Folgenden wird beschreiben, wie damit verfahren wir. „Betriebsstörungen“ (bis „gelb“) werden im Rahmen des üblichen IT-Supports behandelt.

4.1 Grundsätzliches Vorgehen bei IT-Sofortmaßnahmen im IT-Notfall

- Verhindern, dass der Schaden größer wird:
  - Grundsätzlich gilt: Je nach Situation zuerst immer die normalen Rettungsmaßnahmen ergreifen, z. B. Menschen aus der Gefahrenzone bringen, Löschversuch unternehmen, Rettungsdienste alarmieren.
  - z. B. Website in den Wartungsmodus versetzen: Manuelle Tätigkeit durch IT-Admin Backend (siehe Anhang Kontaktdaten)
  - ggf. Server vom Netz abtrennen: Manuelle Tätigkeit durch IT-Admins
  - ggf. Nutzer-IT vom Netz abtrennen: Manuelle Tätigkeit durch Mitarbeiter
- **Beweise sichern:**
  - z. B. Logfiles sichern
  - z. B. Bildschirm mit dem Smartphone abfotografieren
- **Backups sichern:**
  - Backup-Bandroboter: Wenn der Verdacht auf eine Kompromittierung besteht, müssen alle bereits beschriebenen Bänder aus der Tape Library entfernt werden und durch leere Bänder ersetzt werden. Ziel ist es, mit den bisher genutzten Bändern Backups zu haben, die (hoffentlich) vor Verschlüsselung geschützt sind.
- **Situation nachvollziehbar machen:**
  - z. B. Protokoll der Ereignisse mit Datum und Uhrzeit führen
    Protokollvorlage siehe *„Ergänzende-Dokumente\Protokollvorlage“*

Sollte besondere Schnelligkeit nötig sein: Die Mitglieder der IT-Notfallstabes sind berechtigt, im IT-Notfall die hier dokumentierten IT-Sofortmaßnahmen ohne Rücksprache sofort einzuleiten. Die ggf. entstehenden Kosten sind im Rahmen der Zeichnungsbefugnisse freigebbar.

4.2 Ressourcen für IT-Sofortmaßnahmen

4.2.1 IKT-Interne-Zuständigkeiten und Dokumentationsorte

Für IT-Sofortmaßnahmen kann auf die Einschätzungen und Ressourcen des IT-Supports und der technisch bzw. fachlichen Verantwortlichen zurückgegriffen werden, siehe Kapitel 3.3.2.

4.2.2 Dienstleister, Personal

Wer kann bei IT-Sofortmaßnahmen unterstützen?

- Intern:
  Für IT-Sofortmaßnahmen kann auf die Einschätzungen und Ressourcen des IT-Supports und der technisch

bzw. fachlichen Verantwortlichen zurückgegriffen werden, siehe Kapitel 3.3.2.
Für den IT-Notfall erweitert: Anhang „Kontaktdaten“

- Extern:
  - IT-Dienstleister etc.
  - Behörden, Strafverfolgung
  - CyberSchutz Versicherung, s.u.

4.2.3 CyberSchutz Versicherung

Seit dd.mm.YYYY besteht eine CyberSchutz Versicherung. Einsatz-Entscheidung durch ….

Basisdaten:

- Versicherunganbieter: ….
- Versicherungsschein-Nummer: …
- Versicherungsnehmer: ….
- Versicherungsschein: ….
- Kontakt:
  - N. N., Tel / Mail: …..
  - Zuständige Schadensabteilung: ….
  - Krisenhotline: ….

Wichtige Hinweise aus dem Versicherungsschein exzerpieren:

- Wann tritt der ggf. Versicherungsfall ein? Z. B. auch wenn öffentliche Medien berichten?
- Wartefrist: Beginnt zum Eintritt der Betriebsunterbrechung und endet nach Ablauf von X Stunden?
- Haftzeit: Max. X Tage ab Zeitpunkt der Erkennbarkeit des Schadensfalls (nicht des Zeitpunkts der Meldung an den Versicherer)?
- Ist die Zustimmung des Versicherers ist bei bestimmten Maßnahmen vorab nötig (z. B. Engagement externer Experten)?
- Besteht eine **Anzeigepflicht bei Eintritt eines Versicherungsfalls**, insbesondere bei Cyber-Erpressung?
- **Muss der Versicherungsschutz bzgl. Cyber-Erpressung geheim gehalten werden?**
- **Weisungsrecht des Versicherers?**

Was umfasst der Versicherungsschutz?

- Dritt- und Eigenschäden, Abwehrkosten, spezielle Kosten im Rahmen der Versicherungsbedingungen?
- Limitierung durch diverse Kostengrenzen (z. B. grundsätzliche Höchstersatzleitung, Hardwareschäden, Bußgelder…), Selbstbeteiligung?
- Betriebsunterbrechung aufgrund fehlerhafter Bedienung?
- …

Was ist NICHT versichert?

- Stromprobleme (Ausfall, Überspannung,..)
- Überhitzung
- unterlassene Systemupgrades
- Softwarefehler
- Interne Netzwerkfehler
- Hardwarefehler
- Vorsätzliche Pflichtverletzung / Strafbares Verhalten
- ….

5 Ausrufen eines IT-Notfalls

5.1 Reihenfolge

Zunächst sind je nach Situation die IT-Sofortmaßnahmen zu ergreifen bzw. einzuleiten. Es muss eine danach eine erneute Entscheidung getroffen werden, ob es sich

- Doch „nur“ um eine „normale“ Betriebsstörung handelt.
- Oder weiterhin um einen IT-Notfall, zu dem weitere umfangreiche Maßnahmen ergriffen werden müssen.

5.2 Wer ruft den Notfall aus?

Der IT-Notfall kann durch folgende Personen ausgerufen werden, im Idealfall in gegenseitiger Rücksprache:

- Geschäftsführung
- jedes Mitglied des IT-Notfallstabs

5.3 Alarmierung

Schnelle Weitergabe von Infos zur Unterstützung der IT-Sofortmaßnahmen. Tiefer gehende Informationen erfolgen erst später.

5.3.1 Wen im IT-Notfall alarmieren?

Bei Eintritt eines IT-Notfalls sind mindestens die folgende Rollen zu benachrichtigen:

- IT-Notfallstab, Kontaktdaten zu Mitgliedern siehe Anhang Kontaktdaten
- Der IT-Notfallstab entscheidet, wer zusätzlich alarmiert wird. Insbes. gilt das für die Personen mit Rolle „Optional IT-Notfallstab“ (Geschäftsführung, Bereichsleiter Kommunikation, Datenschutz, ProductOwner…).

5.3.2 Wie alarmieren: Alarmierungswege

Sofern vorhanden, sollten immer mehrere Kanäle parallel genutzt werden. **Ggf. stehen diese im IT-Notfall nur teilweise zur Verfügung.**

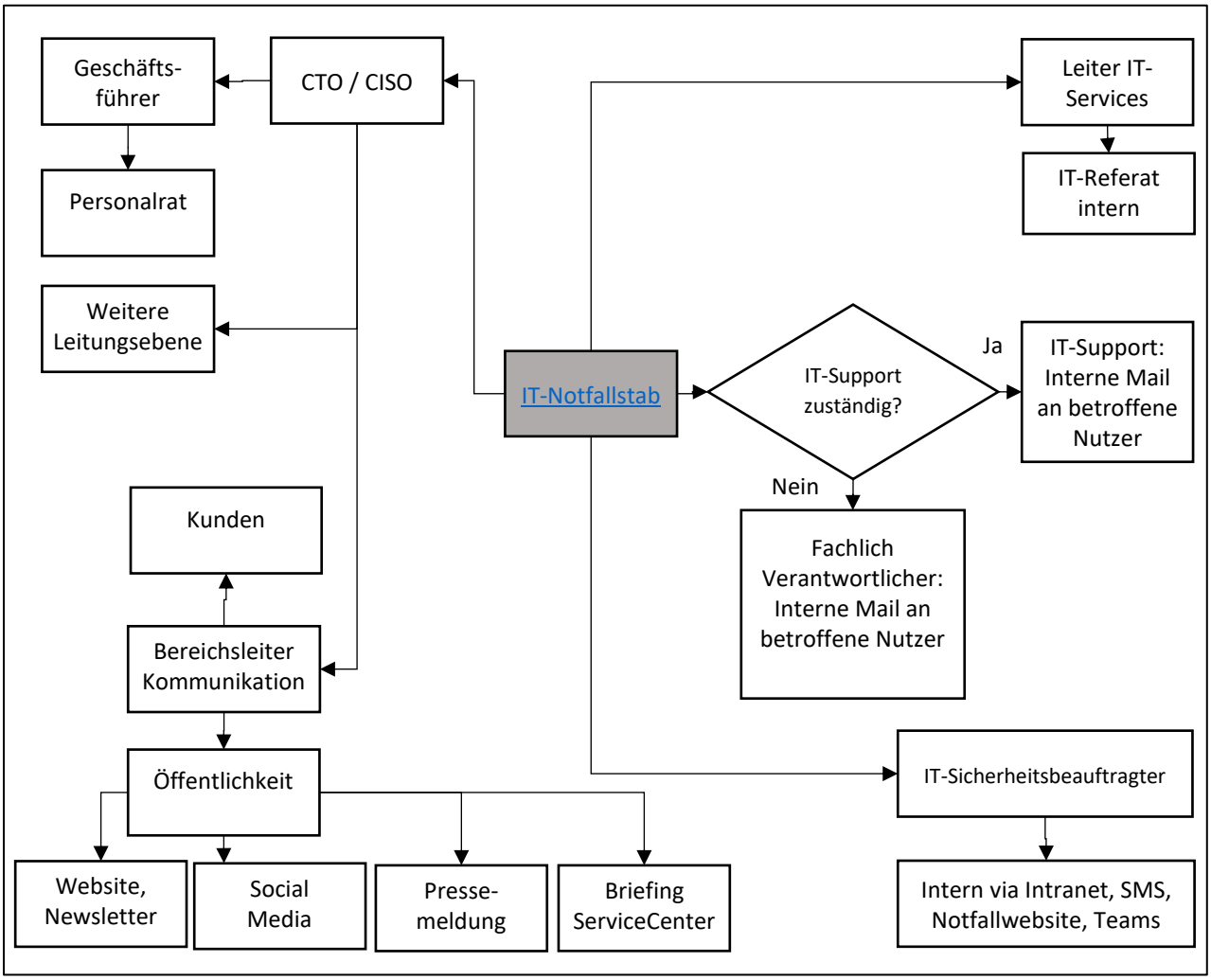
Alarmierungswege sind:

- „Klassische“ E-Mail:
  Nötige Voraussetzung: Zugang zu funktionierendem E-Mailsystem für Sender und Empfänger
- Intranet (insbes. bei Betriebsstörungen)
  Nötige Voraussetzung: Zugang zum Unternehmens-Netz
- Internet: Notfallwebsite
  Nötige Voraussetzung: Öffentlich erreichbare Website mit Passwortschutz
- Messenger-Dienste:
  Nötige Voraussetzung: z. B. interne, informelle Whatsapp-Kontakte / -Gruppen in Referaten oder Bereichen

- SMS:
  Versand von SMS (max. 160 Zeichen) an Diensthandies
  Nötige Voraussetzung: Versandwebsite mit Login & Guthaben zum SMS-Versand:
- Microsoft Teams
  Nötige Voraussetzung: Zugang zu Teams für Sender und Empfänger
- Festnetz-/Mobil-Telefon
  Nötige Voraussetzung: Funktionierendes Telefon beim Sender und Empfänger
- Fax:
  Nötige Voraussetzung: Funktionierendes Fax beim Sender und Empfänger
- persönlich vor Ort, ggf. 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.

5.3.3 Meldebaum für Alarmierung: Schnelle Info-Weitergabe zur Unterstützung der IT-Sofortmaßnahmen

Um die Arbeitslast der Alarmierung aufzuteilen, wird der folgende Melde-Baum verwendet. Der Plan sollte bei den ausführenden Personen griffbereit vorliegen.



5.3.4 Beispielhafte Alarmierungs-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:	schwerer IT-Notfall
betroffene Bereiche:	z. B. Bürokommunikation
Verbote:	z. B. Keine IT-Geräte einschalten oder mit dem Netz verbinden wegen Malware-Gefahr
Handlungen:	z. B. mit dem Vorgesetzten in Kontakt treten, ...
Weitergabe:	Weitergabe dieser Information entsprechend Meldebaum (s.o.)

6 Notfallmanagement durch den IT-Notfallstab

6.1 Ziel des IT-Notfallstabes

Die wichtigste Aufgabe des IT-Notfallstabes ist der Wiederanlauf zu einem Notbetrieb, sowie die Wiederherstellung des Normalbetriebs.

6.2 Zusammenstellung des IT-Notfallstabes

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

Mitglieder des IT-Notfallstabes (siehe Anhang Kontaktdaten):

- Geschäftsführer
- Gebäudemanagement
- Finanzen
- Personalabteilung
- Kommunikation
- IT-Sicherheitsbeauftragter
- …weitere relvante Führungskräfte…

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

Der IT-Notfallstab, ggf. einzelne Mitglieder davon, entscheidet, welche weiteren Personen in den Notfallstab aufgenommen werden sollen (insbes. die optionalen Mitglieder des IT-Notfallstabes).
Siehe hierzu *„Kontaktdaten IT-Notfallplan Anhang.docx“*

Im IT-Notfall zu klärende Fragen:

- Wer soll zusätzlich Mitglied des IT-Notfallstabes sein?
- Ist die Anwesenheit der Mitglieder gewährleistet? Muss eine Urlaubssperre verhängt werden?

6.3 Arbeitsräume für den IT-Notfallstab

Büros:

- …
- …

Ausweichräume außerhalb des Firmengeländes:

- Homeoffice: Digitale Verbindung via MS-Teams (alternativ: Telefonkonferenz oder GoToMeeting)
- Ggf. anzumietende Räumlichkeiten

6.4 Arbeitsmodi des IT-Notfallstabs

Abhängig von der Situation sind für den Notfallstab 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.

Ggf. muss für die Mitglieder des IT-Notfallstabes eine Urlaubssperre verhängt werden. Bzw. dies aus dem Urlaub etc. in das Unternehmen gerufen werden.

Im IT-Notfall zu klärende Fragen:

- Wann findet in welcher Besetzung die nächste Sitzung des IT-Notfallstabes statt?
- Welcher Teilnehmer protokolliert die Aktivitäten des IT-Notfallstabes?
- Muss die Personalabteilung / Personalrat einbezogen werden bzgl. Arbeitszeiten?
- Muss versucht werden, Mitarbeiter aus Urlaub in die Arbeit zu holen?
- Macht eine Urlaubssperre für Mitglieder des IT-Notfallstabes Sinn?

6.5 Meldepflichten, Meldeoptionen

Bei einem IT-Notfall müssen u.U. innerhalb definierter Fristen Meldungen an Behörden und andere Institutionen gemacht werden.
Dadurch sollen Schwierigkeiten durch Ordnungsgelder, Kontopfändungen usw. abgewendet werden, z. B. :

- Sich verzögernde Pflichtmeldungen an Behörden
- Rücksprache bzgl. Erfüllung hoheitlicher Aufgaben
- Sich verzögernde Zahlungen
- Sich verzögernde Bereitstellung statistischer Daten

6.5.1 Aufsichtsbehörden

6.5.1.1 Datenschutz

Bei möglichen oder tatsächlichen Datenschutzverstößen: D. h. wenn personenbezogene Daten in irgendeiner Form involviert sind:

- Verantwortlich: Die Geschäftsführung entscheidet, ob eine Meldung erfolgt, Kontakt siehe Anhang Kontaktdaten.
- Fachlich federführend: Datenschutzbeauftragte

Im IT-Notfall zu klärende Fragen:

- Entscheidung Geschäftsführung, inwieweit der interne Datenschutz einbezogen wird
- Entsprechend kontaktiert HGF den internen Datenschutz

Hintergrund, Ergänzendes:

- Meldung an die Datenschutzbehörde innerhalb von 72 Stunden ab bekanntwerden eines relevanten Vorfalles. Ggf. müssen Datenschutzbeauftragte von Kunden und Dienstleistern benachrichtigt und einbezogen werden (siehe Anhang Kontaktdaten).
- Ggf. Koordination mit anderen Unternehmen, Dienstleistern etc. Hinsichtlich der Meldung.
- Sofern verfügbar und zeitlich angemessen: Meldung über ein Ticketsystem
- Die Meldungen sollten immer nachweisbar sein. Beispiel: schriftlich, Telefonate vor Zeugen führen, nachträglich Mails schreiben, Inhalt mit Datum und Uhrzeit dokumentieren usw.
- Vorlage: Muster Datenschutz-Meldung.doc

6.5.1.2 Aufsichtsbehörden

Prüfung, ob Aufsichtsbehörden informiert werden müssen / sollten.

Im IT-Notfall zu klärende Fragen:

- Entscheidung Geschäftsführung, inwieweit Aufsichtsbehörden informiert werden
- Entsprechend kontaktiert Geschäftsführung die Aufsichtsbehörden

6.5.2 Anzeigepflicht bzgl. Cyber-Versicherung

Falls eine **Anzeigepflicht bei Eintritt eines Versicherungsfalls** (siehe Versicherungsschein) besteht: Insbesondere bei Cyber-Erpressung.

Im IT-Notfall zu klärende Frage:

- Die Geschäftsführung entscheidet, ob eine solche Meldung erfolgt.

6.5.3 Strafverfolgungsbehörden: ZAC, CAZ, ZCB

Die Einbeziehung (insbes. der Polizei) ist ggf. Haftungs- und Versicherungstechnisch notwendig. Einsatz-Entscheidung durch die Geschäftsführung.

- **Zentrale Ansprechstelle Cybercrime (ZAC) am Bay. LKA**
  „Nach einem strafrechtlich relevanten Sicherheitsvorfall in Ihrer Organisation nehmen Sie bitte zunächst telefonisch Kontakt mit einem unserer Sachbearbeiter auf. Dieser wird Ihnen, nach einer

vorläufigen Bewertung der Situation, erforderliche Maßnahmen empfehlen und ggf. ein polizeiliches Ermittlungsverfahren einleiten.

Als Ersthelfer bieten Ihnen die erfahrenen Mitarbeiter der ZAC wichtige organisatorische und technische Hinweise, um die oft chaotische Lage nach einem Angriff zu bewältigen.
Der diskrete Umgang mit Informationen ist für die Polizeibehörden eine gesetzliche Verpflichtung!

„In dringenden Fällen außerhalb der genannten Bürozeiten, etwa bei einem laufenden Cyberangriff auf ihre Organisation, kontaktieren Sie bitte den Polizeinotruf 110!“

Zentrale Ansprechstelle Cybercrime Bürozeiten: Mo-Do 08.00 Uhr - 16.00 Uhr, Fr 08.00 Uhr - 14.00 Uhr
Telefon ZAC: 089/1212-3300
https://www.polizei.bayern.de/kriminalitaet/internetkriminalitaet/002464/index.html

- **Bayerisches Landesamt für Verfassungsschutz, Wirtschaftsschutz, CAZ**
  „Bei einem versuchten oder erfolgreich durchgeführten Elektronischen Angriff auf ein Unternehmens- oder Hochschulnetzwerk berät sich das CAZ gemeinsam mit den Betroffenen zeitnah und vertraulich über das weitere Vorgehen. Das betroffene Unternehmen beziehungsweise die betroffene Hochschule erhält vom CAZ nach der forensischen Analyse und der nachrichtendienstlichen Bewertung eine Rückmeldung mit Handlungsempfehlungen. Andere möglicherweise von einem ähnlichen Angriff betroffene Unternehmen und Einrichtungen erhalten Informationen zu den erkannten Angriffsmustern, selbstverständlich in anonymisierter Form.“
  Knorrstraße 139, 80937 München, Telefon: 089/31201-222, caz@lfv.bayern.de
  https://www.verfassungsschutz.bayern.de/spionageabwehr/cyber_allianz_zentrum/index.html

- **„Zentralstelle Cybercrime Bayern“ (ZCB) bei der Generalstaatsanwaltschaft Bamberg**
  „Bayernweit zuständig für die Bearbeitung herausgehobener Ermittlungsverfahren im Bereich der Cyberkriminalität“
  Wörthstraße 7, 96052 Bamberg, Telefon: 0951/833-0, poststelle@gensta-ba.bayern.de
  https://www.justiz.bayern.de/gerichte-und-behoerden/generalstaatsanwaltschaft/bamberg/spezial_1.php

6.5.4 Verbundene „Einrichtungen“, „Kunden“

- Mail über Probleme und mögliche Verzögerungen
- Informationen zu veränderten Erreichbarkeiten
- Informationsbanner auf der Website
- Ggf. verpflichtend falls Datenschutz dies erfordert

Je nach Situation bzw. Betroffenheit ggf. folgende Einrichtungen informieren:

- Wirtschaftsprüfer
- Andere Unternehmen
- Kunden (siehe Anhang Kontaktdaten)

6.5.5 Dienstleister

Betroffene Dienstleister sind ggf. zu informieren.

6.6 Dokumentation und Beweissicherung

6.6.1 Notwendigkeit der 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.
→ Protokollvorlage siehe „Ergänzende-Dokumente\Protokollvorlage“

6.6.2 Forensische Sicherung auf IT-Systemen

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

6.7 Kommunikation (nachfolgend zur Alarmierung)

Über Meldepflichten / Meldeoptionen hinaus ist ggf. weitere Kommunikation erforderlich:

6.7.1 Interne Kommunikation

6.7.1.1 Mitarbeiter intern 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.

6.7.2 Externe Kommunikation, Öffentlichkeitsarbeit

6.7.2.1 Übersicht

Notfälle haben eine erhebliche Auswirkung auf das Geschäft und sind damit in unterschiedlichen Graden auch außerhalb des Unternehmens wahrnehmbar, für Geschäftspartner und Kunden (siehe Anhang Kontaktdaten) 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.

6.7.2.2 Bereichsleiter Kommunikation

Der Bereichsleiter Kommunikation stimmt die öffentliche Kommunikation ab. Hierbei arbeitet er mit dem Pressesprecher, SocialMedia-/Marketing-Verantwortlichen und dem Leiter des ISZ zusammen. Rollen bzgl. Unternehmens-Kommunikation siehe hier (siehe Anhang Kontaktdaten).

Instrumente:

- Pressemitteilungen: Per Mail an Pressekontakte, auf Unternehmens-Medien, auf Pressportalen. Ggf. Telefonate, Gespräche mit Pressevertretern
- Social Media: Postings auf geeigneten Kanälen
- Unternehmenseigene-Kanäle, z. B. Websites: Veröffentlichung geeigneter Informationen

6.7.2.3 Textbausteine für Pressemitteilungen, Postings…

Unternehmen von Cyber-Angriff betroffen, Beispiel Ransomware

Einleitung:

Am <Datum> wurde unser Unternehmen von einem schweren Cyber-Angriff getroffen. Das führt zu <ernsthaften> Einschränkungen <in der Auftragsabwicklung, bei der Durchführung von Dienstleistungen, ...> an <den Standorten ..., an allen Standorten>.

Geschehen:
Durch Ransomware wurden die Inhalte <mehrerer Server> verschlüsselt, davon betroffen <ist die Bürokommunikation, sind größere Teile der IT-Infrastruktur>.

Maßnahmen:
Wir arbeiten 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, werden wir darüber informieren.
Für weitere Fragen wenden Sie sich bitte an <Kontaktdaten Pressesprecher o.ä.>.

6.8 (Kurzfristige) Wiederherstellung der Arbeitsfähigkeit

Ggf. gibt es Möglichkeiten, ohne oder mit anderer IT die Aufgaben zu erfüllen?
Bei den jeweiligen Aufgaben / Anwendungen / Prozessen sind im Anhang „Notfallszenarien“ jeweils Möglichkeiten dafür beschreiben.

Prüfen, welche Aufgaben in welche der folgenden Kategorien fällt (Quelle: BSI „Erste Hilfe bei einem schweren IT-Sicherheitsvorfall“):

- **„Nicht betroffen“**
  Aufgaben, die keines der betroffenen Systeme verwenden.

- **„Auslagerungsfähig“**
  Aufgaben, die betroffene Systeme verwenden, die aber auf ein anderes eigenes oder fremdes System ausgelagert werden können. Die Auslagerungsfähigkeit kann je nach Aufgabe aber insbesondere auch nach der Größe der Organisation, der Organisationsumwelt etc. stark variieren. In diese Kategorie gehören Aufgaben, bei denen kurzfristig ein anderer Standort der Organisation oder eine andere Organisation innerhalb eines Organisationsverbunds (z.B. andere Unternehmen, Kommune, Geschäftsstellen etc.) die erforderliche IT-Ausstattung (neben Clients auch Server mit entsprechenden Fachverfahren) für die eigenen Beschäftigten zur Verfügung stellen kann.
- **„mit mobilem Equipment zumindest eingeschränkt Arbeitsfähig“**
  Aufgaben, die betroffene Systeme verwenden, aber auch mit mobilem, nicht betroffenen, Equipment (Homeoffice, „sauberer“ Laptop, mobiler Hotspot, Handy) zumindest eingeschränkt erbracht werden können. In Abgrenzung zu auslagerungsfähigen Aufgaben handelt es sich hier um die Bereiche, bei denen die eingesetzten Softwaresysteme entweder rein clientseitig funktionieren oder die externe Serverkomponente über das Internet erreichbar ist.
- **„ohne Neuaufbau nicht Arbeitsfähig“**
  Aufgaben, bei denen die Arbeitsfähigkeit nicht nach den vorgenannten Kategorien besteht oder hergestellt werden kann.

In einem nächsten Schritt können dann unter den Aufgaben jeder Kategorie diejenigen identifiziert werden, die als funktionswichtig angesehen werden und deshalb priorisiert lauffähig gemacht werden müssen.

Mitarbeiter:
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:

- Homeoffice statt Büro
- Arbeitsplätze aufräumen
- In mehreren Schichten arbeiten
- An Wochenenden arbeiten
- Kurzarbeit
- Urlaub abbauen

TEXTVORSCHLAG bzgl. Anwesenheit im Büro
Liebe Kolleginnen und Kollegen, die Systeme mussten am Wochenende erneut runter gefahren werden, einige Anwendungen werden vorerst leider nicht zur Verfügung stehen. Wann einzelne Systeme wieder zugeschaltet werden, lässt sich derzeit schwer vorhersagen. Für uns ist es jetzt in besonderem Maße wichtig, die Geschäftsprozesse im Blick zu haben und ggf. über Workarounds weiterhin am Leben zu halten. Bitte stellt deshalb sicher, dass die Mitarbeiter/-innen weiterhin an ihren Arbeitsplatz kommen und die Teams funktionsfähig bleiben - auch wenn deren Hauptanwendungen vorübergehend nicht zur Verfügung stehen. Sobald die Systeme wieder hochgefahren werden, sollte das Arbeiten schnell losgehen können. Selbstverständlich können einzelne Gleitzeit- oder Urlaubsanträge großzügig genehmigt werden.
FAQs: „Ich könnte ins Büro kommen, aber meine Hauptanwendung steht nicht zur Verfügung, was soll ich tun?“ Bitte kommen Sie trotzdem ins Büro. Die Aktivierung der Systeme kann zur Zeit schlecht geplant werden. Es kann also sein, dass einzelne Anwendungen im Laufe des Tages hochgefahren werden. Dann ist es wichtig, dass die Arbeit in den Systemen wieder zügig aufgenommen wird. Aber auch für die Etablierung von analogen Prozessen ist es wichtig, dass Sie kreativ mitdenken und mitarbeiten. Alternativ können Sie sich mit Ihrer Führungskraft auf Gleitzeit oder Urlaub einigen.

7 Wiederanlauf und Wiederherstellung

Beim Wiederanlauf zu einem Notbetrieb und der Wiederherstellung des Normalbetriebs stellen sich folgende Fragen, die jeweils für die einzelnen IKT-Anwendungen / Anteile beantwortet werden müssen:

- Welche der betroffenen IKT-Teile sind so zeitkritisch (z. B. längere Unterbrechung durch Ausfall dieser IT hätte schwerwiegende Folgen für das Unternehmen), so dass diese prioritär behandelt werden muss?
  Erste Hinweise gibt die Einstufung des Vorfalls („Grün“ bis „Rot“).
  Die Grundlage dafür liefert eine Business Impact-Analyse (BIA). Aus den denkbaren Schäden für das Unternehmen wird die Kritikalität der IKT-Teile eingeschätzt.
- 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 IT-Notfall-Ressourcen, tiefer gehende Informationen

Im IT-Notfall reichen die Ressourcen für IT-Sofortmaßnahmen nicht mehr aus. Weitere Ressourcen sind für den Notbetrieb und die Wiederherstellung des Normalbetriebs nötig:

7.1.1 Weitergehende Ressourcen für IT-Notfälle

- Cyberversicherung
- Strafverfolgungsbehörden
- BSI-Liste von zertifizierten APT Response-Dienstleistern („Ergänzende-Dokumente\Dienstleister“):
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister_APT-Response-Liste.html
  Hierbei vorhandene Erfahrungen mit folgenden Unternehmen:
  - ....
  - ....

7.1.2 Netzwerke, Internet-Anbindung

Diverse Dokumente unter „Ergänzende-Dokumente\netzwerk“:

- Netzwerkplan der Standorte
- Übersicht IT-Netzwerkverbund
- WAN Standorte
- …

7.2 Backup

7.2.1 Selbst gehostete Anwendungen

Eine besondere Rolle spielen für Notbetrieb und v. a. Wiederanlauf zum Normalbetrieb die Backups. Im IT-Notfall auf funktionierende Backups zurückzugreifen ist essentiell. Nicht umsonst sind Backups ein bevorzugtes Ziel von IT-Angriffen.
Das betrifft v. a. die IT-Bereiche mit der Basisinfrastruktur.

Das zentrale Backup umfasst eine Sicherung von

- Cloud…
- M365
- Netzwerklaufwerke
- …

Realisiert wird das Backup mittels der Software „…“
Unterlagen hierzu siehe „Ergänzende-Dokumente\backup“:

- Installations-Dokumentation
- Handbuch Administrative Tätigkeiten

Isolation:
Die Backups werden auf Disk / Tape täglich / wöchtentlich / … gesichert. Insbesondere werden die Tapes physikalisch isoliert aufbewahrt.

Sofortmaßnahme: Wenn der Verdacht auf eine Kompromittierung besteht, müssen alle bereits beschriebenen Bänder aus der Tape Library entfernt werden und durch leere Bänder ersetzt werden. Ziel ist es, mit den bisher genutzten Bändern Backups zu haben, die vor Verschlüsselung (hoffentlich) geschützt sind.

7.2.2 Von Dienstleistern gehostete Anwendungen

Bei von Dienstleistern gehosteten Anwendungen wird das Backup durch den Dienstleister gemangt.
Für besonders wichtige Anwendungen sollte das Unternehmen über eigene, lokale Backups verfügen.

7.2.3 Backup-Herausforderung: Nutzer- und Datenmanagement nach erfolgreicher Wiederinstallation

Wenn es gelungen ist, eine Software samt Daten aus Backup-Dateien neu zu installieren ergeben sich Folgefragen:

- Was ist in der Zeit zwischen Backup und Installation passiert?
- Stehen für die Backup-Installation jede „begleitende“ Software zur Verfügung?
  Damit sind insbesondere Berechtigungssysteme (z. B. LDAP) gemeint, die üblicherweise nicht unmittelbarer Teil des Backups sind.

Im Detail:

- Ggf. hat der mit dem Backup installierte Nutzerpool genau den Datumstand des Backups. Das bedeutet, dass Login von in der Zwischenzeit ausgeschiedenen Mitarbeiter noch aktiv sind (→deaktivieren). Und mittlerweile neue hinzugekommen Nutzer (z. B. neue Mitarbeiter) noch nicht vorhanden sind (-> einspielen).
- Falls nötig: Wie können in der Zwischenzeit aufgelaufene Daten mit korrekten Zeitstempeln versehen werden?
- Falls der Fall: Wie können in der Zwischenzeit aufgelaufene digitale Daten (z. B. aus Übergangs- / Notlösungen) eingespielt werden.

Im IT-Notfall zu klärende Frage:

- Wie können Anwender (z. B. Produktverantwortliche, Keyuser…) möglichst frühzeitig beim der Wiederinbetriebnahme beim zunächst sehr technischen Prozess der Backup-Nutzung einbezogen werden?

7.3 Beendigung und Nachbereitung des IT-Notfalles

7.3.1 Beendigung des IT-Notfalls

Wie beim Ausrufen des IT-Notfalles wird über das Ende des IT-Notfalls informiert.

7.3.2 Nachbereitung

Erkenntnisse aus dem IT-Notfall müssen genutzt werden, um die Wahrscheinlichkeit weiterer IT-Notfälle zu reduzieren.
Dazu können beispielsweise folgende Frage beantwortet werden:

- Wann kam es warum zum IT-Notfall?
- Welche Änderungen am wieder hergestellten System sind nötig, um einen erneuten IT-Notfall zu vermeiden?

In der Folge können Verbesserungen erfolgen:

- evtl. Aktualisierung dieses Dokumentes
- evtl. Dokumentation des IT-Notfalls
- evtl. Anpassung der Betriebshandbücher
- evtl. Anpassung der IT-Prozesse
- evtl. Umstellung der IT-Technik

8 Notfall-Prävention, wiederkehrende Aktivitäten

8.1 Weiterbildung: Mitarbeiter

Zur Notfallvorsorge gehört die Weiterbildung der Mitarbeiter. Diese kann differenziert werden zwischen “Nicht -IT“ Mitarbeitern und „IT“ Mitarbeitern.

8.1.1 „Nicht-IT“ Mitarbeiter

Beständige Sensibilisierung über Intranet und Onlineschulungen. Z.B. über Online-Schulungen zur IT-Sicherheit speziellen Onlineangeboten. Sowie immer wieder verschickte Test-Phishing-Mails inkl. Monitoring.

8.1.2 „IT“--Mitarbeiter

IT-Mitarbeiter sollten grundsätzlich in der Lage sein, technische Abläufe genauere nachzuvollziehen zu können und grundsätzliche Fehlerquellen und Sicherheitsrisiken zu erkennen.
Hierzu werden regelmäßig technische Schulungen durchgeführt, die dazu befähigen. Z. B. bzgl. OWASP für die Sicherheit von Onlineanwendungen für Admins, Softwareentwickler, Projektmanager und andere technisch im Detail interessierte Mitarbeiter.

8.2 Bestehende und neue IT-Anwendungen

8.2.1 Integration von IT in den IT-Notfallplan

Um den Notfallplan aktuell und vollständig vorliegen zu haben, ist es nötig, IT-Anwendungen hinsichtlich

- der Notwendigkeit der Notfallplanung einzuschätzen und ggf.
- Notfall-Szenarien in diesem Notfallplan aufzunehmen (Meldewege, Verifikation, IT-Sofortmaßnahmen, Notfalleinschätzung, Notbetrieb, Wiederanlauf, Nachbereitung)

Dies gilt insbesondere für neu hinzukommende IT-Anwendungen.
Unter „Check-Anwendung-Musterunterlagen“ finden sich dafür hilfreiche Unterlagen.

8.2.2 Monitoring der IT-Anwendungen

Um von Updates, Sicherheitsprobleme etc. zu erfahren ist das Monitoring von ProductOwnern, Anwendern, Admins, Dienstleistern… der IT-Anwendungen nötig. Dies umfasst einerseits die IT-Anwendung selbst, als auch die Herstellerinformationen zur IT (z. B. Updates, Sicherheitswarnungen etc.) als auch öffentliche Stellen (z. B. BSI) und Verzeichnisse (z. B. www.cve.org).

8.3 IT-Admins

Die Zugänge der IT-Admins bedürfen der besonderen Beachtung:

- Passwortwahl in der IT-Infrastruktur
  Der Schutzbedarf von Passwörtern für die IT-Infrastruktur (z. B. für Admins) ist „sehr hoch“. Daher müssen Admin-Passwörter komplexeren Anforderungen (Groß- / Kleinschreibung, Sonderzeichen, Mindestlänge) genügen als Passwörter von Nicht-Admins. Zudem müssen die Admin-Logins immer der jeweiligen Adminaufgabe zugeordnet sein und nicht ein „Admin-Single-Sign-On“ sein.
- Grundprinzip 2FA-Authentisierung:
  - Wo immer möglich wird 2 Faktor-Authentifizierung (2FA) eingesetzt.

8.4 Tests, Notfallübungen

Notfälle sollten immer wieder geübt werden. Insbesondere:

- Test der Meldewege
- Durchführung von IT-Sofortmaßnahmen
- Test der Wiederanlaufpläne
- Test der Nutzbarkeit von Backups