

CHECKLISTE – IT-NOTFALL- PLAN – SICHERN SIE DATEN, TECHNIK UND SYSTEM IHRES UNTERNEHMENS



Unser Muster stellt nur einen Anhaltspunkt dar und vermag eine fachkundige Beratung, etwa durch einen Rechtsanwalt oder Notar, nicht zu ersetzen.

Bitte verwenden Sie für den Ausdruck des Dokuments die Standardeinstellungen Ihres Druckers. Es sind keine Seitenanpassungen oder Verkleinerungen des Druckbereichs erforderlich.

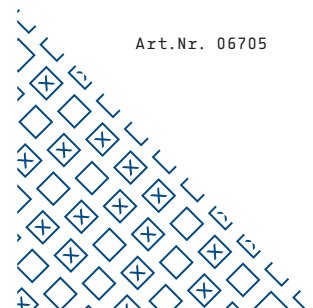
© 2008. Alle Rechte liegen bei der Formblitz AG, Berlin.

Nachdruck, Vervielfältigung und Verbreitung bedürfen der Zustimmung der Formblitz AG.

Diesen Vordruck sowie weitere Formulare und Musterverträge zum Download erhalten Sie auf

www.formblitz.de

IT-NOTFALLPLAN – SICHERN SIE DATEN, TECHNIK UND SYSTEM IHRES UNTERNEHMENS



Stellen Sie sich vor, durch plötzlichen Stromausfall werden Festplatten in Ihrem Unternehmen zerstört und vertrauliche Informationen sowie Kundenstammdaten gehen verloren. Oder durch einen Brand flutet die Feuerwehr ihr Büro, der Serverraum ist stark beschädigt und Sie sollen die IT möglichst schnell wieder in Funktion setzen. Wo fangen Sie an? Wen informieren Sie? Was ist wie zu tun? Ein IT-Notfallplan ist eine Handlungsanleitung mit der Sie sofort auf solche oder andere Szenarien reagieren können.

Sicherlich können Sie Beschädigungen oder Zerstörungen durch „höhere Gewalt“ nicht verhindern. Dennoch werden Sie Ihr Unternehmen schützen und den Betrieb mit so geringen Verlusten wie möglich aufrechterhalten oder wiederherstellen wollen.

Ein Notfallplan ist mehr als nur eine Verhaltensanweisung für Mitarbeiter. Durch solch einen Plan und ein IT-Notfallteam stellen Sie sicher, dass IT-Ereignisse schnell identifiziert und Schäden sofort eingegrenzt oder behoben werden. Des Weiteren gewährleisten Sie als Unternehmer oder IT-Leiter eine zeitgerechte Information der wichtigsten Personen und ermöglichen somit eine schnelle Reaktion auf Störungen und Notfälle.

Mit einem Notfallplan gehen Sie professionell mit IT-Ereignissen um, demonstrieren Zuverlässigkeit und stärken so den Ruf Ihres Unternehmens.

Bei der Notfallplanung geht es jedoch nicht um die Reparatur von einzelnen nicht richtig oder ungenügend funktionierenden Geräten, wie Laptops oder Drucker. Unter einem IT-Notfall ist ein schwerwiegendes Ereignis, wie der Ausfall oder Störungen von IT-Dienstleistungen bzw. ein Angriff auf diese Dienstleistungen zu verstehen, das schnellstmöglich behoben werden sollte.

Mit diesem Kurzatgeber bekommen Sie eine Anleitung zu Hand, mit der Sie einfach und schnell einen Notfallplan erstellen

1. NOTFALLVORSORGE TREFFEN

Bevor es zu einem Notfall kommt, sollten Sie Vorkehrungen treffen, um den Datenverlust so gering wie möglich zu halten.

- ☐ Sie haben das gesamte Unternehmensnetzwerk gegen unerlaubten Zugriff von außen abgesichert.
- ☐ Sie verwenden aktuelle Antiviren und Antispyware-Lösungen.
- ☐ Sie haben mechanische und Software-Firewalls eingebaut.
- ☐ Sie haben angewiesen, dass regelmäßig Backups mit gestützter Datensicherungssoftware erstellt werden.
- ☐ Sie lassen regelmäßig die Internetzugänge und den E-Mail-Verkehr (Dialerschutz) überprüfen.
- ☐ Sie achten darauf, dass Garantien, Wartungsverträge und Versicherungen regelmäßig erweitert und aktualisiert werden.
- ☐ Eine kurzfristige Wiederbeschaffung von kritischen Komponenten ist gesichert.
- ☐ Es gibt ein Lager für typische Verschleißteile (z.B. Lüfter, Netzteile, Sicherungsmedien etc.).

- ☐ Es gibt genügend Mitarbeiter, die typische Verschleißteile austauschen können.
- ☐ Wichtige oder gar alle Räume sind mit Brand- und Wassermeldern ausgestattet.
- ☐ Es gibt räumlich Ausweichmöglichkeiten für Prozesse und IT-Komponenten, in denen nach einem Notfall weiter gearbeitet werden kann und der Betrieb aufrechterhalten wird.
- ☐ Es gibt Maßnahmen zum eingeschränkten IT-Betrieb (Notbetrieb).
- ☐ Es gibt regelmäßige Schulungs- und Informationsveranstaltungen, in denen das Sicherheitsbewusstsein gestärkt und das Verhalten im Notfall geplant wird.
- ☐ Ähnlich den Evakuierungsübungen zum Brandfall sollten Sie Notfallübungen durchführen. So können Ihre Mitarbeiter lernen, wie sie reagieren müssen. Mögliche Notfallübungen sind
 - ☐ Serverausfall
 - ☐ Stromausfall
 - ☐ Hackerangriff
 - ☐ Ausfall sämtlicher Onlineverbindungen
 - ☐ Lokaler Brand im Serverraum
 - ☐ Probealarm zur Überprüfung der unterschiedlichen Benachrichtigungsketten

2. GEFAHREN UND RISIKEN ANALYSIEREN

- ☐ Damit Sie sich auf Notfälle vorbereiten und Vorsorge treffen können, sollten Sie sich bewusst machen, welche Gefahren Sie bzw. Ihr Unternehmen bedrohen könnten.
- ☐ Sie haben alle potentiellen Gefahren, die die Sicherheit des IT-Systems Ihres Unternehmens bedrohen könnten, aufgeschrieben.
- ☐ Sie haben das IT-System Ihres Unternehmens in Bereiche eingeteilt:
 - ☐ Computernetzwerk
 - ☐ Internet
 - ☐ Kommunikationseinrichtungen
 - ☐ Stromversorgungseinrichtungen
 - ☐ Kühlsysteme
- ☐ Sie haben für die von Ihnen bestimmten IT-System-Bereiche verschiedene Bedrohungen und Notfälle definiert.
 - ☐ lokale und komplette Stromausfälle
 - ☐ lokale Brände und Großbrände

- ☐ lokale Wasserrohrbrüche, großflächige Wassereinträge und Unwetterschäden (Sturm, Hagel, Blitzeinschlag)
- ☐ Explosion
- ☐ Sabotageakt
- ☐ Einbruch/Diebstahl
- ☐ Vandalismus
- ☐ Streik/Demonstration
- ☐ Ausfall der Datenfernübertragungseinrichtung
- ☐ Weil Beschädigungen verschiedener Einheiten verschieden behoben werden, haben Sie die IT-Einheiten wie folgt eingeteilt:
 - ☐ mobile Geräte
 - ☐ Server
 - ☐ Netzwerksegmente
 - ☐ das komplette lokale Netzwerk (LAN)
 - ☐ WLAN-Verbindungen
 - ☐ externe Internetserver und die Internetanbindung
 - ☐ WAN-Verbindungen
- ☐ Sie haben die einzelnen Gefahren, die Technik und System Ihres Unternehmens bedrohen, in Gefahrenstufen (z.B. hoch, mittel, niedrig) eingeteilt und ihnen Gefahrenklassen (z.B. Fehler, Problem, Notfall) zugeordnet. So überblicken Sie schnell die Gefahrenlage und können Gefahrenschwerpunkte leichter erkennen.
- ☐ Sie haben potentielle Risiken genau analysiert und aufgelistet, mit welchen Folgen bei Fehlern, Problemen und Notfällen gerechnet werden muss.
- ☐ Sie haben die wichtigsten IT-Anwendungen und Prozesse identifiziert und bestimmen dann, wie lange diese ohne negative Konsequenzen ausfallen dürfen.

3. LÖSUNGSHANDBUCH: STÖRUNGEN, FEHLER UND PROBLEME BEHEBEN

Ist ein Notfall eingetreten, benötigen Sie einen Leitfaden, an dem Sie sich schnell und lösungsgerecht orientieren können.

- ☐ Sie haben die Verfügbarkeit von Personen und technischen Geräten analysiert, durch deren Einsatz Probleme, Fehler und Notfälle schnell behoben werden können.
- ☐ Sie haben die Analysen, deren Ergebnisse und Lösungen zusammengefasst, so dass Sie einen detaillierten Lösungskatalog für Fehler, Probleme und Notfälle zur Hand haben.
- ☐ Sie haben die Ergebnisse niedergeschrieben und genaue Handlungsanweisungen für die Lösung des jeweiligen

Fehlers, Problems oder Notfalls formuliert.

- ☐ Sie haben bei der Formulierung und Zuordnung der Handlungsanweisungen darauf geachtet, dass diese den Fähigkeiten und dem Kenntnisstand des jeweiligen Fachpersonals und Mitarbeiters entspricht.
- ☐ Je nach Ereignis, d.h. einfaches Problem oder komplexer Notfall, haben Sie den Detaillierungsgrad Ihrer Handlungsanweisung angepasst.
- ☐ Ihre Lösungen und Handlungsanweisungen reichen je nach Ereignis von einem Neustart bei Programmabsturz bis zur Evakuierung im Katastrophenfall.
- ☐ Sie haben für Ihre Handlungsanweisung ein Grundschema formuliert, das Sie einmal gewählt überall einsetzen (z.B. „Was tun, wenn...“ oder „Wenn..., dann...“).

4. DAS NOTFALLTEAM AUFSTELLEN

Mit einem Notfallteam, das sich aus freiwilligen Mitarbeitern aber auch aus externen Fachleuten zusammensetzt, stellen Sie sicher, dass Notfälle und Störungen kompetent gelöst werden.

- ☐ Sie haben Ansprechpartner für verschiedene Notsituationen, das Notfallteam, festgelegt und klare Regeln für deren Zuständigkeit und Erreichbarkeit definiert.
- ☐ Das Notfallteam wird sich mindestens aus Personen mit den folgenden Fachkompetenzen zusammensetzen:
- ☐ Spezialisten für das Datennetzwerk (Netzwerksicherheit, Router, Switch etc.)
- ☐ Systemspezialisten für alle im Unternehmen eingesetzten Systeme (Windows, Unix, Macintosh etc.)
- ☐ Datenbankspezialisten
- ☐ Applikationsspezialisten für alle strategisch wichtigen Dienstleistungen
- ☐ Personen mit Erfahrung in Dokumentation und Reporting
- ☐ Personen mit Erfahrung in Logistik
- ☐ Vor Eintritt eines Notfalls werden dem Notfallteam folgende Hilfsmittel und Arbeitsunterlagen verfügbar gemacht:
 - ☐ Liste aller Kontakte (E-Mail-Adressen, Telefonnummern, Faxnummern etc.)
 - ☐ Kommunikationsmittel (Telefon, Fax etc.)
- ☐ Intakte Computer mit Netzwerk, Internetzugang und eine unabhängige Stromversorgung (Generator)
- ☐ Arbeitsraum mit Büromaterial für die Einsatzleitung
- ☐ Unterlagen über die Infrastruktur Ihres Unternehmens (Netzwerke, Strom, Telefon etc.)
- ☐ Mit dem Aufstellen von Bereitschaftsplänen haben Sie sichergestellt, dass im Notfall immer ein autorisierter und zuständiger Mitarbeiter erreichbar ist.

5. DEN NOTFALLPLAN VERBINDLICH MACHEN

Damit nicht in einer Abteilungsecke verschwindet und sich alle Mitarbeiter an die Vorsorgemaßnahmen und Regeln halten, machen Sie den Notfallplan verbindlich und für alle zugänglich.

- ☐ Indem Sie den Notfallplan nicht nur online veröffentlichen oder per E-Mail versenden sondern auch ausgedruckt aushängen, haben Sie dafür gesorgt, dass er für alle immer zugänglich ist.
- ☐ Sie haben den Notfallplan verbindlich gemacht, indem Sie ihn in die Sicherheitsrichtlinien Ihres Unternehmens integrieren.
- ☐ Sie haben einen Notfallverantwortlichen ernannt, der regelmäßig den Notfallplan aktualisiert und darüber Bericht erstattet.