Notfallplan

Definition Notfall

Ein Notfall ist ein unerwünschtes, zeitlich nicht vorhersehbares Ereignis, das den Geschäftsbetrieb nachhaltig gefährden kann. Zur Bewältigung des Notfalls im Falle eines Notfalls gelten die nachfolgenden Richtlinien mit dem Zweck, den Geschäftsbetrieb aufrechtzuerhalten bzw. unverzüglich wieder einen Zustand einer funktionsfähigen IT-Infrastruktur herzustellen.

Generelles Verhalten

Beim Auftreten eines Notfalles ist ein besonnenes Vorgehen besonders geboten. Vorrangig ist in einem Notfall Ruhe zu bewahren. Die Situation ist unverzüglich zu analysieren, und der Meldeplan ist unbedingt einzuhalten.

Bei einem reinen Verdacht auf Unregelmäßigkeiten, die auf einen Notfall oder sich ankündigenden Notfall hindeuten, ist in jedem Fall der Vorgesetzte und im Zweifel auch die IT-Abteilung zu informieren.

Feuer

In allen Räumen, in denen sich IT-Systeme befinden, die für den laufenden Geschäftsbetrieb zwingend erforderlich oder kritisch sind, sind Rauchmelder und/oder Brandmeldeanlagen in Betrieb.

Darüber hinaus befinden sich in allen Gebäuden an mehreren Stellen die erforderlichen Feuerlöscher. Diese sind gut sichtbar angebracht und im Bedarfsfall zu nutzen. Im Falle eines Brandes ist zudem unverzüglich die Feuerwehr zu informieren.

Ferner sind der Vorgesetzte, die IT-Abteilung und das Datenschutz- und Informationssicherheitsteam (DST) sofort zu informieren.

Im Falle eines größeren Brandereignisses werden die Beschäftigten an den jeweiligen Betriebsstätten umgehend evakuiert. Fluchtwegepläne hängen in jedem Gebäude an gut sichtbarer Stelle aus.

Wasser

Größere Wasserschäden, die die für den Geschäftsbetrieb erforderlichen, kritischen IT-Systeme negativ beeinträchtigen könnten, stellen an allen Betriebsstätten aufgrund der Lage nur ein sehr geringes Risiko dar. Es ist regelmäßig nicht damit zu rechnen, dass ein Wasserschaden zu einer Beeinträchtigung der kritischen IT-Systeme führt. Die IT-Systeme befinden sich an Orten, an denen

kein Hochwasser zu befürchten ist. Auch Schäden durch Wasserleitungen sind aufgrund der räumlichen Gegebenheiten äußerst unwahrscheinlich.

Sollte dennoch ein Wasserschaden auftreten, der eine Gefahr für die kritischen IT-Systeme oder andere IT-Systeme darstellen könnte, sind sofort der Vorgesetzte und die IT-Abteilung zu informieren. Diese werden dann nach Sichtung der Lage eine Risikobewertung und die weiter erforderlichen Maßnahmen vornehmen.

Stromausfall

Alle kritischen IT-Systeme, die für den Geschäftsbetrieb unerlässlich sind, verfügen über eine unterbrechungsfreie Stromversorgung (USV).
Diese tragen Sorge dafür, dass Stromausfälle von mehreren Minuten überbrückt und im Falle eines längeren Stromausfalls die IT-Systeme geordnet heruntergefahren werden können, um die Integrität der Daten zu gewährleisten.

Der wesentliche Teil der kritischen IT-Systeme befindet sich in einem Rechenzentrum, das über Generatoren mit alternativer Stromerzeugung im Falle eines Stromausfalls verfügt und so auch bei längeren Stromausfällen eine Verfügbarkeit der IT-Systeme gewährleistet.

Ausfall von IT-Systemen

Alle kritischen IT-Systeme unterliegen einem Monitoring, mit dem die Verfügbarkeit und etwaige Störungen überwacht werden.

Im Falle eines Ausfalls wird der diensthabende IT-Mitarbeiter automatisch informiert. Dieser wird unverzüglich den Vorfall prüfen und bei nicht nur kurzen, vorübergehenden Störungen unverzüglich den Vorgesetzten informieren.

Der Grund für den Ausfall ist umgehend zu beheben. Bei kritischen IT-Systemen ist Sorge dafür zu tragen, dass immer ausreichend Ersatzteile und/oder Ersatzsysteme vorrätig sind, mit denen der Ausfall kurzfristig überbrückt bzw. beseitigt werden kann.

Angriffe von außen

Alle Server-IT-Systeme und alle kritischen IT-Systeme werden durch Firewall-Technologie gesichert und überwacht. Ein Zugriff unbefugter Dritter von außen wird auf diese Weise wesentlich erschwert. Die Firewall-Technologie wird regelmäßig gewartet und aktualisiert, um eine Anpassung an neue Gefahrenlagen zu gewährleisten.

Einbruch und Diebstahl

Alle Büro- und Geschäftsräume sind vor dem Zutritt unbefugter Dritter gesichert. Dies gilt insbesondere für den Zutritt zu Gebäuden außerhalb der Büro- und Geschäftszeiten.

Alle kritischen IT-Systeme befinden sich in besonders gesicherten Räumlichkeiten (z.B. Rechenzentren), die nur nach entsprechender Authentifizierung betreten werden können.

Für den Fall, dass ein Einbruch und/oder ein Diebstahl von IT-Systemen bemerkt wird, hat er jeweilige Mitarbeiter unverzüglich den Vorgesetzten sowie die IT-Abteilung zu informieren.

Ausfall von IT-Administratoren

Im Unternehmen verfügen zwar nur wenige Personen über Administrator-Rechte. Diese Personen sind entsprechend geschult und ausgebildet. Im Falle eines Ausfalls eines IT-Administrators (z.B. durch Krankheit) ist Sorge dafür getragen worden, dass mindestens ein weiterer Mitarbeiter mit Administrator-Rechten sofort erreichbar ist, um ggf. erforderliche Administrator-Handlungen durchzuführen.

Notfall-Verantwortlicher

Im Unternehmen gibt es einen Notfall-Verantwortlichen, der bei Vorliegen eines Notfalles für die Veranlassung der jeweils vorgesehenen und gebotenen Maßnahmen verantwortlich ist.

Hierbei handelt es sich um den Informationssicherheitsbeauftragten.

Wiederanlaufplan

Die IT-Abteilung trägt Sorge dafür, dass für kritische IT-Systeme stets die erforderlichen Ersatzteile bzw. Alternativsysteme vorrätig sind und Wiederanlaufpläne vorliegen. Die Wiederanlaufpläne sind in jedem Fall auch in Papierform zu dokumentieren und an einer Stelle zu hinterlegen, die im Falle eines Notfalls schnell zugänglich ist und sicherstellt, dass die in den Wiederanlaufpläne aufgezeigten Aktionen unverzüglich begonnen werden können.

Im Falle eines Funktionsausfalles eines IT-Systems wird die Ursache des Vorfalls unverzüglich untersucht. Parallel dazu werden sofort Maßnahmen in die Wege geleitet, um einen Wiederanlauf des IT-Systems oder eines Alternativsystems kurzfristig zu ermöglichen.

In der IT-Abteilung werden alle verantwortlichen Personen dahingehend geschult, Funktionsauswahl zu untersuchen und ein Wiederanlaufen der kritischen IT-Systeme schnellstmöglich vorzunehmen. Dabei ist in besonderer Weise dafür Sorge zu tragen, dass die Integrität der Daten gewährleistet ist.

Adressliste / Meldeliste

Hier finden Sie eine Übersicht der verantwortlichen Personen für die genannten Bereiche:

Name / Rufbereitschaft	Telefon (intern)	Handy/Privat-Nr.	Funktion/Bemerkung
Frank Hochdorfer	21	0162-9126323	Notfallverantwortlicher / Informationsicherheitsbeauftragter /IT-Leiter
Ralf Gebhard	13	0172-9723690	IT-Leiter, Geschäftsführer