CHECKLISTE

IT-Notfallplan

IT-Systeme sind in den letzten Jahren ausfallsicherer geworden. Dennoch kann es jederzeit zu schwerwiegenden Fehlern und Problemen kommen. Diese bedeuten im Extremfall den Verlust sämtlicher Unternehmensdaten. Auslöser kann z. B. ein Stromausfall, aber auch eine simple Fehlbedienung sein.
Das Gefahrenspektrum reicht von

- Hard- und Softwarefehlern, über
- Bedienungsfehler,
- Viren- und Schadprogramme, die über das Internet in das IT-System gelangen, bis hin zu
- Stromausfall, Wasserschäden, Brand oder Naturkatastrophen.

Obwohl ein Grundschutz der IT-Systeme und deren einzelner Komponenten gegen Bedrohungen aus dem Internet mittlerweile obligatorisch ist, werden viele andere Aspekte der Datensicherheit immer noch sträflich vernachlässigt. Es fehlt an angemessenen Sicherheitsrichtlinien, Datensicherungen werden nur sporadisch und ohne umfassendes Konzept durchgeführt und eine Notfallplanung ist oft gar nicht vorhanden. Wie notwendig aber gerade eine Notfallplanung gewesen wäre, zeigt sich oft erst, wenn der Ernstfall eingetreten ist.

In vielen kleineren Unternehmen sind die Mitarbeiter mehr oder weniger auf sich gestellt, wenn es Probleme mit der Datensicherheit gibt. Deshalb sind gerade hier **„Was tun, wenn...“-Anleitungen** wichtig. Hier ist genau festgelegt, was im Notfall zu tun und wer zu verständigen ist.

PRAXIS-TIPP:

- Im Idealfall liegt an jedem Computerarbeitsplatz eine Notfallbroschüre, in der alle möglichen Fehler und Katastrophen aufgelistet und mit konkreten Handlungsanweisungen versehen sind. Außerdem sind Mitarbeiterschulungen und Informationsveranstaltungen zu Datensicherheitsthemen von zentraler Bedeutung.
- Ziehen Sie Kollegen zu Rate und scheuen Sie sich nicht, auch fremden Sachverstand in Anspruch zu nehmen, um Ihren Notfallplan für die Datensicherheit so umfassend wie irgend möglich abfassen zu können. Als Planungsgrundlage benötigen Sie eine aktuelle Dokumentation und/oder einen aktuellen Strukturplan sämtlicher IT-Einrichtungen.

Anweisung	Erledigt ✓	Anmerkung
Beantworten Sie zunächst die Leitfrage: **Was kann alles passieren?** Listen Sie dann **alle potenziellen Gefahren** auf, die die Sicherheit und die Integrität des vorhandenen IT-Systems (Computernetzwerk, Internet, Kommunikationseinrichtungen) bedrohen. Es hat sich bewährt, dass Sie dabei von klein nach groß vorgehen, also mit einem Arbeitsplatz-PC beginnen und dann folgende Bereiche betrachten: • mobile Geräte • Server • Netzwerksegmente • das komplette lokale Netzwerk (LAN) • WLAN-Verbindungen • externe Internetserver und die Internetanbindung • WAN-Verbindungen		
Listen Sie dann die äußeren Bedrohungen und Notfälle auf. Denken Sie dabei besonders an folgende Bereiche: • Lokale und komplette Stromausfälle • Andauernder Ausfall der Internetverbindungen • Lokale Brände und Großbrände • Lokale Wasserrohrbrüche und großflächige Wassereinbrüche • Unwetterschäden (z. B. Sturm, Hagel, Blitzeinschlag) • Allgemeine Katastrophen (z. B. Gasexplosion, Sabotageakt)		
Beantworten Sie dann die nächste Leitfrage: **Wie hoch ist die Gefahr einzustufen?** Teilen Sie dazu die Gefahren in unterschiedliche **Gefahrenklassen** ein, z. B. Fehler, Problem, Notfall. Sie erhalten dadurch sehr schnell ein genaues Bild über die Gefahrenlage und können Gefahrenschwerpunkte sehr leicht ausmachen.		
Fertigen Sie eine genaue **Risikoanalyse** an. Aus dieser geht vor allem hervor, wie wahrscheinlich ein Fehler/Problem/Notfall ist und mit welchen konkreten Folgen gerechnet werden muss.		
Stellen Sie eine **Verfügbarkeitsanalyse** an und legen Sie fest, wie schnell bestimmte Probleme gelöst werden müssen.		
Fassen Sie die Ergebnisse der unterschiedlichen Analysen zusammen und fertigen Sie einen **detaillierten Katalog mit Lösungsmöglichkeiten** für die unterschiedlichen Fehler/Probleme/Notfälle an.		

Anweisung	Erledigt ✓	Anmerkung
Lassen Sie all Ihre Erkenntnisse in **schriftliche Handlungsanweisungen** für die unterschiedlichen Fehler/Probleme/Notfälle münden. Achten Sie dabei darauf, dass tatsächlich das gesamte Gefahrenspektrum abgedeckt wird und die Handlungsanweisungen dem Kenntnisstand und den Fähigkeiten der jeweiligen Adressaten angemessen sind (Fachpersonal, normale Mitarbeiter). Je nach den lokalen Erfordernissen sind bei den Handlungsanweisungen **unterschiedliche Detailgrade** möglich. Die Bandbreite reicht dabei von der einfachen Meldung eines Problems bis hin zu seitenlangen exakten Detailanweisungen zur konkreten Problemlösung. Genauso weit gefasst ist auch die Themenbreite, die etwa vom einfachen Programmabsturz und Datenverlust auf einem Arbeitsrechner bis hin zu Evakuierungsmaßnahmen im Katastrophenfall reicht. Wichtig ist, dass jede Handlungsanweisung dem Grundschema **„Was tun, wenn...“** folgt und tatsächlich jede notwendige Maßnahme berücksichtigt.		
Legen Sie **Ansprechpartner für unterschiedliche Notsituationen** fest und treffen Sie klare Regelungen für deren Zuständigkeit und Erreichbarkeit.		
Stellen Sie **Bereitschaftspläne** auf und treffen Sie **Bereitschaftsvereinbarungen mit Vertreterlösungen**, die sicherstellen, dass in Notfällen immer autorisierte und zuständige Mitarbeiter erreichbar sind.		
Legen Sie den Notfallplan und damit verbundene Handlungsanweisungen verbindlich fest (z. B. **Betriebsvereinbarung**) und sorgen Sie dafür, dass dieser immer zugänglich ist. Veröffentlichen Sie den Notfallplan daher nicht nur online (z. B. via Intranet), sondern händigen Sie ihn **in gedruckter Form** aus und legen Sie ihn zusätzlich noch an besonders gekennzeichneten Punkten aus – am besten auch an jedem PC-Arbeitsplatz.		
Integrieren Sie den Notfallplan in die **Sicherheitsrichtlinien** Ihres Unternehmens.		
Benennen Sie einen **Notfallplanverantwortlichen**, der für zeitnahe Aktualisierungen (z. B. Pflege der Benachrichtigungsketten und Bereitschaftspläne) und als zentraler Koordinator zuständig ist und regelmäßig (z. B. fester Monatstermin) berichtet.		

Anweisung	Erledigt ✓	Anmerkung
Nutzen Sie die Gefahrenanalyse für die **Notfallvorsorge**. Beachten Sie bei der **Planung der Vorsorgemaßnahmen** unter anderem folgende Aspekte: • Planen Sie die kurzfristige Wiederbeschaffung von kritischen Komponenten. • Legen Sie ein Lager mit typischen Verschleißteilen an (z.B. Lüfter, Prozessorkühler, Netzteile, Sicherungsmedien) und sorgen Sie dafür, dass genügend Mitarbeiter diese Verschleißteile austauschen können. • Lassen Sie wichtige Räume mit Brand- und Wassermeldern ausstatten und sichern. • Verbessern Sie die Zugangskontrollen (Türöffner, Pförtnersystem, Besucherbegleitung etc.). • Planen Sie Ausweicharbeitsräume und Arbeitsszenarien und legen Sie die Mindestanforderungen für die dann notwendige IT-Infrastruktur fest (Day-after-Planung). • Sorgen Sie für regelmäßige **Schulungs- und Informationsveranstaltungen** zum Thema IT-Notfälle, um das allgemeine Sicherheitsbewusstsein zu stärken und ein planvolles Handeln in Notsituationen zu ermöglichen.		
Proben Sie den Ernstfall und halten Sie **Notfallübungen** ab. Lassen Sie unterschiedliche Szenarien regelmäßig üben, damit Ihre Mitarbeiter lernen, bei tatsächlichen Problemen und Notfällen möglichst optimal zu reagieren. Diese Katastrophenübungen können sehr gut mit Übungen zur Datenwiederherstellung kombiniert werden. Mögliche Szenarien wären z. B.: • Serverausfall • Stromausfall • Hackerangriff • Ausfall sämtlicher Online-Verbindungen • Lokaler Brand im Serverraum • Probealarm zur Überprüfung der unterschiedlichen Benachrichtigungsketten		

TIPP:
Damit Sie in einem Notfall schnell wieder auf Ihre Daten zugreifen können, empfiehlt es sich, eine Sicherung davon anzulegen. Mit Lexware datensicherung online werden die Daten aus Ihren Lexware Produkten in einem Hochsicherheitszentrum gesichert. So sind sie auch vor einem Brand oder einem Wasserschaden optimal geschützt.

Autor: Lexware Redaktion
Quelle: www.lexware.de/wissen-tipps