

EDV Notfallplan - ein Praxis-Test

Machen Sie einen kurzen Test!

Schildern Sie verschiedenen Mitarbeitern der EDV-Abteilung den Fall, „daß sämtliche Daten auf Ihren Servern unlesbar sind“ und fragen Sie nach möglichen Wegen zur Vorgehensweise für die Wiederherstellung.

Erhalten Sie mehrere, möglicherweise unterschiedliche oder gar gegensätzliche Reaktionen und Meinungen zur Vorgehensweise? In diesem Fall ist die Ausarbeitung und Umsetzung eines EDV Notfallplans empfehlenswert.

Wozu ein EDV Notfallplan?

Ein EDV Notfallplan dient als Leitfaden für den akuten Schadensfall (z.B. Datenverlust, nicht autorisierter Zugriff, physische Zerstörung) und soll Ihnen und Ihren Mitarbeitern helfen, den Überblick im Notfall zu behalten.

Der Notfallplan enthält in einer komprimierten Form Kontaktinformationen, Verfahren und Anweisungen, Übergangsprozesse sowie Definitionen für die Erstmaßnahmen für den Übergang in den operativen Betrieb.

Was kostet die Erstellung eines Notfallplans?

Die Ausarbeitung, Einführung und Pflege eines EDV Notfallplans kostet Zeit und Geld. Oft sind auch - als Konsequenz der Planung zusätzliche Investitionen in Hard- und Software erforderlich. Ein derartiges Unterfangen erfordert eine genaue Analyse, welche Teile Ihrer EDV in welchem Umfang für Ihren täglichen operativen Betrieb wichtig sind. Beispiele dazu:

Welche direkten und indirekten Kosten entstehen, wenn Ihre komplette EDV für einen Arbeitstag nicht zur Verfügung steht? Berechnen Sie neben den direkten Kosten für den Auftragsstillstand auch die unproduktive Zeit der Mitarbeiter sowie entgangene Kundenaufträge (falls es eine Abhängigkeit zum EDV-System gibt) sowie eventuelle Folgekosten mit ein.

Welche EDV-Systeme in Ihrem Unternehmen sind als betriebskritisch einzustufen und müssen zukünftig durch einen Notfallplan abgesichert werden?

Welcher Aufwand ist für eine Absicherung durch einen Notfallplan aus Ihrer Sicht angemessen?

Ein Beispiel: Brand im Serverraum

Das nachfolgende Beispiel dient als Anregung und ist nicht zur Nachahmung gedacht. - Nach einem Brand im Serverraum eines mittelständischen Unternehmens empfehlen wir folgende wesentliche Schritte zur Wiederaufnahme des operativen Betriebs:

1. Stellen Sie ein Team mit den wichtigsten Personen (z.B. aus organisatorischer, rechtlicher und technischer Sicht) zusammen.
2. Stellen Sie fest, welche Daten und Systeme aus externen Beständen verfügbar sind. Versuchen Sie nicht, beschädigte Server wieder in Betrieb zu nehmen und überlassen Sie die Datenwiederherstellung Spezialisten.
3. Schätzen Sie den Gesamtschaden sowie die Wiederherstellungsdauer und -kosten ab und kommunizieren Sie die wesentlichen Schlüsselinformationen an die betroffenen Abteilungen oder Organisationen.
4. Halten Sie sich an Ihren Notfallplan für die Wiedereinbetriebnahme. Falls Sie keinen Notfallplan haben, definieren Sie jetzt die Vorgehensweise, wie und in welchem Umfang Serverdienste und Daten wieder bereitgestellt werden müssen, um einen operativen Betrieb des Unternehmens sicherzustellen. Nehmen Sie hierfür bei Bedarf externe Spezialisten hinzu.
5. Halten Sie Ihre Schlüsselpersonen für die Kommunikation auf dem laufenden Stand und berichten Sie, zu welchem Zeitpunkt mit einer Wiederaufnahme des Betriebs gerechnet werden kann.
6. Führen Sie die Wiedereinbetriebnahme schrittweise durch und halten Sie die Kommunikation zu den Fachabteilungen aufrecht um Feedback zu erhalten.
7. Protokollieren Sie die aufgetretenen Schäden und die Vorgehensweise zur Behebung zur Optimierung Ihres Notfallplans.

Dieses Beispiel dient nur zur Orientierung für einen möglichen Notfall. Neben der Gefahr durch Brand, Hackerangriffe und Sabotage existieren auch ganz alltägliche Vorfälle, die sich schnell zu kostspieligen Notfällen entwickeln können: z.B. ein einfacher Hardwaredefekt an einer neuralgischen bzw. zentralen Stelle.

Vorgehensweise zur Erstellung eines Plans

1. Halten Sie fest, welche EDV Dienste und Richtlinien wichtig für Ihren Betrieb sind und priorisieren Sie diese (z.B. Schutz der Buchhaltungsdaten ist wichtiger als der VPN-Remote-Zugriff).
2. Definieren Sie mögliche Notfall-Zustände (z.B. Serverabsturz, Datenverlust, physische Zerstörung, Stromausfall)
3. Schätzen Sie das Gefährdungspotential und die Wahrscheinlichkeit ein und priorisieren Sie die Notfall-Zustände
4. Erstellen Sie eine Matrix für jeden EDV-Dienst (Punkt 1) in Zusammenhang mit dem Eintritt eines möglichen Notfalls.
5. Definieren Sie, woran ein Notfall erkannt wird. Ein kurzfristiger Serverausfall ist in der Regel kein Notfall. Prüfen Sie interne SLA's (Service Level Agreements) und orientieren Sie sich an den Schwellen-werten. Beispiel: ein Notfall ist eingetreten, wenn ein Mail-Server a) innerhalb von 4 Stunden und b) nach der Einleitung einfacher Fehlerbehebungen nicht wieder betriebsbereit ist.
6. Definieren Sie einen festen Ansprech-partner für jeden Notfall, sowie eine weitere Person als Vertretung
7. Legen Sie die Kommunikations-Reihenfolge fest (Wer informiert wen in welcher Reihenfolge).
8. Definieren Sie, wie der Wiedereintritt in den Normalbetrieb gestaltet werden soll (z.B. Aktivierung des Ausfallservers und Wiederherstellung der letzten Datensicherung, danach Kommunikation über einen definierten Kanal)
9. Halten Sie fest, wie die Protokollierung während eines Notfalls aussehen soll.

Weniger ist mehr

Achten Sie bei der Erstellung eines Notfallplans auf einfache, beschreibende Sätze und erstellen Sie verständliche Schaubilder. Verzichten Sie auf aufwendige Formulare und akribisch ausgefeilte Prozessabläufe. Weniger ist in diesem Fall mehr. Spätestens im Falle eines eingetretenen Notfalls wird sich in der Regel kein Mitarbeiter mit einem Notfallhandbuch hinstellen und lesen, was er denn nun zu tun hat. Deshalb:

Testen Sie Ihren Notfallplan

Prüfen Sie Ihren Notfallplan mit plausiblen und einfachen Tests. Wichtig: Immer ausserhalb der Betriebszeiten, immer in Absprache mit dem Kunden, dem Vorgesetzten oder der Geschäftsleitung. Das nachfolgende Beispiel ist als Anregung und nicht zur Nachahmung gedacht. Die Firma Service Kiosk IT Consulting GmbH wird keine Forderungen aus Schäden durch Nachahmung übernehmen.

„Stromausfall durch Fremdverschulden“

Bei Renovierungsarbeiten wird ein wichtiges Stromkabel zum Serverraum getrennt. Simulieren Sie diesen Fall durch „Abschalten der Sicherung zum Serverraum“ auf dem Papier und prüfen Sie folgende Beispiel-Punkte:

1. Welche Server sind für den Betrieb wichtig?
2. Zu welchem Zeitpunkt wird der Ausfall festgestellt?
3. Wer meldet den Ausfall an wen?
4. Verfügen alle, bzw. die wichtigen Server über eine USV (Unterbrechungsfreue Stromversorgung)?
5. Wie lange hält die Stromversorgung über die USV?
6. Welche alternativen Stromquellen können für die Aufrechterhaltung des Serverbetriebs genutzt werden? (Generator, redundanter Stromkreislauf, Nebengebäude)
7. Werden die Server vor dem Ausfall der USV ordnungsgemäß heruntergefahren (Dienste und Applikationen beenden, Datenbankdienste herunterfahren, Betriebssystem abschalten)?
8. Gibt es Abhängigkeiten für das Herunterfahren der Server?
9. Welche Vorgehensweise wird verfolgt, falls der Strom länger als x Stunden ausbleibt?
10. Existiert die Möglichkeit, die Server in separaten Räumlichkeiten wieder in Betrieb zu nehmen?
11. Falls der Notfall-Umstand behoben wurde: In welcher Reihenfolge werden die Server wieder in Betrieb genommen?
12. Welche Methoden werden verwendet, um die Server auf Datenverluste zu prüfen?

Fazit

Dieses Beispiel zeigt wenige Punkte auf, die in diesem Fall berücksichtigt werden müssen. Wichtig ist in jedem Fall, ein Notfallhandbuch nicht zu überladen. Definieren Sie pro Ereignis die wesentlichen und wichtigsten Tätigkeiten.

SERVICE KIOSK IT Consulting GmbH
Breitscheidstr. 65, 70176 Stuttgart

Ihre Ansprechpartner:

Frau Emine Tahtabasi
Herr Kay Buhlinger

Telefon +49 (0) 711 4889-020

Telefax +49 (0) 711 4889-029

E-Mail vertrieb@service-kiosk.com

www.service-kiosk.com

www.it-servicecenter.com