KANZLEI-IT

Auch Ihre Kanzlei braucht einen Disaster-Recovery-Plan

von Dipl.-Ing Wolfgang Neumann, Westerstede, www.avisara.de

| Das Thema IT-Sicherheit wird zunächst mit Trojanern, Viren oder Cyberangriffen in Verbindung gebracht. Aber neben den akuten Bedrohungen von Außen existieren auch Risiken, die banaler Natur sind, jedoch große Auswirkungen nach sich ziehen können. Am hier geschilderten Fall, der sich tatsächlich so ereignet hat, wird aufgezeigt, wie sich schon kleinere Nachlässigkeiten extrem auswirken können. |

Wasserrohrbruch in der Steuerkanzlei Esser

Kanzlei-Server steht im Wasser

Es ist ein verregneter Montagmorgen. Der Steuerberater Hubert Esser (Name geändert) betritt um 7:45 Uhr sein Büro. Irgendetwas ist anders. Auf dem Weg zu seinem Arbeitsplatz bemerkt Hubert Esser Wasserlachen vor dem Lagerraum. Er ahnt nichts Gutes. Beim Blick in den Raum sieht er das Chaos. Das Wasser steht auf dem Boden. Ein Wasserrohrbruch über der darüber befindlichen Toilette muss die Ursache sein. Aber viel schlimmer ist die Tatsache, dass der Kanzleiserver im Wasser steht. Totalschaden. Der Server lässt sich nicht mehr starten. Zwischenzeitlich treffen auch die Mitarbeiter ein. Alle sind ein wenig früher gekommen, da die Steuerfristen zwingend eingehalten werden müssen. Was nun? Hubert Esser hat zwar regelmäßig eine Datensicherung auf einem Datenträger, wenn auch sehr konservativ, durchgeführt, aber ohne Server geht nichts.

Neuen Server gibt es nur mit Lieferzeit

Der IT-Dienstleister wird kontaktiert. Es muss ein neuer Server her. Dieser ist jedoch erst in zwei bis drei Tagen lieferbar. Auch nach Lieferung kann nicht garantiert werden, dass die Konfiguration des Servers mit der Anwendersoftware unmittelbar durchgeführt werden kann.

Nur eine Reaktionszeit, aber keine Fehlerbehebungszeit vereinbart

Darüber hinaus sieht der Wartungsvertrag mit dem IT-Dienstleister auch keine festgelegte Zeit für eine Fehlerbehebung vor. Lediglich eine Reaktionszeit wurde vereinbart. Nun wird es langsam kritisch. Wie lange kann eine Steuerkanzlei ohne IT/EDV überleben? Diese Frage stellt sich Hubert Esser jetzt. Da der Server schon einige Jahre in Betrieb war und auch nur rudimentär Software-Updates durchgeführt wurden, ist es fraglich, ob die gesicherten Daten überhaupt mit der neuen und aktuellen Software kompatibel und einlesbar sind. Was, wenn nicht? Durch die unterschiedlichen Softwarestände ein durchaus denkbares Szenario.

Hubert Esser erinnert sich an die Gespräche mit seinem IT-Dienstleister. Sein Ansprechpartner hatte oft darauf hingewiesen, dass ein sogenanntes Disaster-Recovery, also das Wiederherstellen der Arbeitsfähigkeit im Notfall, durchgeführt werden sollte. Aber wie so oft klang das alles zwar plausibel und sollte auch beauftragt werden, ist aber durch den Arbeitsalltag immer wieder auf der Prioritätenliste nach unten gerutscht.

Was ist ein Disaster-Recovery?

Disaster Recovery ist ein Notfallplan

Beim Erstellen eines Disaster-Recovery oder eines Notfallplans sollten folgende Kriterien hinterfragt werden:

1. Welche Systeme sind kritisch? Wie arbeitet das Unternehmen? Welchen Stellenwert haben die Systeme und wo liegen die Prioritäten?

2. Wie lange geht es ohne IT/EDV? Wie lange kann ohne das System weitergearbeitet werden?

3. Datensicherungskonzept: Welche Systeme und Daten werden gesichert und wer hat Zugriff auf die Daten?

4. Plan B: Welche Möglichkeiten gibt es im Härtefall, um wieder arbeitsfähig zu werden? Wie kann ggf. ohne Produktivsystem weitergearbeitet werden?

RTO und RPO definieren

Es sind verschiedene Lösungen im Markt verfügbar. Eine, gerade für kleinere und mittlere Unternehmen attraktive Variante, ist eine Wiederherstellung aus der Cloud. Wichtig dabei ist, dass Kennwerte für die Wiederherstellung mit dem Anbieter definiert werden – Recovery Time Objective (RTO) und Recovery Point Objektive (RPO). RTO informiert darüber, wie lange ein System oder ein Service ausfallen darf. RPO beantwortet die Frage, wie viel Datenverlust hinnehmbar ist, also wie lange der Zeitraum ist, der zwischen zwei Datensicherungen liegen darf.

Notfallwiederherstellung als Leistung aus der Cloud

Gerade für kleinere Unternehmen eine sinnvolle Lösung

Die Notfallwiederherstellung umfasst Services aus der Cloud, mit denen sich bei einem Notfall oder einer Störung IT-Services, IT-Strukturen oder Daten wiederherstellen lassen. Hierfür stellt ein IT-Dienstleister oder Provider (z. B. Deutsche Telekom) Speicherplatz, Backup-Services, virtuelle IT-Strukturen oder virtuelle Server als Cloud-Dienstleistung zur Verfügung. Diese ermöglichen es, Notfälle abzusichern, ohne selbst zusätzliche Hard- und Software in einem eigenen Rechenzentrum bereitstellen zu müssen. Sinnvoll kann die Absicherung beispielsweise für kleinere und mittlere Unternehmen sein, die selbst nur wenig Know-how und Ressourcen für eigene Notfallmaßnahmen und -strukturen besitzen.

Wie ging es mit der Steuerkanzlei Esser weiter?

Nach vier Tagen der Anruf des IT-Dienstleisters: Server wurde geliefert, Kanzleisoftware konnte aufgespielt werden, Konfiguration ist soweit abgeschlossen. Man hat kurzerhand die neuesten Softwareversionen für die Anwendung und das Betriebssystem eingespielt. Nun wird die Datensicherung benötigt. Das Einspielen erfolgt mit der Installation vor Ort, was erst am übernächsten Tag geschehen kann.

Beim Einlesen der Datensicherung, die sich als problematisch herausstellte, kommt der nächste Schock. Die Daten konnten ausgelesen werden, aber der Datenstand war mehrere Wochen alt! Hubert Esser hatte zwar regelmäßig Datensicherungen durchgeführt, aber niemals überprüft, ob die Sicherungen auch einwandfrei durchgelaufen waren.

Letztes Sicherheits-Update war veraltet

Fazit für die Kanzlei

Eine leicht vermeidbare Situation hat zu einem großen Risiko geführt: Insgesamt ein technischer Arbeitsausfall von sechs Tagen mit nicht unerheblichen Folge- und Zeitkosten für die Aktualisierung und Wiederaufbereitung der verloren gegangenen Daten. Alle Fristen konnten nicht eingehalten werden. Das Aktualisieren der Daten erfolgte mühevoll in Kleinarbeit. Das Risiko, ob die Arbeitsfähigkeit überhaupt wiederhergestellt werden kann, war entsprechend hoch.

Teuer und vermeidbar

Was ist zu tun

IT-Sicherheit konzentriert sich nicht nur auf Viren, Cyberangriffe und Trojaner, sondern auch auf die gesamte IT-Landschaft in der Kanzlei, was sehr häufig vernachlässigt wird und, wie beschrieben, nicht kalkulierbare Risiken enthält. Grundsätzlich sollten die in der kurzen Checkliste genannten Punkte berücksichtigt werden:

Mindestregeln bei Server-Aufstellung und beim Zugang beachten

CHECKLISTE Server-Aufstellung und Zugang

- Aufstellungsort (niemals in der Nähe von (Ab-)Wasserleitungen)
- Temperaturentwicklungen berücksichtigen
- USV-Anlagen in die Stromversorgung zwischenschalten (unterbrechungsfreie Stromversorgung)
- Serverraum gegen unbefugten Zugang sichern
- Prüfen, ob die Datensicherung ordnungsgemäß durchgelaufen ist (hierzu gibt es entsprechende Lösungen) oder dies vom IT-Dienstleister remote durchführen lassen
- Wartungsverträge mit dem IT-Dienstleister regelmäßig aktualisieren und ggf. anpassen
- Konzept für ein Disaster-Recovery mit dem IT-Dienstleister erstellen, Tests durchführen und darauf basierend eine entsprechende Dokumentation erstellen (kann bereits Bestandteil einer Verfahrensdokumentation werden).

↘ WEITERFÜHRENDER HINWEIS
- Kanzlei-IT – Die Server-Umstellung professionell gestalten (Koss/Penner, KP 20, 85)