SORGFALTSPFLICHT

Zwei, die zusammengehören: EDV und Datensicherung

von Ilona Cosack, ABC AnwaltsBeratung Cosack, Mainz

| Wir alle nutzen die Vorteile der EDV, doch Gefahr droht, wenn die Technik versagt. Ein absolutes Muss für jede Rechtsanwaltskanzlei ist es daher, Daten professionell zu sichern. Schon 1996 verstand der BGH die Datensicherung als allgemein bekannte Selbstverständlichkeit (2.7.96, X ZR 64/94, Abruf-Nr. 146722). Aus einem Datenverlust resultieren in der Regel schwere wirtschaftliche Schäden für den EDV-Anwender. Der folgende Beitrag liefert ein zuverlässiges Konzept zur Datensicherung – mit den zehn Schritten der folgenden Checkliste bewahren Sie Ihre Kanzleidaten sicher auf. |

1. Für jede RA-Kanzlei unerlässlich: Konzept entwickeln

Fristenwahrung: strenge BGH-Rechtsprechung

Die Rechtsprechung des BGH zur Fristenkontrolle einer Anwaltskanzlei ist streng. Erst am 27.1.15 entschied der BGH, dass die Sorgfaltspflicht des Rechtsanwalts, der seinen Fristenkalender ausschließlich elektronisch führt, es in Fristsachen ggf. gebietet, auf eine manuelle Fristenkontrolle umzusteigen. Dies ist der Fall, wenn wegen eines technischen Defekts vorübergehend nicht störungsfrei gewährleistet ist, auf den elektronisch geführten Fristenkalender zuzugreifen (II ZB 21/13, Abruf-Nr. 175701). Im zugrunde liegenden Fall hatte die Kanzlei wegen technischer Probleme Wiedereinsetzung in die versäumte Berufungsfrist beantragt. Weil der Server komplett ausgefallen sei, habe die Berufungsbegründung nicht ordnungsgemäß bearbeitet und eingereicht werden können. Ein Unwetter habe die EDV-Anlage der Kanzlei so schwer beschädigt, dass sie mehrfach ausgefallen sei. Der BGH hat die Wiedereinsetzung in den vorigen Stand versagt. Das Verschulden der Prozessbevollmächtigten liege nicht in dem über geraume Zeit untauglichen Versuch, Überspannungsschäden am Kanzleiserver nachhaltig zu beseitigen, sondern darin, dass sie es vollständig unterlassen haben, parallel manuell zu sichern, obwohl die elektronische Fristenkontrolle unzuverlässig war.

EDV-Ausfall vorbeugen

Beachten Sie | Ein Datensicherungskonzept hilft zu verhindern, dass die EDV durch Überspannungsschaden und andere Risiken ausfällt.

Zuständige und Vertreter benennen

PRAXISHINWEIS | Legen Sie fest, wer in Ihrer Kanzlei für die Datensicherung verantwortlich und wer zuständig ist, die Maßnahmen praktisch anzuwenden. Benennen Sie für beide Bereiche auch Vertreter. Es genügt nicht, dies dem externen EDV-Dienstleister zu überlassen. Binden Sie diesen ein, verantwortlich bleibt jedoch die Kanzlei. Seit 1.7.15 ist mit § 2 BORA n. F. die bisherige Übung, externe Dienstleister für die Kanzlei arbeiten zu lassen, legitimiert. Lassen Sie jeden Dienstleister eine Verschwiegenheitserklärung unterzeichnen und holen Sie von Ihren Mandanten eine Einverständniserklärung ein, dass Sie externe Dienstleister einsetzen. Dokumentieren Sie alle Regelungen schriftlich, überprüfen Sie sie mindestens jährlich und passen Sie sie bei Bedarf an. Rekonstruieren Sie regelmäßig Ihre Daten und prüfen Sie, ob die Datensicherung auch funktioniert, damit Sie für den Fall der Fälle gewappnet sind.

2. Eigene Daten kontrollieren: intern oder extern?

Viele Kanzleien spiegeln – in bestem Glauben, dass es ausreicht – die Daten auf eine zweite Festplatte im Server oder ein externes Speichermedium, das innerhalb des Büros aufbewahrt wird. Für Extremfälle (z. B. Einbruch, Diebstahl, Vandalismus, Hochwasser, Wasserschaden durch auslaufende Spülmaschine, Brand) ist dies keine gute Lösung. Zumindest bei Einbruch gilt: Die Daten sind sicherer, wenn sie außer Haus aufbewahrt werden.

Interne Sicherung: Bietet keinen Schutz vor Gefahren in der Kanzlei

Eine externe Datensicherung bietet den Vorteil, dass alle Gefahren, die innerhalb der Kanzlei auftreten können, ausgeschaltet werden. Zu klären ist, wie weit die externe Datensicherung den anwaltlichen Berufspflichten und den deutschen Datenschutzgesetzen genügt. Wo stehen die Server, wie werden diese wiederum gesichert, wie werden die Daten transportiert und aufbewahrt? Werden die Daten verschlüsselt? Welcher Datenschutz wird gewährleistet? Die beliebten Cloud-Systeme wie Dropbox, OneDrive von Microsoft oder iCloud von Apple speichern die Daten weltweit und sind für Anwaltskanzleien ungeeignet. Der DAV hat 2015 in Zusammenarbeit mit TeamDrive eine Cloud für DAV-Mitglieder ins Leben gerufen, die den besonderen Anforderungen des Berufsstands als Geheimnisträger nach § 203 StGB gerecht wird (siehe S. 55).

SIEHE AUCH
S. 55 in dieser Ausgabe

3. Welche Daten sollen gesichert werden?

Genügt es, die sich täglich ändernden Daten (Adressdaten, Schriftsätze, Terminkalender, Buchhaltungsdaten etc.) zu sichern oder ist dies auch für Betriebssystem, Programmdaten und Softwarestände nötig? Soll eine Vollsicherung erfolgen oder sollen nur die Daten, die seit der letzten Sicherung verändert wurden bzw. hinzugekommen sind, gesichert werden? Dies erhöht die Geschwindigkeit der Datensicherung, hat aber im Rücksicherungsfall Nachteile. Hier wird in der Regel der IT-Dienstleister seine Kompetenzen einbringen und eine geeignete Lösung vorschlagen, die den Bedürfnissen der Kanzlei entspricht.

Einzelheiten mit IT-Dienstleister klären

4. Wie oft soll gesichert werden? Je kürzer, desto sicherer

Je kürzer der Zeitraum zwischen zwei Datensicherungen ist, desto einfacher ist es, die fehlenden Daten wieder zu rekonstruieren. Je höher also das Datenvolumen ist, desto wichtiger ist es, die Daten täglich – ggf. sogar mehrmals täglich – zu sichern.

Hohes Datenvolumen: Ggf. mehrmals täglich sichern

5. Verschiedene Versionen sichern!

Legen Sie mit Ihrem IT-Dienstleister das passende Programm fest. Die Sicherung sollte automatisch zu einem festgelegten Zeitpunkt starten. Nur so ist gewährleistet, dass die Daten kontinuierlich gesichert werden. Das sog. Generationenprinzip stellt sicher, dass immer mehrere Sicherungen in verschiedenen zeitlichen Abstufungen (Großvater, Vater, Sohn) vorhanden sind. So können verschiedene Versionen wiederhergestellt werden.

Dafür wird an jedem Tag eine separate Datensicherung erstellt (Sohn). Am letzten Tag der Woche erfolgt die Wochensicherung (Vater). Am letzten Tag des Monats erfolgt die Monatssicherung (Großvater). Dieses System wird kontinuierlich verwendet, sodass eine Datenrücksicherung bis zu einem Jahr möglich wäre. Zusätzlich kann es bei besonderen Datenbeständen und Software-Updates ratsam sein, vorher die Daten vollständig manuell zu sichern.

6. Auf welchem Medium soll gesichert werden?

Cloud muss wiederum selbst gesichert sein

Es genügt nicht die Festplatte zu spiegeln, denn dann sind die Gefahren (siehe Punkt 2.) noch nicht gebannt. Je nach Datenmenge bieten sich externe Festplatten an, die außerhalb der Kanzlei aufbewahrt werden. Bei der Datensicherung in der Cloud ist zu gewährleisten, dass die Cloud selbst ebenfalls gesichert ist und sowohl der anwaltlichen Verschwiegenheit Rechnung trägt als auch den deutschen Datenschutzgesetzen genügt.

7. Verschleiß der Datenträger berücksichtigen

Weitere Gefahren für Sicherungsmedium ausschließen

Manche Kanzleien verwahren in feuerfesten Tresoren, andere lagern ohne große Achtsamkeit „irgendwo“ im Serverraum, der manchmal auch die Küche beherbergt, sodass sich ggf. weitere Gefahren für die Sicherungsmedien ergeben können. Im Idealfall werden die externen Datenträger außerhalb der Kanzlei aufbewahrt. Legen Sie in Ihrem Datensicherungskonzept fest, wo und wie lange die Datenträger verwahrt werden und wie oft ein Datenträger wiederbeschrieben werden darf. Auch Datenträger unterliegen dem Verschleiß, sodass regelmäßig kontrolliert werden muss, ob sie noch funktionieren. Marode Teile müssen ausgetauscht werden.

8. Datenrücksicherung üben

Praktische Übungen sollen gewährleisten, dass die Rücksicherung der Daten für den Ernstfall geprobt wird. Das hätte im Fall der Kanzlei, die der BGH auf den manuellen Weg verwiesen hat (27.1.15, II ZB 21/13, a.a.O.), dazu geführt, dass mit einem parallelen System die IT-Struktur der Kanzlei kurzfristig wiederhergestellt und die Frist gewahrt worden wäre.

9. Gefahr sitzt auch vor dem Computer

Anwälte und Mitarbeiter sensibilisieren

Schulen Sie alle Personen, die in Ihrer Kanzlei Umgang mit der EDV haben. Neben einer Firewall und einem jederzeit aktuellen Virenschutz ist es notwendig, Anwälte und Mitarbeiter zu sensibilisieren, um den Gefahren aus dem Netz wirksam zu begegnen.

Aktuell hat eine Erpresser-Software an einem Tag 17.000 deutsche Computer infiziert, weltweit sind bereits 400.000 betroffen. Möglicherweise versteckt sich der Trojaner „Locky“ bereits seit längerer Zeit auf vielen Rechnern und ist jetzt scharf geschaltet worden. Unter anderem wurden nach Angaben der dpa auch am Fraunhofer-Institut in Bayreuth 60 PC-Arbeitsplätze lahmgelegt. Die Schadsoftware ist offenbar über einen der PC-Arbeitsplätze ins Netzwerk des Instituts gelangt und hat sich selbstständig weiterkopiert.

Gefahr durch Virus „Locky“

Die Erpresser infizieren Windows-Computer mit einem Trojaner, der wichtige Dateien zunächst verschlüsselt und dann umbenennt. Sodann erscheint ein Erpresserbrief mit einer Lösegeldforderung. Ein Krankenhaus in Los Angeles hat offenbar 17.000 US-Dollar bezahlt, um an die verschlüsselten Daten zu gelangen. „Locky“ ist über gefälschte Rechnungen, die den E-Mails angehängt waren, auf den PC gelangt. Bedenken Sie aber, dass Sie sich den Trojaner als Nutzer auch über den Browser einhandeln können. Wenn Sie über eine aktuelle Datensicherung verfügen, um Ihre Daten wiederherzustellen, können Sie solche Gefahren von Ihrer Kanzlei abwehren.

Mit dieser Checkliste schaffen Sie sich in zehn Schritten ein sicheres Konzept, um die Daten in Ihrer Kanzlei sicher aufzubewahren:

CHECKLISTE / In zehn Schritten zur professionellen Datensicherung

- Schritt 1: Benennen Sie einen Verantwortlichen und einen Vertreter für die Datensicherung.
- Schritt 2: Legen Sie fest, wer dafür zuständig ist, die Maßnahmen der Datensicherung praktisch umzusetzen und wer ihn vertritt (z. B. für folgende Aufgaben: Datensicherung täglich kontrollieren; überprüfen, ob die Sicherungsmedien korrekt aufbewahrt werden; Rücksicherung durchführen und prüfen; Sicherungsmedien austauschen).
- Schritt 3: Prüfen Sie die abzudeckenden Risiken und Gefährdungen.
- Schritt 4: Legen Sie fest, welche Daten in welchem Abstand auf welchen Medien zu sichern sind und wo diese aufbewahrt werden.
- Schritt 5: Interne oder externe Datensicherung? Entscheiden Sie sich, was zu Ihrer Kanzlei passt.
- Schritt 6: Der Zukunftstrend geht zur Cloud. Vertrauen Sie Ihre Daten nur einer sicheren Cloud an (z. B. TeamDrive, siehe unter 2).
- Schritt 7: Üben Sie regelmäßig die Rücksicherung.

Praktisch üben

- Schritt 8: Datensicherung ist kein Selbstzweck, informieren Sie mindestens einmal im Quartal alle Anwälte und Mitarbeiter in Ihrer Kanzlei, um potenzieller Gefährdung aus dem Netz zu begegnen. Dokumentieren Sie schriftlich und an sicherer Stelle, wie im Falle eines Datenverlusts zu handeln ist.
- Schritt 9: Sorgen Sie für eine sog. USV (unterbrechungsfreie Stromversorgung).
- Schritt 10: Kontrollieren Sie kontinuierlich, ob Ihr Datenschutzkonzept eingehalten wird.

Regelmäßige Kontrolle

↘ WEITERFÜHRENDER HINWEIS

• Selbstständigkeit – Fehler vermeiden: „Dos and Don'ts“ für Junganwälte, AK 14, 150

ARCHIV
Ausgabe 9 | 2014
Seite 150