Datenverlustrisiko bei Rechtsanwalts-, Steuerberater- und Wirtschaftsprüferkanzleien

Diebstahl oder Verlust von Mandantendaten

Kanzleien haben eine Vielzahl an sensiblen Mandantendaten. Diese Daten sind analog Bundesdatenschutzgesetz (BDSG) schützenswerte Daten. Steuerberater unterliegen wie auch Rechtsanwälte und Wirtschaftsprüfer der Verschwiegenheit. Dies ist gesetzlich bzw. berufsrechtlich geregelt. Gerade auch Daten von gewerblichen oder prominenten Mandanten sind ob ihrer Inhalte ein begehrtes Objekt. Kosten die entstehen, sollten Speichermedien (z.B. Laptops, Speichersticks, etc.) verloren gehen oder entwendet werden, liegen bei einem Laptop schnell bei über 30.000 € zur Wiedererlangung der Daten und Dokumentierung. Kosten für die Wiederherstellung von Netzwerken, Datenbanken, etc. sind analog um ein Mehrfaches höher. Sind Mandantendaten entwendet worden oder verloren gegangen, sind die betreffenden Personen hierüber unverzüglich zu informieren (§42 a BDSG). Dadurch können hohe Kosten entstehen. Ebenfalls können sich daraus auch Schadenersatzansprüche (§7 BDSG) und Strafen herleiten.

Ist die Rechtsanwalts-, Steuerberater- oder Wirtschaftsprüferkanzlei auf einen Datenverlust vorbereitet?

- Gibt es einen Krisenplan? Weiß jeder Inhaber und Mitarbeiter was bei Verlust von Daten zu tun ist?
- Wer muss beim Diebstahl oder Verlust von Mandantendaten informiert werden? Nur die Mandanten? Oder auch andere offizielle Stellen?
- Auf welche Art und Weise muss die Information erfolgen?
- Welche Kosten kommen auf die Kanzlei zu?
- Wie verhält man sich, wenn die Kanzlei nach Datenverlust erpresst wird?
- Wie können verloren gegangene Mandantendaten wieder hergestellt werden?
- Welche Strafen und Schadenersatzansprüche drohen?
- Was macht man, wenn das Computernetz der Kanzlei oder die eigene Internetseite offline geht oder durch einen Virus gesperrt wird und längere Zeit nicht wieder zu aktivieren ist? Kann die Kanzlei die dadurch entstehenden Kosten bei Unterbrechung des laufenden Geschäftsbetriebs ohne Probleme bewältigen?

Lösung: Zielstrebiges und schnelles Handeln im Schadensfall mit Hilfe kompetenter Ansprechpartner, die sich mit dieser Materie auskennen und wissen was zu tun ist. Hier setzt die Cyberdeckung an:

- Ein Deckungskonzept, das verschiedene Unterstützungs- und Versicherungsleistungen in einer Police vereinigt.
- Bereitstellung von internen und externen Spezialisten, die präventiv tätig sind und im Schadensfall die Krise managen.
- Übernahme der Kosten für IT-Experten, die Sicherheitslücken schließen oder den Sachverhalt aufklären und gerichtsverwertbar dokumentieren.
- Sicherstellung der Funktionsfähigkeit der eigenen Website durch zeitnahe Reparatur bzw. Ersatz.
- Ausarbeitung und Aushändigung eines IT Krisenplans.

Weitere Risikosituationen

Reputationsschaden

Ein öffentlich gewordener Datenschutzverstoß kann einen immensen Reputationsschaden hinter sich herziehen. Dies zu verhindern ist die Zielvorgabe der Cyberdeckung, mit Hilfe der Kooperationspartner und der Versicherungsleistung.

Haftung des Vorstandes oder der Geschäftsführung

Nur mittels eines vorausschauenden Krisenmanagements lässt sich auch ein ggfs. möglicher interner Anspruch aus der organschaftlichen Pflichtverletzung, z.B. mangelnde Organisation des Unternehmens, fehlendes und/oder ungenügendes Risikomanagement, vermeiden. Ansprüche wegen einer organschaftlichen Pflichtverletzung ziehen eine unbegrenzte, persönliche Haftung hinter sich her.

Schadensszenarien

- Kanzlei wird nach Datendiebstahl erpresst;
- Computervirus legt Geschäftsbetrieb lahm;
- Hacker manipulieren Computer;
- bei der Entsorgung alter Mandantenunterlagen geht etwas schief: sie gelangen in das Altpapier oder werden zu schlecht zerkleinert, so dass personenbezogene Daten wie Namen, Adressen und Telefonnummern noch zu lesen sind;
- Mandantendaten werden bei Einbruch in Kanzlei entwendet;
- bei Autodiebstahl kommen Mandantendaten abhanden;
- Mandantendaten oder Prozessunterlagen werden an falsche Faxnummer gefaxt;
- Rechtsanwalt wird Koffer mit Handakten gestohlen;
- Mandantenunterlagen werden falsch kuvertiert und an falsche Adressen versendet;
- Kanzlei verschickt E-Mail mit Mandantendaten an falsche E-Mail-Adresse;
- in E-Mail wird versehentlich falscher Anhang beigefügt, der Mandantendaten enthält;
- gestohlene Mandantendaten werden für Spam-Mails missbraucht;
- Mandantendaten werden versehentlich weitergegeben;
- fahrlässiger Umgang mit mobilen Endgeräten, z. B. durch unzureichende Verschlüsselung, führt zum Verlust von Mandantendaten infolge von Diebstahl des Endgeräts oder dem Ausspähen dieses (z.B. Laptop, Smartphone);
- mobiler Datenträger (z.B. USB-Stick oder Festplatte) mit Mandantendaten und Prozessakten verschwindet bzw. kann einfach nicht mehr aufgefunden werden;
- Mandantenliste wird bei Datendiebstahl entwendet;
- Mandantendaten werden vertauscht;
- Computer oder Server mit Mandantendaten wird aus Kanzlei gestohlen;
- bei der Online-Vergabe von Terminen kommt es zu einer Fehladressierung;
- ehemalige Mitarbeiter nehmen Mandantendaten mit;
- nicht hinreichend geschwärzte Prozessakten gelangen an Dritte.