Digitaler Nachlass – Passwortentschlüsselung im Auftrag der Rechtspflege

Text — Dipl.-Ing. Sascha Lüdtke

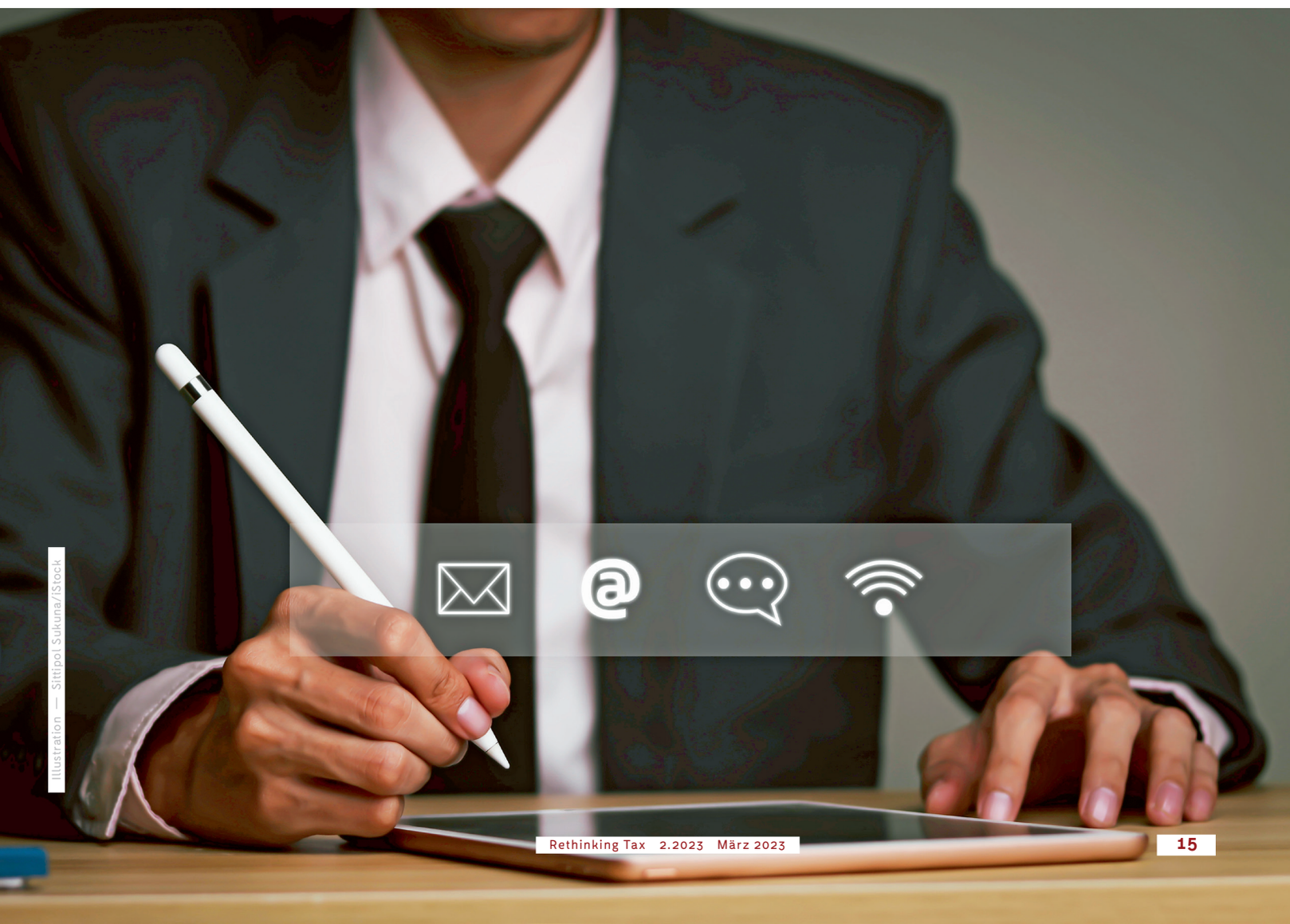

Illustration — Sittipol Sukuna/iStock

In den letzten Jahren hat die Digitalisierung rasant zugenommen und die Wirtschaft zunehmend beschleunigt. Gleichermaßen hat die digitale Welt auch in der Privatsphäre Einzug gehalten. Wichtige Dokumente und persönliche Unterlagen werden vermehrt auf elektronischen Endgeräten bzw. Datenspeichern wie Laptops, Computern, externen Festplatten, USB-Sticks oder Cloud-Speichern hinterlegt und nicht - wie in der Vergangenheit - in Papierform aufbewahrt. Entsprechend gewinnen auch immer mehr Fragen rund um den sog. digitalen Nachlass zunehmend an Bedeutung und stellen nicht nur Rechtsanwälte und Steuerberater, sondern auch Nachlass- und Insolvenzverwalter vor gänzlich neue Herausforderungen. Insbesondere passwortgeschützte Endgeräte hemmen dabei regelmäßig die (steuerliche) Erfassung des gesamten Nachlasses.

Zum digitalen Nachlass rechnen beispielsweise E-Mail- und Online-(Banking)-Konten, Social Media-Accounts oder große Datenmengen, die sich auf Computern oder in der Cloud wiederfinden. Vor diesem Hintergrund ist es essenziell, den digitalen Nachlass im Voraus zu planen, damit der Zugriff auf Daten und Passwörter durch Einzel- oder Gesamtrechtsnachfolger sowie andere Berechtigte sichergestellt wird. Für eine sichere Aufbewahrung von Zugangsdaten und Passwörtern eignen sich speziell für den Nachlassfall entwickelte Software-Lösungen, wie beispielsweise „MyLastKey“. Das gilt sowohl für natürliche Personen als auch Unternehmen.

Eine repräsentative Umfrage zeigt jedoch, dass viele mit diesem Thema eher stiefmütterlich umgehen:

„Nach einer repräsentativen Umfrage im Jahre 2016 informierten in Deutschland nur 8 % ihre Hinterbliebenen über Zugangsdaten zu von ihnen in Anspruch genommenen Diensten und Online-Konten einschl. weiterer Passwörter.
Eine diesbezügliche Einschätzung der E-Mail-Anbieter Web.de und GMX aus dem Jahre 2019 geht davon aus, dass gerade mal 15% der Internetnutzer ihren digitalen Nachlass für zumindest einige ihrer Online-Konten geregelt hatten.“

Dieses Ergebnis verwundert umso mehr, als die herrschende Meinung inzwischen davon ausgeht, dass dem digitalen Nachlass mittlerweile die gleiche Bedeutung beizumessen ist, wie dem physischen Erbe. Entsprechend ist im Erbfall folgenden Fragen nachzugehen:

- Wurde ein digitales Testament gefertigt?
- Wurden Excel-Aufstellungen über Geldanlagen vorgehalten?
- Existieren Wallets für Kryptowährungen?
- Bestehen Social Media-Accounts, die ggfs. gelöscht werden müssen?
- Ergeben sich aus E-Mail-Konten zu bedienende Verbindlichkeiten?
- Bestehen kostenpflichtige Online-Dienste wie bspw. Amazon Prime oder Netflix?
- Sind steuerlich erhebliche Daten ermittelbar, damit Steuererklärungen erstellt oder im Falle von steuerlichen Außenprüfungen Datenzugriffsrechte der Finanzverwaltung gewährleistet werden können?

Wurden die hierfür erforderlichen Zugangsdaten und Passwörter durch den Erblasser leicht auffindbar in Papierform hinterlegt, kann der

Die Verwaltung eines digitalen Nachlasses erfordert ein hohes Maß an Fachwissen sowie den Einsatz moderner und leistungsfähiger IT-Werkzeuge.

digitale Nachlass weitgehend unproblematisch (ggf. forensisch) untersucht und zusammengestellt werden. Dies ist jedoch nicht immer der Fall, ganz im Gegenteil.

In einer Vielzahl der Fälle bleibt der Zugriff trotz intensiver Bemühungen zunächst verwehrt. Was es dann braucht sind IT-Spezialisten, die in der Lage sind, Sicherungssysteme zu umgehen, respektive Passwörter zu entschlüsseln, um Daten zu sichern, einzusehen und für die Nachlassabwicklung relevante und möglicherweise beweiserhebliche Sachverhalte festzustellen und zusammenzutragen.

So komplex sich der Dechiffrier-Vorgang darstellt, letztlich ist es „nur“ eine Frage der Zeit, bis Passwörter entschlüsselt werden. Hierfür müssen verschlüsselte Datenträger zunächst forensisch analysiert werden, um anschließend das verschlüsselte Passwort, den sogenannten „Passwort-Hash“, aus dem Datenträger zu extrahieren. Weiter bedarf es entsprechender Softwarelösungen wie etwa „GovCracker“, welche mittels „Trial-and-Error“ bis zu mehrere Millionen bis Milliarden Passwörter pro Sekunde abprüfen. Hardware-seitig werden sogenannte GPU-Server eingesetzt, die hochleistungsfähige Grafikkarten besitzen und herkömmlichen Computer-Prozessoren (CPUs) in Bezug auf den Faktor „Zeit“ deutlich überlegen sind. Der künftige Einsatz von Quantencomputern dürfte diesen Vorgang nochmals um ein Vielfaches beschleunigen, zumindest so lange, bis auch Quantenkryptographie Verwendung findet.

Fazit

Bei passwortgeschützter Hardware ist der Einsatz professioneller IT-Spezialisten in der Regel das einzige Mittel, den digitalen Nachlass schnell und umfassend zu sichern, zu analysieren sowie in einem detaillierten Bericht zusammenzufassen. Anders lässt sich das Ziel (aber auch die Pflicht) einer Nachlassverwaltung, den Nachlass auf Vollständigkeit zu ermitteln und eine umfassende und steuerlich korrekte Nachlassaufstellung anzufertigen, kaum erreichen. ▪

Weitere Informationen zu diesem Themenfeld finden Sie unter

www.decrypta-technologies.com

Dipl.-Ing. Sascha Lüdtke
Geschäftsleitung der Decrypta Technologies GmbH, Schwerte, NRW

Die Decrypta Technologies GmbH unterstützt internationale Strafverfolgungsbehörden mit speziellen Dienstleistungen und eigens entwickelter Software („GovCracker“ und „GovCrypto“) vorrangig beim Entschlüsseln von Passwörtern und Aufspüren von Kryptowährungen. Darüber hinaus stellt sie Nachlassverwaltern, Rechtsanwälten und Steuerberatern in berechtigten Fällen die beschriebenen Dienstleistungen und Softwares zur Verfügung.