Müssen Hausdurchsuchungen eine Überraschung sein?

Mag. Thomas Havranek
StB, HFP-Steuerberater

Nicht nur seitdem auch das Finanzstrafrecht ab einer betraglichen Grenze von EUR 75.000,00 in die Zuständigkeit der Strafgerichtsbarkeit fällt, sind Hausdurchsuchungen in Wirtschaftsfällen von der Ausnahme zur Regel geworden. Auffällig ist dabei auch die stark gesunkene Hemmschwelle, Hausdurchsuchungen bei den gesetzlichen Parteienvertretern der Beschuldigten, Rechtsanwälten und Wirtschaftstreuhändern, durchzuführen. Das alles ist noch nicht wirklich verwunderlich, vielmehr wie unvorbereitet Betroffene in vielen Fällen immer noch reagieren.

Hausdurchsuchungen können jedes Unternehmen treffen. Die durchsuchenden Beamten sind exzellent vorbereitet. Sie haben bereits zahlreiche Informationen gesammelt, oftmals Insider-Informationen von Whistleblowern oder verärgerten Mitarbeitern. Sie kommen frühmorgens, überraschend und klopfen beim schwächsten Glied in der unternehmerischen Kette an, dem Empfang. Unternehmen und Berater können sich in mehreren Schritten auf diese Unannehmlichkeit vorbereiten.

Gute Vorbereitung.

Wesentlich ist ein Verhaltensleitfaden für den richtigen Umgang mit einer solchen Situation. Wie ist den Beamten entgegen zu treten? Kein unkooperatives Verhalten. Aufforderung im Besprechungszimmer Platz zu nehmen, bis Management, falls vorhanden Leiter Rechtsabteilung oder Compliance (jedenfalls bewanderter Jurist) des Hauses und Rechtsanwalt, sowie IT- Experte vor Ort ist. Wenn die Beamten dennoch fortfahren, exaktes Protokollieren aller Unterlagen und Geräte, die sie mitnehmen.

Der IT Experte ist heute der meistvernachlässigte und fast wichtigste Experte, der beizuziehen ist. Üblicherweise wird im Durchsuchungsbefehl exakt angeführt, wonach zu suchen und was zu beschlagnahmen ist. Die EDV ist daher jedenfalls Ziel der Beamten. Der IT-Experte kann dabei kooperieren die richtigen Daten weiter zu geben und jedenfalls genauestens protokollieren, welche Daten die Beamten kopieren oder spiegeln. Denn letztlich spiegeln Beamte meistens einfach den gesamten Datenbestand. Dies kann zu unangenehmen Zufallsfunden führen – vgl. in Folge IT Compliance. Geschäftsführung und Parteienvertreter sollen jedenfalls Versiegelung der beschlagnahmten Unterlagen und Daten mit Hinweis auf vertrauliche Kommunikation zwischen Mandanten und Parteienvertretern beantragen. Dem wird heute üblicherweise nur bei Hausdurchsuchungen bei gesetzlichen Parteienvertretern statt gegeben. Umso wichtiger ist es, hier eine schlüssige Argumentation zu entwickeln.

Ein guter Leitfaden beinhaltet für sämtliche Mitarbeiter ein exaktes Protokoll über Auftreten, Verhalten, Kooperation und Aufgaben im Zuge einer Hausdurchsuchung. Eine Hausdurchsuchung ist jedenfalls eine böse Überraschung für MitarbeiterInnen. Ein Verhaltensleitfaden ist eine gute Unterstützung,

aber erst die Simulation eines potenziellen Echtszenarios zeigt die Schwächen auf, mit denen es umzugehen gilt. So wie regelmäßig Brandschutzübungen abgehalten werden, ist es zweckmäßig sowohl für Unternehmen als auch für Parteienvertreter eine „Brandschutzübung" für Hausdurchsuchungen durchzuführen. Insbesondere Sachverständige und Forensik-Dienstleister, die als Experten oftmals auf Seiten der Staatsanwaltschaft oder Exekutive beigezogen waren und mit eigenen IT-Experten auch die gesamte Expertise für eine Hausdurchsuchung abbilden können, sind hier die erforderlichen Ansprechpartner um alle Fragen zu beantworten.

IT Compliance.

Am Ende des Tages und in immer papierloser werdenden Büros zeichnet sich seit Jahren ab, dass die größte Schwachstelle aller Betroffenen die EDV ist. Und hier vor allem das mangelnde interne Know-how über Datenablage, Datenspuren, E-Mail-Archivierung, etc. IT-Administratoren sind nicht immer gleich Experten für IT-Security, Daten Redemption und Datenvernichtung. Insbesondere die Kommunikation in Unternehmen über E-Mail kann nicht perfekt kontrolliert werden, ohne Datenschutzrechte zu verletzen. Daher besteht ebendort ein sehr hohes Risiko. In 80% aller Fälle finden wir als beigezogene Experten in Wirtschaftsfällen Spuren zu oder Beweise selber in der E-Mail Kommunikation. Es ist daher erforderlich mit Counter Forensik die eigene EDV aufzuräumen.

Dabei wird mit Hilfe von mit künstlicher Intelligenz ausgestatteter Software der Datenbestand durchsucht und auf Risiken analysiert. Wenn Risikodaten identifiziert werden gilt es unter Beiziehung von Haus- oder externen Juristen zu beurteilen, welche Daten gelöscht, welche wie und wo versiegelt gelagert werden und welche als Grundlage rechtlicher Maßnahmen herangezogen werden. Wir verwenden hierzu eine von uns auf Basis von IBM Watson Explorer weiter entwickelte Softwarelösung, IC Investigations. Wir können damit in kürzester Zeit riesige Datenmengen durchsuchen.

Dies dient nicht nur der Prävention, es ist auch in Zeiten wie diesen für die Compliance besonders relevant. Denn nichts ist schlimmer als Kommunikationsstränge zu finden die, wie in einem Fall kürzlich, auf eine Umgehung der Russlandsanktionen hinweisen oder in einem Fall kartellrechtliche Fragen aufgeworfen haben. Die Konsequenzen sind nicht nur nervenaufreibend, sondern können ein Unternehmen oder eine Beratungskanzlei zerstören.

Um daher auf Hausdurchsuchungen vorbereitet zu sein, sollte man wissen, was man in seinem Datenbestand hat. Das papierlose Büro und die unlimitierte Größe von E-Mail-Konten führen zu einem exponenziellen Wachstum. Die Behörden arbeiten mit Softwaresystemen wie „The Analyst Notebook", mit dem Kommunikationsströme und Geldbewegungen analysiert werden. Es kommen Software Systeme wie Intella aus den USA zum Einsatz, die ebenso wie unser IC Investigation auch Terrabyte von Daten, also Abermillionen von Dokumenten, durchsuchbar machen. Man denke nur an die exzessiven Auswirkungen und anhaltenden Gerichtsverfahren nur durch die berühmten Schmid-WhatsApp-Nachrichten. Und niemand weiß, was seine MitarbeiterInnen wann und mit wem kommunizieren und vor allem leider dann, wenn Emotionen dahinter sind. Einfach gesagt, die E-Mail-Server von Unternehmen sind für die Steuerfahndung, die Kriminalpolizei eine Goldgrube und für die betroffenen Unternehmen Hellfire und Highwater zur selben Zeit.

Sun Tzu hat schon vor über 2000 Jahren geschrieben: „Wenn du dich und den Feind kennst, brauchst du den Ausgang von hundert Schlachten nicht zu fürchten. Wenn du dich selbst kennst, doch nicht den Feind, wirst du für jeden Sieg, den du erringst, eine Niederlage erleiden. Wenn du weder den Feind noch dich selbst kennst, wirst du in jeder Schlacht unterliegen."

Sie kennen sich nicht, weil sie eben nicht wissen, was Ihre KollegInnen und MitarbeiterInnen alles kommunizieren. Und sie kennen naturgemäß die Ermittler nicht, außer Sie sind regelmäßiger Gast im Straflandesgericht und vor dem BFG. Damit wird ein Sieg in einem (Finanz)Strafverfahren langwierig, teuer und schwierig, denn die Ermittler kommen nicht zufällig bei Ihnen zu einer Hausdurchsuchung vorbei. ■

Resümee

Eine Hausdurchsuchung ist immer unangenehm. Die Beamten können davon nicht abgehalten werden. Durch vernünftige Fragestellungen, Ersuchen um genaue Erläuterung des Hausdurchsuchungsbefehls und höfliches Entgegentreten kann üblicherweise genug Tempo herausgenommen werden, bis Rechtsberater, (im Falle Finanzstrafverfahren) Steuerberater und jedenfalls IT-Experten vor Ort sind.

Man kann sich darauf so vorbereiten, dass eine professionelle Abwicklung mit geringst möglichstem Schaden erfolgt und danach die bestmögliche Verteidigung durch genaue Protokolle der beschlagnahmten Unterlagen, Daten und Hardware möglich ist.