Illustration: © Alexandr Sidorov

WENN DER **STAATSANWALT** KLINGELT...

… am Ende auch eine Compliance-Frage?

Melden sich die Ermittlungsbehörden sollten Sie Ruhe bewahren und gut vorbereitet sein. Das ist nicht so üblich ist, wie das Klingeln des Paketboden, aber auch ernsterer Natur ist. Sie sollten vorbereitet sein. Denn: Vorbereitung schafft Selbstsicherheit und diese führt zu Besonnenheit. Vorbereitung und Besonnenheit ist wichtig, denn wird an Sie nicht als Beschuldigter, sondern als Dritter herangetreten, müssen Sie auch den Schutz Ihrer Kunden oder Auftraggeber im Auge haben.

Der erste Kontakt

Gerade die Situation der Durchsuchung oder der Vernehmung vor Ort ist die Stunde der Staatsanwaltschaft und von jeder Gegenmaßnahme ist abzuraten. Gleichwohl sind eigene Rechte zu wahren und als Dienstleister müssen Sie auch die Rechte Ihrer Kunden im Auge behalten.

Gleichgültig, ob die Staatsanwaltschaft oder die Polizei bei einer Durchsuchung vor Ort präsent sind oder ob an Sie ein schriftliches Auskunftsverlangen gerichtet wird, die entscheidende erste Frage lautet: Sind Sie als Beschuldigter oder als Zeuge betroffen? Denn

danach richten sich Ihre Rechte und Pflichten. Die Ermittlungsbehörden dürfen Sie hierüber nicht im Unklaren lassen. Aber Achtung: Auch noch während der Durchsuchung oder einer Zeugenvernehmung kann sich die Sichtweise der Behörden ändern, so dass plötzlich von einer Beschuldigten-Situation auszugehen ist. Hierauf sollten Sie vorbereitet sein.

Dieser Beitrag behandelt nachfolgend die Situation, in der Ihr Unternehmen nicht als Beschuldigter, sondern als allgemein Auskunftspflichtiger oder aber Mitarbeiter als Zeugen in einem Ermittlungsverfahren gegen einen Dritten betroffen sind.

Foto: © bilderbox

Auskunftsverlangen

Die Behörden richten meist zunächst schriftliche Auskunftsverlangen an Sie. Dies ist von der allgemeinen Ermittlungsbefugnis gedeckt und eine informelle Form der Zeugenvernehmung. Ein solches Auskunftsverlangen ist nicht erzwingbar, was nicht heißen sollte, dass Sie es auf eine Eskalation ankommen lassen müssen oder sollten. Auch hier gilt es, eine stimmige Abwägung für den Einzelfall zu treffen. Wird einem Auskunftsverlangen nicht Folge geleistet, ist die nächste Eskalationsstufe ein Durchsuchungsbeschluss oder eine Zeugenvernehmung.

Entscheiden Sie sich für eine Beantwortung des Auskunftsverlangens, haben Sie zu prüfen, welche Informationen betroffen sind. Geht es um Daten, welche dem Fernmeldegeheimnis unterliegen, kann nicht ohne Weiteres die erbetene Auskunft erteilt werden. Auch wenn Daten von Kunden, insbesondere sensible Daten, betroffen sind, sollten Sie vorsichtig sein. Hier können Schadensersatzansprüche drohen. In diesem ist es besser, die Auskunft zu verweigern und auf einen Durchsuchungsbeschluss oder eine Zeugenvernehmung zu bestehen. Gegenüber der ersuchenden Behörde ist dann mitzuteilen, dass das Auskunftsverlangen keine ausreichende Rechtsgrundlage darstellt und daher Weiterungen erforderlich sind. Zuweilen werden vor diesem Hintergrund durch die Staatsanwaltschaften auch eingeholte Durchsuchungs- und Beschlagnahmebeschlüsse vorab zugesendet. Diese erfahren jedoch nur dann eine Umsetzung, wenn die Auskunft nicht erteilt wird.

Aber Vorsicht: Erteilen Sie nunmehr zur Vermeidung der Maßnahme die erbetene Auskunft, müssen Sie dabei schriftlich klarstellen, dass Sie dies nicht freiwillig, sondern nur zur Abwendung der Zwangsmaßnahme tun.

Ähnliches gilt für die Ladung zur Zeugenvernehmung. Hierzu gibt es noch zwei Dinge zu wissen: Einer polizeilichen Ladung zur Zeugenvernehmung muss nicht Folge geleistet werden. Nur bei einer Ladung durch die Staatsanwaltschaft oder den Richter kann das Erscheinen erzwungen werden. Bei jeder Vernehmung sollte es die Regel sein, sich von einem anwaltlichen Zeugenbeistand begleiten lassen.

Fernmeldegeheimnis

Die Inhalte und die näheren Umstände der Telekommunikation sind durch Art. 10 GG und §206 StGB geschützt. Die Schutzpflicht trifft allerdings nur den Telekommunikationsdienstleister, nicht den Teilnehmer der Telekommunikation.

Handelt es sich um durch das Fernmeldegeheimnis geschützte Daten, ist zu prüfen, ob die Ermittlungsmaßnahme der Strafverfolgungsbehörden die richtige ist. Die Rechtsprechung hierzu ist zwischenzeitlich sehr differenziert, weshalb schematische Antworten hierzu nicht gegeben werden können. Sie müssen im Vorfeld geklärt haben, ob die Daten entsprechend geschützt sind und unter welchen Voraussetzungen welche Daten herausgegeben werden dürfen.

Das Dilemma bei diesen Daten besteht darin, dass bei einer zu Unrecht verweigerten Herausgabe der Ärger groß ist und eine Strafe wegen (versuchter) Strafvereitelung droht. Werden die Daten hingegen zu Unrecht herausgeben, droht eine Strafe nach §206 StGB wegen eines Verstoßes gegen den Schutz des Fernmeldegeheimnisses (§206 StGB). Aber Achtung: Trotz Ihrer Schutzpflicht dürfen Sie keinen Widerstand bei einer Durchsuchung leisten!

Wenn es klingelt

Die Situation einer Durchsuchung zur Auffindung von Beweismitteln ist immer unangenehm. Auch für die Ermittlungsbeamten ist dies zu Beginn eine angespannte Situation, da auch sie nicht wissen, was sie erwartet. Entspannen Sie diese Situation durch ruhiges und sachliches Vorgehen! Bitten Sie die Ermittlungsbeamten in einen leeren Raum. Fragen Sie nach dem die Durchsuchung leitenden Beamten. Lassen Sie sich die Dienstausweise und den richterlichen Durchsuchungsbeschluss zeigen. Aus dem Beschluss ergibt sich,

wonach die Beamten suchen. Vergewissern Sie sich, dass der Beschluss an Ihr Unternehmen adressiert ist und die benannten Räume, auf die sich die Durchsuchung bezieht, mit der zutreffenden Adresse angegeben sind.

Sind Sie Auskunftspflichtiger richtet sich der Beschluss in der Regel nur auf eine bestimmte Information, bestimmte Unterlagen oder bestimmte Daten, die im Zusammenhang mit dem Beschuldigten stehen. Um eine allgemeine Durchsuchung und die damit einhergehende umfassende Beeinträchtigung Ihres Unternehmens zu vermeiden, empfiehlt es sich, die geforderten Informationen einzugrenzen. Dies auch zum Schutz Ihrer übrigen Kunden, da ohne eine kooperierende Eingrenzung alles durchsucht wird. Hier sind zivilrechtliche Kollateralschäden zu vermeiden. Einen pauschalen Rat für das zu wählende Vorgehen gibt es jedoch leider nicht. Es ist immer auf die Umstände des jeweiligen Einzelfalls abzustellen.

Sofern die Bewertung des Einzelfalls eine kooperierende Vorgehensweise ermöglicht, können in Abstimmung mit den Beamten gezielt Kopien oder Images der gesuchten Datenträger oder Unterlagen gefertigt werden, sofern dadurch nicht auch Daten weiterer Kunden herausgegeben werden (siehe hierzu auch unten). Denn im Falle der Kooperation gilt für die Ermittlungsbeamten im besonderen Maße der Grundsatz der Verhältnismäßigkeit, wonach Ihrem Unternehmen kein unnötiger Schaden zugefügt werden darf.

Regeln beachten

Falls eine Durchsuchung erfolgt, dann gibt es zu beachtende Regeln. Diese sollten in einem entsprechenden Plan oder Protokoll für das Unternehmen festgelegt und den Mitarbeitern bekannt sein. Hier mag es unterschiedliche Varianten geben, aber einige Regeln sollten stets Beachtung finden:

Kein Ermittlungsbeamter bewegt sich ohne eine Begleitperson aus dem Unternehmen, die das Vorgehen protokolliert.

- Es werden grundsätzliche keine Gespräche der Ermittlungsbeamten mit Mitarbeitern zugelassen. Befragungen und Vernehmungen erfolgen gesondert.
- Die Ermittlungsbeamten bedienen die IT nicht selbst. Das macht ein Mitarbeiter des Unternehmens im Beisein des Ermittlungsbeamten.
- Bei Vernehmungen und Befragungen ist bestenfalls ein anwaltlicher Zeugenbeistand hinzuziehen. Jedenfalls aber sollte ein leitender Mitarbeiter zusätzlich anwesend sein.
- Nach der Durchsuchung findet eine Besprechung aller Mitarbeiter, die die Durchsuchung begleitet haben, statt und der Ablauf wird in einem Protokoll festgehalten.
- Stellen Sie klar und lassen Sie es im Durchsuchungsprotokoll vermerken, dass nichts freiwillig herausgegeben, sondern alles beschlagnahmt wurde. Das ist entscheidend, wenn es später um Ihre Rechte geht und wenn Sie Ihren Kunden erklären müssen, warum deren Daten bei den Strafverfolgungsbehörden sind.
- Lassen Sie sich von den Ermittlungsbeamten das Verzeichnis der beschlagnahmten Gegenstände aushändigen.

Trennung der Kundendaten

Wenn Sie als Dienstleister die Daten von Kunden verarbeiten, dann müssen Sie diese getrennt verarbeiten. Das ist bereits eine datenschutzrechtliche Pflicht, die sich aus §9 BDSG nebst Anlage zu §9 BDSG (Trennungsgebot) ergibt. Hier kann eine virtuelle Trennung auf derselben Hardware ausreichend sein. Diese muss mit Blick auf Ermittlungsmaßnahme so gestaltet sein, dass bei einem Zugriff auf die Daten, nur die Daten eines einzelnen Kunden eingesehen werden können und diese isoliert werden können, um sie den Ermittlungsbehörden als Kopie oder Image zu übergeben. Klären Sie das mit Ihrem IT-Dienstleister.

Sie sollten aber auch unter dem Aspekt von Ermittlungsmaßnahmen die Daten so getrennt haben, dass die Herausgabe oder der Zugriff der Ermittlungsbehörden auf die relevanten Daten beschränkt ist. Wenn Sie ernsthaft mit Beschlagnahmen rechnen müssen, dann sollten die Daten auf unterschiedlicher Hardware verteilt sein, sodass bei der Mitnahme durch die Ermittlungsbehörden nur die Daten des entsprechenden Kunden bzw. Auftraggebers und nicht auch weitere mitgenommen werden. Insbesondere dann, wenn die Inhalte „aus der Verkehr gezogen werden sollen“, weil diese selbst inkriminiert sind (bspw. strafrechtlich verbotene Inhalte oder Verletzungen Gewerblicher Schutzrechte), werden die Ermittlungsbehörden sich nicht mit einer Kopie der Daten bzw. einem Image einverstanden erklären.

Vorbereitet zu sein, ist für beide Seiten gut

Wenn Sie auf Ermittlungsmaßnahmen gut vorbereitet sind, entsteht nicht so viel Stress. Es werden Fehler vermieden und die Angelegenheit verläuft schneller und geräuschloser, was wiederum Zeit und Geld spart.

Verarbeiten Sie Daten von Kunden oder Dritten, ist es eine Frage der Compliance, mit einem entsprechenden Vorgehensplan auf Ermittlungsmaßnahmen vorbereitet zu sein. Gesetzeskonformität bedeutet hier die Vermeidung von Schadensersatzansprüche infolge einer unberechtigten Herausgabe von Daten oder eines (System-) Ausfalls anlässlich von Ermittlungsmaßnahmen. Auch hier gilt wie in der IT-Security: „Plan-Do-Check-Act“-Vorbereitung vermeidet Kosten!

Jens Eckhardt
und Konrad Menz

Rechtsanwalt Dr. Jens Eckhardt ist Fachanwalt für IT-Recht, Datenschutz-Auditor (TÜV) bei Derra, Meyer & Partner. Rechtsanwalt Konrad Menz ist Fachanwalt für Strafrecht, und Fachanwalt für Steuerrecht in derselben Kanzlei.