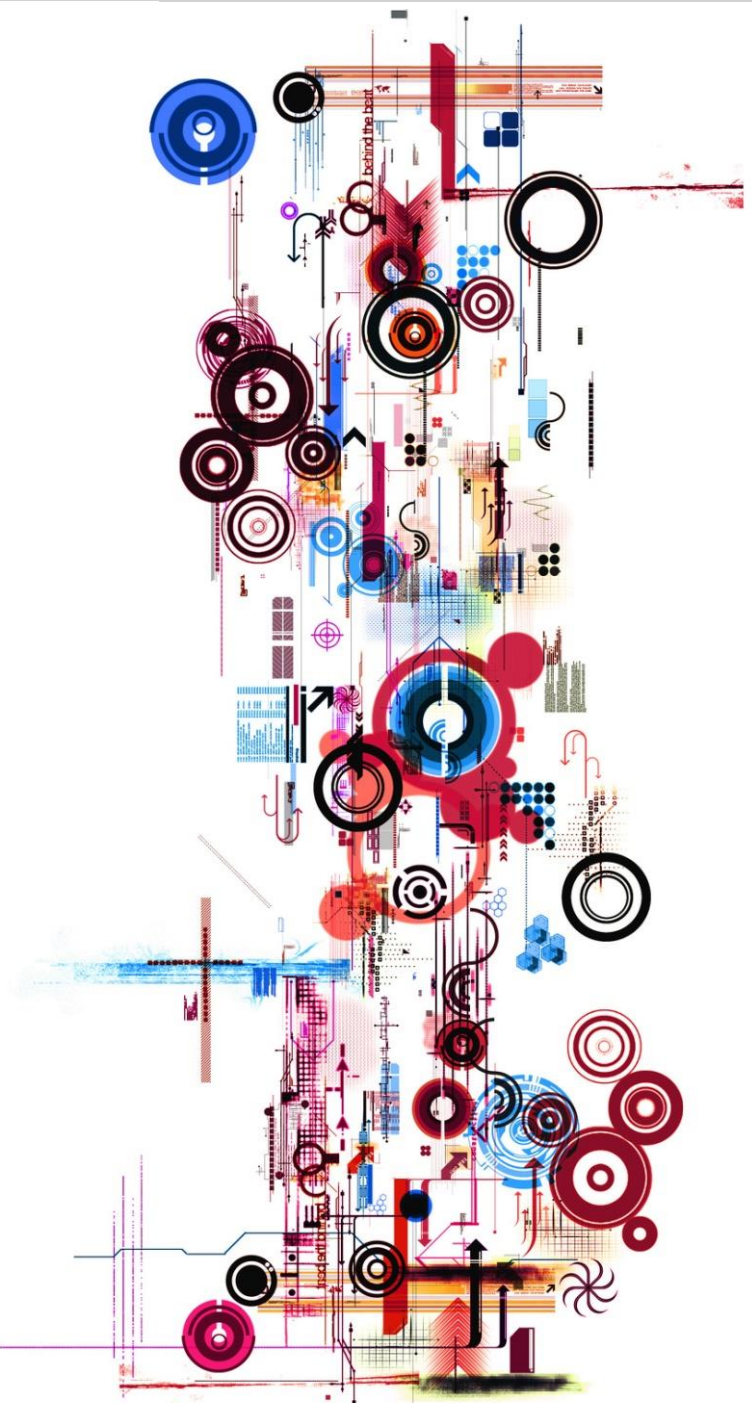


Der Zugriff von Ermittlungsbehörden auf die IT des Rechtsanwalts

Die Beschlagnahme von Daten, Servern, E-Mail-
Postfächern und die Herausgabe von Passwörtern



Einführung

- Durchsuchungen und Beschlagnahmen ohne Bezug auf Datenbestände sind heutzutage nicht mehr denkbar
- die gesetzlichen Regelungen für Durchsuchung und Beschlagnahme sind aber auf körperliche Gegenstände zugeschnitten
 - Rechtsunsicherheit
- Verhaltenshinweise für die Durchsuchung beim Rechtsanwalt gibt es überall; jüngst *Dann*, NJW 2015, 2609
- Organisationshinweise für das Vorfeld einer Durchsuchung gibt es kaum



Referent: Michael Reinhart

Mögliche Eingriffsschienen:

1. Durchsuchung gem. §§ 102 ff. StPO
 - Objekte: Wohnungen, Geschäfts- und sonstige Räume; Personen; Sachen (auch Computer, externe Speichermedien, Hand-Heids)
 - Zweck: Ergreifung des Verdächtigen; Auffinden von Spuren und Beweismitteln
 - Voraussetzung: Anfangsverdacht; offene Vorgehensweise
2. Sicherstellung und Beschlagnahme gem. §§ 94 ff. StPO
 - Objekte: bewegliche Sachen jeder Art, auch Datenträger; digital gespeicherte Informationen, wohl einschließlich Cloud-Inhalten (dazu *Dalby* CR 2013, 361)
 - Zweck: Beweissicherung
 - Voraussetzung: Anfangsverdacht; offene Vorgehensweise
3. Überwachung der Telekommunikation gem. §§ 100a f. StPO
 - Objekt: Telekommunikation als Vorgang des Aussendens, Übermittels und Empfanges von Nachrichten
 - Zweck: Aufklärung schwerer Straftaten; Aufenthaltsermittlung des Täters
 - Voraussetzung: Anfangsverdacht einer Katalogtat gem. § 100a Abs. 2 StPO; Tatschwere im Einzelfall; verdecktes Vergehen

Referent: Ihr Name

BEI WEM DARF DURCHSUCHT WERDEN?

1. Gem. § 102 StPO beim Verdächtigen wegen

- nicht mandatsbezogener Straftaten (z.B. eigener Steuerhinterziehung)
- mandatsbezogener Straftaten (z.B. Untreue, Parteiverrat, Geheimnisverrat, Gebührenüberhebung)
- Unterstützung von Straftaten des Mandanten

2. Gem. § 102 StPO beim Unverdächtigen wegen

- Straftaten des Mandanten
- Straftaten Dritter (auch seiner Angestellten)

kein vollständiger Ausschluss durch § 160a Abs. 1 S. 1 StPO

WO DARF DURCHSUCHT WERDEN?

1. „Beim“ Betroffenen, d.h. in dessen räumlichem Herrschaftsbereich im Inland
2. Problemfall: externe Speicher
 - Erstreckung der Durchsuchung auf den Speicherort, wenn bekannt und im Inland (§ 103 StPO)
 - Durchsicht des externen Speichermediums gem. § 110 Abs. 3 StPO:
„Die Durchsicht eines elektronischen Speichermediums bei dem von der Durchsuchung Betroffenen darf auch auf hiervon räumlich getrennte Speichermedien, soweit auf sie von dem Speichermedium aus zugegriffen werden kann, erstreckt werden, wenn anderfalls der Verlust der gesuchten Daten zu besorgen ist. Daten, die für die Untersuchung von Bedeutung sein, können, dürfen gespeichert werden; § 98 Abs. 2 gilt entsprechend.“

Referent: Michael Reinhart

WAS GILT BEI CLOUD-STORAGE?

1. § 110 Abs. 3 StPO, wenn Speicherung im Inland (Souveränitätsprinzip); weitergehend *Meyer-Goßner/Schmitt*, § 110 StPO Rn. 7b, *Wicker MMR* 2013, 765: auch bei Speicherung im Ausland, wenn Zugriff über Computer im Inland und Account des Betroffenen
2. Art. 32 lit. a Cybercrime-Convention für offen zugängliche Daten im Konventionsgebiet
3. Völkergewohnheitsrecht (*Gehrke*, *StraFo* 2009, 272) für offen zugängliche Daten außerhalb des Konventionsgebiets
4. Art. 32 lit. b Cybercrime-Convention bei Zustimmung des Verfügungsberechtigten für nicht frei zugängliche Daten im Konventionsgebiet

Referent: Michael Reinhart

WIE WIRD DURCHSUCHT?

1. Aufgrund richterlichen Durchsuchungsbeschlusses (§ 105 Abs. 1 S. 1 StPO), der nicht älter ist als sechs Monate (BVerfG NJW 1997, 2165); bei Gefahr im Verzug auf (mündliche) Anordnung durch StA oder Polizei
2. regelmäßig nicht zur Nachtzeit, s. § 104 StPO
3. in Anwesenheit des Betroffenen § 106 StPO
4. bei Kanzleiräumen regelmäßig im Beisein eines Staatsanwalts; fehlt dieser, müssen zwei Zeugen hinzugezogen werden, die weder Volljuristen noch gar Rechtsanwältinnen zu sein brauchen (LG Landshut, Beschluss v. 31.08.2011 - 6 Qs 92/11)

Referent: Michael Reinhart

WIE ERFOLGT DIE DURCHSUCHUNG VON COMPUTERN?

1. Es gelten die allgemeinen Formalia
2. Durchsuchungsbeschluss berechtigt auch zur Inbetriebnahme von EDV-Anlagen
3. § 110 Abs. 3 StPO
4. Verhältnismäßigkeitsgrundsatz gewinnt besondere Bedeutung
 - besteht milderes Mittel (z.B. Befragen von Zeugen, freiwillige Herausgabe von Unterlagen durch Dritte)?
 - wie kann Suche eingegrenzt werden (mittels Ordnungskriterien, Suchbegriffen u.a.m.)? Beschlagnahme des gesamten Datenbestands ist regelmäßig unzulässig, BVerfGE 113, 29; EGMR, NJW 2013, 3081
 - rechtfertigt die Schwere des Verdachts und/oder der Tat eine Durchsuchung?
 - ist der Verdacht überhaupt konkret genug?
5. Online-Durchsuchung ist unzulässig

DÜRFEN DATEN VOR ORT GESICHTET WERDEN?

1. Durch Staatsanwaltschaft und deren Ermittlungsbeamte, wenn dies durch die StA angeordnet ist, § 110 Abs. 1 StPO
2. Durch Steuerfahndung und Zollfahndung, § 404 S. 2 AO
3. „Papiere“ sind auch Daten
4. Für die Durchsicht darf eigene Soft- und Hardware der Ermittlungsbehörden verwendet werden
5. Es dürfen Hilfspersonen (EDV-Fachleute) hinzugezogen werden
6. „Grobsichtung“ von Daten durch nicht ermächtigte Beamte? (s. *Meyer-Göbner* § 110 Rn. 4 und KK-Nack § 110 Rn. 7)

Referent: Michael Reinhart

WIE WERDEN DATEN SICHERGESTELLT?

1. § 94 Abs. 1 StPO Inverwahrnehmung oder auf anderer Weise
2. „Gegenstände“ sind jedenfalls die Datenträger; deshalb: grundsätzlich dürfen die Originaldatenträger in Verwahrung genommen werden
3. aber: es gibt regelmäßig mildere Mittel:
 - Anfertigung und Inverwahrnehmung von (Teil-)Kopien
 - direktes Überspielen von Daten auf Speichermedien der Ermittlungsbehörden
4. Ausnahme: bei Verdacht auf verschlüsselte, verschleierte, verborgene Daten bleibt es bei Sicherstellung des Originaldatenträgers
5. Möglichste Schonung von vertraulichen Daten Dritter (insbesondere Mandanten)
6. Beschleunigte Auswertung und Rückgabe von Originaldatenträgern (AG Reutlingen, Beschluss v. 05.12.2011, 5 Gs 363/11)

Referent: Michael Reinhart

WIE WERDEN E-MAILS SICHERGESTELLT?

1. E-Mails auf Server des Providers oder Speichermedien des Betroffenen: § 94 StPO (unabhängig davon, ob gelesen oder nicht, archiviert oder nicht)
2. E-Mails während des Sende- oder Abrufvorgangs: § 100a StPO; BVerfGE 124, 43)
3. verdeckter Zugriff auf abgelegte E-Mails: § 100a StPO
4. Verhältnismäßigkeit:
 - Vollzugriff auf E-Mail-Postfach regelmäßig unverhältnismäßig (BGH NJW 2010, 1297)
 - Vorsortierung anhand von Ordnungskriterien, Suchbegriffen u.ä.
 - Wahrung der Privat- und Intimsphäre

WAS GILT FÜR PASSWÖRTER UND ZUGANGHILFEN?

1. Verkörperte und gespeicherte Passwörter können sichergestellt werden (LG Trier NJW 2004, 869)
2. Gleiches gilt für Unterstützungsssoftware (z.B. Entschlüsselungsprogramme)
3. Der Beschuldigte muss nicht-verkörperte Passwörter nicht nennen (nemo-tenetur-Prinzip)
4. Zeugen sind aussage- und wahrheitspflichtig, es sei denn:
 - Auskunftsverweigerungsrecht gem. § 55 StPO
 - Zeugnisverweigerungsrecht gem. § 53 Abs. 1 Nr. 2, 3 StPO? Passwörter dem Anwalt anvertraut oder sonst bekannt geworden?

Referent: Michael Reinhart

WAS DARF NICHT BESCHLAGNAHMT WERDEN?

1. Beschlagnahmeverbot des § 97 Abs. 1 Nr. 1 - 3 StPO
 - nur für Beziehung Anwalt - Beschuldigter
 - nur bei Gewahrsam des Anwalts
 - auch Datenträger (vgl. § 11 Abs. 3 StGB)
 - nicht bei Teilnahmeverdacht oder bei Einziehungsgegenständen (§ 97 Abs. 2 S. 3)
 - Sonderfall: Mitteilungen an Unternehmensanwalt
2. Beschlagnahmeverbot gem. § 160a StPO?
 - Verhältnis zu § 97 StPO strittig; mittlerweile wohl h. M.: § 97 StPO geht vor (so z.B. *Meyer-Göbner/Schmitt*, § 160a Rn. 17 m.w.N.)

KANN DIE DURCHSUCHUNG AD HOC NOCH VERHINDERT WERDEN?

1. Regelmäßig: Nein!
2. Möglich ist nur:
 - Widerspruch gegen die Art und Weise der Durchsuchung
 - Widerspruch gegen Umfang der Durchsuchung und Beschlagnahme
 - Versiegelung von sichergestellten Gegenständensämtlich ohne aufschiebende Wirkung

Referent: Michael Reinhart

WELCHE RECHTSMITTEL GIBT ES?

1. Gegen nicht-richterliche Anordnungen von Durchsuchung oder Beschlagnahme:
Antrag auf gerichtliche Entscheidung § 98 Abs. 2 S. 2 StPO (analog)
2. Gegen richterliche Anordnungen: Beschwerde § 304 StPO
3. Antrag auf richterliche Zwischenverfügung, um Verwertung vorläufig zu verhindern
4. Rechtsbehelfe sind nicht fristgebunden
5. Sie stehen auch Drittbetroffenen zu (EGMR NJW 2008, 3409)
6. Fazit: „Das Rechtssystem der StPO ist schwer zu durchschauen.“

Referent: Michael Reinhart

SIND RECHTSMÄßIG ERLANGTE BEWEISE UNVERWERTBAR?

1. Ja
2. Bei schwerwiegenden, bewussten oder willkürlichen
Verfahrensverstößen: Ja
3. im Übrigen: Nein

Referent: Michael Reinhart



BEKOMMT MAN BESCHLAGNAHME DATEN, DATENTRÄGER ETC. ZURÜCK?

1. Nach rechtskräftigem Abschluss des Verfahrens
2. Es sei denn, sie unterliegen der Einziehung
3. Vorher nur, wenn sie nicht mehr zu Beweiszwecken benötigt werden
4. Kopien auf eigene Kosten sind meist möglich

Referent: Michael Reinhart

DURCHSUCHUNGSPRÄVENTION: KANN MAN KONKRETE VORBEREITUNGEN FÜR EINE DURCHSUCHUNG TREFFEN?

Ja:

- Herstellen von Kopien bei Daten und Akten
- Separieren wahrscheinlicher Durchsuchungsgegenstände
- Einholen von Schweigepflichtentbindungen



Referent: Michael Reinhart

DURCHSUCHUNGSPRÄVENTION: WIE IST DIE AKTENFÜHRUNG ZU ORGANISIEREN?

1. Aktenvollständigkeit: kein papierloses Büro
2. Aktenwahrheit: was auf der Akte steht, muss auch drin sein
3. Aktentransparenz: jede Akte muss so geführt werden, dass auch ein Dritter sich darin zurechtfindet
4. Aktenpräsenz: jede Akte muss schnell aufzufinden sein

Referent: Michael Reinhart

DURCHSUCHUNGSPRÄVENTION: WIE SIND DATEN ZU ORGANISIEREN?

1. DATENKLARHEIT: keine kryptischen Dateinamen, keine Verschlüsselung
2. DATENSTRUKTUR: klare Mandatszuordnung, übersichtliche Ordner
3. DATENREDUNDANZ: Kopien auf abtrennbaren Speichermedien
4. DATENZURÜCKHALTUNG: Briefe oder Faxschreiben statt E-Mail

Referent: Michael Reinhart

DURCHSUCHUNGSPRÄVENTION: WAS IST MIT PASSWÖRTERN?

1. Die sichere Organisation der Daten erfordert Passwortsicherung
2. Passwörter sollten aber nur mit Einverständnis der Mandanten herausgegeben werden
 - entweder Einverständnis bereits bei Mandatsbegründung schriftlich einholen
 - oder so schnell wie möglich bei der Durchsichtung einholen

GEHT CLOUD-STORAGE?

1. Aus strafprozessualer Sicht: ja, ist möglicherweise sogar ein „Rettungsanker“
2. materiell strafrechtlich: wohl nicht, wegen § 203 StGB

Referent: Michael Reinhart

WAS MUSS DAS PERSONAL WISSEN?

1. Kenntnis der allgemeinen Verhaltensregeln
2. Training für Rolle als Durchsuchungszeugen
3. Sorgfalt bei Akten- und Datenhandhabung

Referent: Michael Reinhart



SIND RECHTSMITTEL ANZURATEN?

Einzelfallentscheidung:

- Verzögerungstaktik?
- Verfahrensklima?
- Erfolgsaussichten?
- Absicherung gegenüber eigenen Mandanten?

Referent: Michael Reinhart

Vielen Dank für Ihre Aufmerksamkeit!
Ihre Fragen?

Referent: Michael Reinhart



Roxin Rechtsanwalte LLP

Michael Reinhart

Brienner Str. 9

80333 Munchen

Tel.: 089 / 2444386 - 00

Fax: 089 / 2444386 - 66

muenzen@roxin.de

www.roxin.de

Referent: Michael Reinhart