EuroCloud DEUTSCHLAND | eco

Verband der Cloud-Computing-Wirtschaft

Leitfaden für

IT-, Daten- und Service-Provider

Durchsuchung als wichtiger Bestandteil der IT-Security-Policy

Wir fördern Kompetenzen.
Wir schaffen Transparenz.

Leseprobe!
Kapitel 9 bis 11

www.eurocloud.de

Impressum

EuroCloud Deutschland_eco e. V.
Lichtstraße 43h
50825 Köln
Tel.: 0221 / 70 00 48 – 0
Fax: 0221 / 70 00 48 – 111
E-Mail: info@eurocloud.de
Web: www.eurocloud.de

Vereinsregister:
Amtsgericht Köln – VR 16215

Sitz des Vereins:
Köln

Mitherausgeber:
Derra, Meyer & Partner Rechtsanwälte PartGmbB

Inhalt

Vorwort

Liebe Leserinnen und Leser,

wenn der Staatsanwalt zwecks Durchsuchung klingelt, dann kommt er stets unangekündigt. Genauso wie Polizei, Steuer- und Zollfahndung sowie andere Ermittlungsbehörden mit entsprechendem richterlichen Durchsuchungsbeschluss. Worauf dürfen diese zugreifen und wie gelingt Ihr Balanceakt zwischen Kooperation und Verpflichtungen gegenüber Ihren Kunden?

Dieser Leitfaden klärt Sie über Ihre Rechte sowie Pflichten auf und bereitet Sie auf den Ernstfall vor, damit Sie ruhig und besonnen reagieren können. Dabei müssen Sie sich im Klaren sein: Die Ermittlungen bedeuten ein legales Durchbrechen der technischen und organisatorischen Maßnahmen, die Ihre IT vor Angriffen und Ausfällen schützen sollen. Je nach Verlauf kann die Durchsuchung dieselben Auswirkungen wie ein IT-Sicherheitsvorfall haben. Deshalb sollten Sie die Vorbereitung auf eine Durchsuchung als Bestandteil Ihrer IT-Security-Policy verstehen.

Schwerpunktmäßig behandelt der Leitfaden die Situation, in der Ihr Unternehmen – oder die Organe Ihres Unternehmens (Vorstand, Geschäftsführer) – nicht als Beschuldigter, sondern als allgemein Auskunftspflichtiger betroffen ist. Für gewöhnlich sind die Organe und Mitarbeiter des Unternehmens dann Zeugen in einem Ermittlungsverfahren gegen einen Dritten.

Dabei konzentriert sich der Leitfaden vor allem auf IT-, Daten- und Service-Provider. Ob Sie zum Kreis potenziell Betroffener gehören, die in Kontakt mit den Ermittlungsbehörden geraten, hängt davon ab, welche Dienste Sie anbieten und wer Ihre Kunden oder Auftraggeber sind. Host-Provider und Internetzugangsanbieter werden sicherlich häufiger von Ermittlungsbehörden kontaktiert als beispielsweise Anbieter von Call-Center-Leistungen. Wenn es ernst wird, ist die Situation aber für alle gleich …

Wir wünschen Ihnen viele wertvolle Erkenntnisse beim Lesen des Leitfadens und danken den Autoren herzlich für ihr Engagement.

Köln, den 1. März 2018

Andreas Weiss
Direktor, EuroCloud Deutschland_eco e. V.

9 Die richtige Vorbereitung

Vorbereitet zu sein, ist für beide Seiten gut. Wenn Sie auf Ermittlungsmaßnahmen gut vorbereitet sind, entsteht nicht so viel Stress. Sie vermeiden Fehler und die Angelegenheit verläuft schneller und „geräuschloser“, was wiederum Zeit und Geld spart.

9.1 Services einordnen – Daten trennen

Die richtige Vorbereitung setzt die Bewertung und Einordnung der eigenen Services voraus. Hier gilt nicht „one size fits all“. Davon ausgehend müssen aus rechtlicher Sicht die Risiko-Konstellationen bestimmt und bewertet werden.

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 Schadensersatzansprüchen infolge einer unberechtigten Herausgabe von Daten oder eines (System-)Ausfalls anlässlich von Ermittlungsmaßnahmen.

Verarbeiten Sie als Provider die Daten mehrerer Kunden, dann müssen Sie diese getrennt verarbeiten. Das ist bereits eine datenschutzrechtliche Pflicht, die sich aus § 9 BDSG nebst Anlage zu § 9 BDSG (Trennungsgebot) ergibt. Unter der DS-GVO wird sich ab dem 25.05.2018 kein geringeres Schutzniveau ergeben. Eine virtuelle Trennung auf derselben Hardware kann ausreichend sein. Diese muss beispielsweise mit Blick auf Ermittlungsmaßnahmen so gestaltet sein, dass bei einem Zugriff nur die Daten eines einzelnen Kunden eingesehen und diese isoliert werden können, um sie den Ermittlungsbehörden als Kopie oder Image zu übergeben. Klären Sie vertraglich mit dem Kunden, was geht und was nicht.

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 die Ermittlungsbehörden ausschließlich die Daten des entsprechenden Kunden beziehungsweise Auftraggebers mitnehmen können. Insbesondere dann, wenn die Inhalte „aus dem Verkehr gezogen werden sollen“, weil diese selbst inkriminiert sind (beispielsweise strafrechtlich verbotene Inhalte oder Verletzungen gewerblicher Schutzrechte), werden die Ermittlungsbehörden sich nicht mit einer Kopie der Daten beziehungsweise einem Image einverstanden erklären.

9.2 Testlauf zwingend erforderlich

Im Rahmen der Vorbereitung brauchen Sie stets einen eingespielten Organisationsplan für den konkreten Ernstfall. In der IT-Sicherheit nutzt Ihnen auch die beste Notstromversorgung nichts, wenn sie im Ernstfall nicht anspringt

und nicht bedient werden kann. Klären Sie unbedingt die Zuständigkeiten im Unternehmen für den Fall einer Durchsuchung.

Wie im Bereich IT-Sicherheit üblich, muss der Ablauf konkret getestet werden, denn auch hier gilt, dass sich die echten Probleme erst beim Test zeigen.

Verstehen Sie die Ermittlungsmaßnahmen – insbesondere die Durchsuchung und Beschlagnahme – als legale Umgehung der IT-Sicherheitsmaßnahmen im Unternehmen. Denn die IT-Sicherheit kann technisch noch so gut sein, die Ermittlungsbehörde kommt dennoch legal an die Beweismittel. Auch hier gilt wie überall in der IT-Security: Plan – Do – Check – Act. Vorbereitung vermeidet Kosten!

9.3 Wichtige Parameter

Die wichtigsten festzulegenden Parameter und Verantwortlichkeiten einer Ablaufbeschreibung für das Szenario einer Durchsuchung sind:

- Wer hat wen zu informieren (zu denken ist an: Geschäftsleitung, Strafverteidiger beziehungsweise Rechtsanwalt, …)?
- Wer kümmert sich darum, die Beamten zu empfangen und ohne erkennbare Beeinträchtigung des Geschäftsbetriebes in einen separaten Raum zu begleiten?
- Wer koordiniert seitens des Unternehmens die Kommunikation mit dem leitenden Ermittlungsbeamten und den vor Ort eingetroffenen Anwälten des Unternehmens?
- Welche Mitarbeiter sind dafür zuständig, die Ermittlungsbeamten im Haus zu begleiten und die mit den Beamten gewählten oder von diesen bestimmten Vorgehensweisen zu protokollieren?
- Inwiefern dürfen die Mitarbeiter kooperieren – und wo liegen die Grenzen? Seien Sie in Bezug auf das, was Sie zulassen, präzise und restriktiv, damit es für die Mitarbeiter nicht zu Entscheidungsspielräumen kommt. Briefen Sie diese entsprechend.
- Welche Auskünfte sind erlaubt? Geben Sie klare Dienst-/Arbeitsanweisungen, dass Zeugenvernehmungen in den Geschäftsräumen nicht erlaubt sind.
- Wer ist im Betrieb legitimiert, Widerspruch gegen die Sicherstellung von Daten oder Gegenständen einzulegen, sodass nur der hoheitliche Akt der Beschlagnahme bleibt?
- Wer sorgt für die Vollständigkeit des Sicherstellungsverzeichnisses und nimmt es entgegen?
- Wer fertigt ein Protokoll über den Verlauf der Durchsuchung in Rücksprache mit allen beteiligten Mitarbeitern an?

10 Umgang mit „Beweissicherungsverlangen“ der Strafverfolgungsbehörden

Für Privatpersonen oder private Unternehmen gibt es grundsätzliche keine Verpflichtung, an Ermittlungen und Ermittlungsmaßnahmen der Strafverfolgungsbehörden mitzuwirken oder diese aktiv zu unterstützen. Allerdings ist zu beachten: Wer Daten vernichtet/löscht, die zu Beweiszwecken in Ermittlungsverfahren verwandt werden können, kann sich zum Beispiel wegen Strafvereitelung (§ 258 StGB) strafbar machen.

Problematisch wird es immer dann, wenn Mitarbeiter oder Verantwortliche des Unternehmens Kenntnis von Daten mit strafbarem Inhalt haben oder wissen, dass gespeicherte Daten Relevanz für ein Ermittlungsverfahren aufweisen können. Entsteht diese Kenntnis durch ein Herantreten der Ermittlungsbehörden an das Unternehmen, müssen diese Daten im Rahmen der gesetzlichen Verpflichtungen aus den Regelungen des TKG und TMG gespeichert und am besten auf externen Datenträgern gesichert werden. Auch hier gilt, wie bei einem Auskunftsverlangen der Ermittlungsbehörden, dass darauf zu bestehen ist, dass von den Ermittlungsbehörden ein solches „Beweissicherungsverlangen“ schriftlich und unter Angabe der gesetzlichen Rechtsgrundlagen zu stellen ist. Keinesfalls sollte vorschnell gehandelt werden und auf „erstes Zurufen“ der Polizei oder Staatsanwaltschaft weitergehende Daten, außerhalb der ohnehin bestehenden Verpflichtung nach dem TKG (§§ 113, 95, 111) und TMG, gespeichert oder gar herausgegeben werden. Anderenfalls könnten Ordnungswidrigkeiten oder gar Straftaten wegen Verstößen gegen unter anderem Datenschutzregularien verwirklicht werden.

Im Ergebnis ist daher festzustellen, dass außerhalb der Verpflichtungen nach dem TKG (§§ 95 und 111) i. V. m. § 100j StPO keinerlei Verpflichtung besteht, einem Beweissicherungsverlangen der Ermittlungsbehörden Folge zu leisten. Natürlich ist auch hier zur Vermeidung eines größeren Aufwands oder weitergehender Ermittlungs- und Zwangsmaßnahmen auf Deeskalation zu achten und im Rahmen des gesetzlich Zulässigen, ruhig und verhältnismäßig zu reagieren. In Zweifelsfällen sollte stets ein Fachanwalt für Strafrecht hinzugezogen werden.

11 Kenntnisse über strafrechtlich Relevantes

Wie sollten Sie damit umgehen, wenn Sie potenziell strafrechtlich Relevantes entdecken oder darauf hingewiesen werden?

11.1 Anzeigepflicht prüfen

In diesem Zusammenhang ist zunächst klarzustellen, dass für private Personen und Privatunternehmen nur für die in § 138 StGB explizit genannten Strafta-

ten eine Anzeigepflicht besteht. Bei den dort genannten Straftaten handelt es sich allesamt um schwere Straftaten des Friedens- und Hochverrats, staatsgefährdende oder terroristische Straftaten, aber auch Mord und Totschlag, Straftaten gegen die persönliche Freiheit, Raub, räuberische Erpressung und gemeingefährliche Straftaten wie Brandstiftung.

Diese Anzeigepflicht von geplanten und/oder bereits begangenen Straftaten ist in § 138 StGB abschließend aufgezählt. Eine darüber hinausgehende Pflicht zur Anzeige von Straftaten besteht nicht. Sind Sie unsicher, ob eine solche Anzeigepflicht besteht, sollten Sie auch hier einen Fachanwalt für Strafrecht zurate ziehen.

Darüber hinaus besteht in bestimmten Fällen eine Pflicht zur Meldung von Verdachtsfällen, beispielsweise nach § 11 Abs. 1 des Geldwäschegesetzes. Auch hier kann die Nichtanzeige zu einer Ordnungswidrigkeit führen, die mit Geldbußen geahndet werden kann.

Außerhalb dieser gesetzlich geregelten Fälle existiert kein Straftatbestand der „Mitwisserschaft". Allerdings könnten Mitarbeiter des Unternehmens in den Verdacht der Beihilfe zu einer strafbaren Handlung eines anderen gelangen. Wegen des fehlenden Vorsatzes wird dies jedoch regelmäßig ausscheiden, es ist aber gleichwohl nicht auszuschließen, dass die Strafverfolgungsbehörden ein Ermittlungsverfahren einleiten. Daher ist es wichtig, vorzusorgen und möglichst frühzeitig durch Aufklärung etwaige Verdachtsmomente auszuräumen.

11.2 Verhaltensanweisungen festlegen

Es versteht sich von selbst, dass weder Sie noch Ihr Unternehmen sich zum „Helfershelfer" von Straftätern gerieren möchten. Dies sollten Sie durch entsprechende Regelungen in Ihren AGBs klarstellen und darauf hinweisen, dass die Nutzung Ihrer Dienstleistungen für strafbare Handlungen untersagt ist und zur Kündigung des Vertragsverhältnisses sowie zur Strafanzeige führt.

Um selbst nicht in den Verdacht strafbaren Handelns zu gelangen, sollten Sie mit den Ermittlungsbehörden kooperieren und bei Kenntnis von begründeten Verdachtsfällen entsprechende Daten beweisfest sichern – also dokumentieren wann, was, von wem, aus welchem Anlass und mit welchem Inhalt gesichert wurde. Zudem sollten Sie die Geschäftsbeziehung beenden und parallel die Strafverfolgungsbehörden informieren. Dieses Vorgehen sollte zudem im Rahmen eines transparenten Compliance-Systems mit konkreten Verhaltensanweisungen für alle Mitarbeiter implementiert sein.

11.3 eco Beschwerdestelle – nicht polizeiliche Meldemöglichkeiten

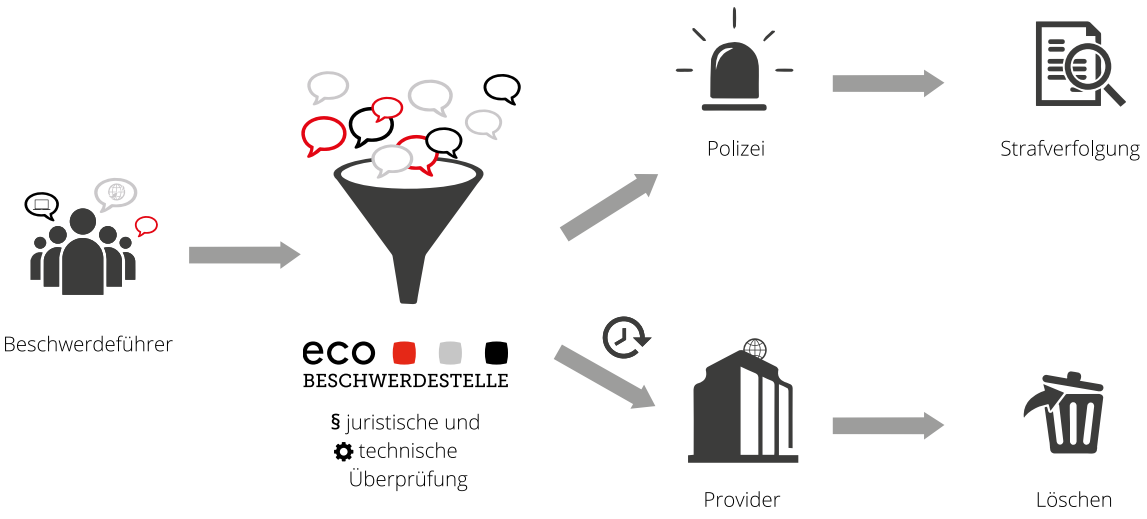
Die eco Beschwerdestelle bekämpft seit über 15 Jahren illegale Inhalte im Netz. Sie ist in das System der regulierten Selbstregulierung eingebettet und hat insbesondere auch die Aufgabe, den Jugendschutz im Internet zu verbessern.

Internetnutzer, die auf illegale, insbesondere jugendgefährdende Internetinhalte stoßen, oder Internet Service Provider (ISP), die solche Inhalte auf ihren eigenen Servern vorfinden, können diese kostenlos und anonym unter https://beschwerdestelle.eco.de oder per E-Mail an hotline@eco.de melden. Zu solch strafrechtlich relevanten Inhalten gehören zum Beispiel:

- jugendgefährdende und entwicklungsbeeinträchtigende Inhalte,
- frei zugängliche Erwachsenenpornografie, Gewalt-, Tier-, Kinder- und-Jugendpornografie,
- entgeltliches Herstellen beziehungsweise Verschaffen von Nacktbildern Minderjähriger,
- Verbreitung von Kennzeichen und Propaganda verfassungswidriger Organisationen,
- Volksverhetzung,
- Anleitung oder Aufforderung zu Straftaten,
- extreme Gewaltdarstellungen,
- Grooming oder
- unerlaubte Zusendung von Werbemails und Newslettern.

Das eco Beschwerdestellenteam besteht aus Mitarbeitern mit juristischer Ausbildung, die eingehende Beschwerden zunächst einer umfassenden juristischen Vorprüfung unterziehen. Sollten die gemeldeten Inhalte rechtswidrig sein, wird je nach Verstoß die Polizei und/oder der ISP informiert. Dabei werden die konkreten Inhalte samt Fundquelle eindeutig benannt und die rechtliche Begründung dargelegt, gegebenenfalls wird auf bereits erstellte Strafanzeige hingewiesen.

Vereinfachte Darstellung für die Bearbeitung deutscher Fälle



Für die effektive Bekämpfung illegaler Internetinhalte kooperiert die Beschwerdestelle unter anderem mit Providern, Partnerbeschwerdestellen und Strafverfolgungsbehörden. Zudem ist eco Gründungsmitglied des internationalen Netzwerks von Beschwerdestellen (INHOPE) und Teil des deutschen Safer Internet Center. Diese Kooperationen helfen bei dem Ziel, die Inhalte schnell an der Quelle zu entfernen, damit sie von keinen weiteren Personen mehr wahrgenommen werden können, sowie eine effektive Strafverfolgung zu gewährleisten und somit die Täter zur Verantwortung zu ziehen. Die eco Beschwerdestelle unterstützt zudem die Strafverfolgungsbehörden und ISP durch Austauschmöglichkeiten und Schulungen, insbesondere im Bereich Jugendmedienschutz, bei Policies und im Umgang mit Hinweisen auf rechtswidrige Inhalte.

Autoren

Rechtsanwalt Dr. Jens Eckhardt

Sozietät Derra, Meyer & Partner Rechtsanwälte, Düsseldorf, Ulm, Berlin
Fachanwalt für Informationstechnologierecht
Datenschutz-Auditor (TÜV)
Compliance-Officer (TÜV)
Mitglied des Vorstands des EuroCloud Deutschland_eco e. V.

Dr. Jens Eckhardt ist seit 2001 als Rechtsanwalt in den Bereichen Datenschutz, Informationstechnologie, Telekommunikation und Marketing tätig. Er promovierte zum Thema Telekommunikationsüberwachung. Er berät nationale und internationale Unternehmen in diesen Bereichen – sowohl strategisch (insbesondere beim Outsourcing, bei der Einführung von neuen Systemen, Prozessen, Technologien sowie bei Marketingstrategien und -technologien) als auch fallbezogen (insbesondere bei Anfragen durch Aufsichtsbehörden, gerichtlichen Auseinandersetzungen und Einzelfragen).

Rechtsanwalt Konrad Menz

Sozietät Derra, Meyer & Partner Rechtsanwälte, Ulm, Stuttgart
Fachanwalt für Strafrecht
Fachanwalt für Steuerrecht
Fachanwalt für Insolvenzrecht
Compliance-Officer (TÜV)

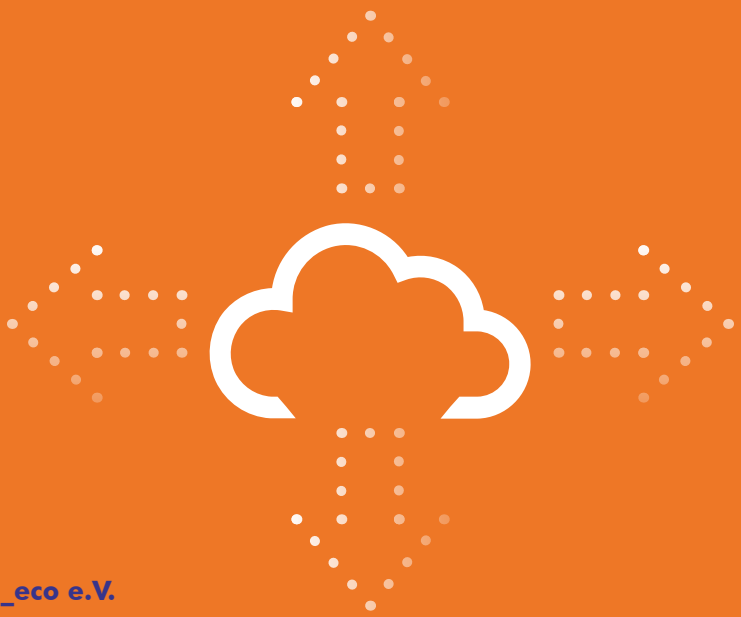
Konrad Menz verteidigt in allen Bereichen des Wirtschaftsstrafrechts. Mit seinen besonderen Kenntnissen unterstützt er zudem Unternehmen in der Risiko- und Präventivberatung. Hier vereint er die jahrelange praktische Erfahrung aus den Bereichen Straf-, Steuer- und Insolvenzrecht, um praxisbezogene Compliance-Strukturen zu etablieren und zu bewerten.

Rechtsanwalt Ralph E. Walker

Sozietät Derra, Meyer & Partner Rechtsanwälte, Ulm, Augsburg
Fachanwalt für Strafrecht

Ralph E. Walker bearbeitet ausschließlich strafrechtliche Mandate. Bereits von Anbeginn seiner beruflichen Laufbahn hat er sich ganz auf die Tätigkeit als Strafverteidiger konzentriert und spezialisiert. Rechtsanwalt Walker verteidigt bundesweit, wobei der Schwerpunkt auf Wirtschafts- und Insolvenzstrafrecht liegt. Durch seine langjährige Tätigkeit als Strafverteidiger vor Amts- und Landgerichten, aber auch durch Verteidigung vor dem Staatsschutzsenat des OLG München und OLG Stuttgart, verfügt Ralph E. Walker über herausragende Kenntnisse des Strafverfahrens- und Strafprozessrechts.

Verband der Cloud-Computing-Wirtschaft



EuroCloud Deutschland_eco e.V.
Lichtstraße 43h
50825 Köln

Tel.: 0221 / 70 00 48 – 0
Fax: 0221 / 70 00 48 – 111
E-Mail: info@eurocloud.de
Web: www.eurocloud.de