CHECKLISTEN
IT-FORENSIK IM UNTERNEHMEN

Checklisten zur Vorbereitung, Durchführung und Dokumentation einer IT-Ermittlung zur Beweissicherung

Mit freundlicher Empfehlung von:

audatis® Consulting - Datenschutz und Informationssicherheit
Datenschutz | Informationssicherheit | IT-Forensik | Sachverständige
Inh. Carsten Knoop
Wittekindstr. 3
32051 Herford

Fon: 05221 / 854 96 90
Fax: 05221 / 854 96 99

Mail: info@audatis.de
Web: www.audatis.de

1 Allgemeines

1.1 Bedeutung der IT-Forensik

Als „IT-Forensik“ bezeichnet man die Untersuchung von verdächtigen Vorfällen im Zusammenhang mit IT-Systemen (z.B. PC, Servern oder Smartphones) sowie der Feststellung ob ein „Incident“ bzw. „Sicherheitsvorfall“ (definiert als: technisch oder rechtlich erheblicher Vorfall) vorliegt.

Besteht der Verdacht auf eine Pflichtverletzung oder eine Straftat eines Mitarbeiters, so ist es die Aufgabe der IT-Forensik, den Tatablauf durch die Erfassung, Analyse und Auswertung digitaler Spuren in IT-Systemen zu belegen und den Täter zu identifizieren. Dabei müssen die Spuren für spätere Gerichtsprozesse verwertbar gesichert werden, ohne diese zu manipulieren oder zu zerstören.

Da immer mehr IT-Systeme in Unternehmen eingesetzt werden, steigt auch die Häufigkeit von Vorfällen, die erst mit Hilfe von IT-Systemen begangen werden können (z.B. Hacking eines Webservers) oder bei denen in Systemen genutzt werden und dabei „unsichtbare“ Spuren hinterlassen (z.B. unrechtmäßige Mitnahme von vertraulichen Unternehmensdaten).

Da für die Auswertung und Analyse von solchen Vorfällen im Regelfall Spezialkenntnisse und spezielle forensische Untersuchungswerkzeuge (Hardware und Software) benötigt werden und dabei auch die Unterbrechung der betroffenen IT-Systeme möglichst gering gehalten werden soll, ist die Einbeziehung eines Experten ein wichtiger Erfolgsfaktor.

1.2 Informationen über audatis Consulting

audatis Consulting ist auf die Beratung von Unternehmen im Bereich der Informationssicherheit und des Datenschutzes spezialisiert und hat seinen Sitz in Herford / Ostwestfalen. Seit 2012 unterhält audatis Consulting ebenfalls ein Büro in der Region Rhein-Main-Neckar.

Der Wirtschaftsinformatiker Carsten Knoop (M. Sc.) gründete das Unternehmen im Jahre 2010 und ist Sachverständiger für IT-Forensik, TÜV-zertifizierter Datenschutzauditor, IT-Security-Manager und ISO 27001 Auditor.

Er hat über 10 Jahre Erfahrungen im IT-Bereich gesammelt und war zuvor u.a. als Chief Information Security Officer (CISO) für einen internationalen Medienkonzern tätig.

Wir stehen Ihnen und Ihren Mandanten bundesweit als kompetenter Ansprechpartner rund um die gerichtsverwertbare Beweissicherung, Gutachtenerstellung sowie Datenrettung zur Verfügung.

audatis Consulting berät Unternehmen bei der präventiven Umsetzung von Sicherheitsmaßnahmen, führt forensische Untersuchungen durch und stellt hierfür eigene Sachverständige zur Beweissicherung, Auswertung und Gutachtenerstellung zur Verfügung. Weiterhin werden Seminare zur Schulung von IT-Mitarbeitern und IT-Sicherheitsspezialisten durchgeführt, um eigenes Know-How im Bereich der IT-Forensik aufbauen zu können.

1.3 Über diese Checklisten

Um sich einen schnellen Überblick über das Gebiet der IT-Forensik zu verschaffen und bei der Beratung von Kunden oder Mitarbeitern bereits frühzeitig über mögliche Fehler bei der Durchführung von Maßnahmen zur Beweissicherung informieren zu können, ist diese Arbeitshilfe gedacht. Sie darf gerne kostenlos weitergegeben werden.

Alle Inhalte wurden nach bestem Wissen und Gewissen erstellt, eine Haftung kann jedoch nicht übernommen werden. Auch ein abweichendes Vorgehen ist im Einzelfall möglich.

2 Checklisten zur Beratung bei IT-Ermittlungen

Sofern Sie einen Kunden beraten, der mit einem Betrugsfall, einer vermuteten Straftat oder eines sonstigen Verstoßes gegen Recht oder Verträge zu Ihnen kommt, welcher einen Bezug zu IT-Systemen hat, sollten Sie stets prüfen, ob eine Beweissicherung vorgenommen werden muss bzw. welche ersten Schritte eingeleitet werden sollten, um eine spätere forensische Auswertung nicht zu gefährden.

Gleiches gilt natürlich auch, wenn Ihr eigenes Unternehmen betroffen ist.

Digitale Spuren sind zwar nicht sichtbar, stellen jedoch vollgültige Beweismittel dar. Der IT-Forensiker wird dabei zum sachverständigen Zeugen und sollte daher mit Bedacht ausgewählt werden.

Ihnen und Ihrem Kunden sollen diese Checklisten erste Anhaltspunkte liefern, um die wichtigsten Punkte nicht zu vergessen und keine Fehler beim Umgang mit den möglicherweise betroffenen IT-Systemen zu machen.

Hinweise zu den Checklisten

Die Checklisten können natürlich nicht jeden Einzelfall berücksichtigen. Sie sollten sich also möglichst zeitnah mit einem erfahrenen Experten für IT-Forensik abstimmen oder den Mandanten an diesen verweisen.

Bei der Beantwortung von Fragen, die mit diesem Symbol gekennzeichnet sind, sollten Sie besonders aufmerksam sein und evtl. weitere Prüfschritte im Einzelfall vornehmen bzw. einen Experten hinzuziehen.

2.1 Checkliste zu Prävention und Vorbereitung

	ja	nein
1. Wurde der datenschutzkonforme Einsatz von IT-Systemen geregelt (z.B. Einwilligung zur Einsicht bei erlaubter Privatnutzung)?	☐	☐
2. Wurden im Vorfeld Prozesse und Anweisungen definiert, was als Sicherheitsvorfall gilt bzw. wie im Verdachtsfall damit umgegangen werden soll (z.B. wer meldet welche Informationen an wen)?	☐	☐
3. Sind die Informationen allen Mitarbeitern bekannt gemacht worden (Awareness) und im Bedarfsfall auch für jeden verfügbar?	☐	☐
4. Liegt eine Checkliste zumindest in der IT-Abteilung bereit, um im Notfall schnellstmöglich handeln zu können und dabei keine Fehler zu begehen (auch die Kontaktdaten zu einem IT-Forensik-Experten sollten griffbereit sein)?	☐	☐

2.2 Checkliste zu rechtlichen Prüfschritten

	ja	nein
1. Ist der Verdächtige Berufsgeheimnisträger, mit anderweitigen Sonderstatusrechten versehener Arbeitnehmer, Beamter, Richter oder Soldat?	☐	☐
2. Ist der Eigentümer des Gerätes Arbeitnehmer (z.B. im Rahmen von Bring-your-own-Device = BYOD) oder ein Dritter?	☐	☐
3. Besteht der Verdacht einer Straftat bzw. eines Grundes zur Kündigung aus wichtigem Grund und wurde dieser bereits dokumentiert?	☐	☐
4. Wurden alle datenschutzrechtlichen Vorgaben (z.B. im Rahmen des Beschäftigtendatenschutzes nach § 32 BDSG oder anderen Vorschriften) berücksichtigt?	☐	☐
5. Wurde bei Bedarf der Betriebs- oder Personalrat einbezogen, um die Mitbestimmungsrechte zu wahren?	☐	☐
6. Sofern die Privatnutzung (z.B. von Geräten, Internet oder E-Mail) nicht wirksam verboten wurde, besteht eine Einwilligung des Verdächtigen zum Zugriff auf seine Daten (zur Vermeidung von Konflikten mit Fernmeldegeheimnis oder Persönlichkeitsrechten)?	☐	☐

<u>Wenn Frage 6 mit Nein beantwortet wurde</u>, sollte auf jeden Fall die Einsicht / Auswertung der privaten Daten bei der IT-Forensik ausgeschlossen werden.

2.3 Checkliste zur Einleitung der forensischen Ermittlung

	ja	*nein*
1. Ist das Vier-Augen-Prinzip gewahrt, so dass keine Tätigkeiten ohne Zeuge an den IT-Systemen vorgenommen werden?	☐	☐
2. Wurde der „Tatort“ abgesperrt bzw. der Zugang zu den betroffenen IT-Systemen für Unberechtigte (wie den Verdächtigen oder Dritte) wirksam verhindert?	☐	☐
3. Können alle noch laufenden IT-Systeme (Smartphones etc. berücksichtigen) ermittelt werden, ohne diese zu verändern (keine Tasten drücken!)?	☐	☐
✋ Wenn Frage 3 mit ja beantwortet wurde, sollten diese Geräte dokumentiert werden. Dabei sollten Fotobeweise vom Gerät (Rückseite und Vorderseite) samt Standort angefertigt werden.		
4. Sofern das System noch eingeschaltet ist und auf dem Ausgabegerät z.B. Bildschirm etwas angezeigt wird, sollten Fotoaufnahmen vom Bildschirminhalt gemacht werden (KEINE Screenshots – da hierfür Tasten gedrückt werden müssten!).	☐	☐
5. Müssen evtl. flüchtige Daten gesichert werden (z.B. beim Einsatz von Verschlüsselungsprodukten wie verschlüsselten Festplatten, virtuellen Maschinen)?	☐	☐
✋ Wenn Frage 5 mit ja beantwortet wurde, sollte spätestens hier ein IT-Forensik-Experte zu Rate gezogen werden, da beim kleinsten Fehler während der Datensicherung der weitere Zugriff auf die Daten u.U. nicht mehr möglich sein kann.		
6. Ist das Gerät (z.B. Server) mit dem Internet verbunden und es findet gerade eine relevante Handlung (z.B. Angriff, Fernsteuerung, etc.) statt? Dann kann das Ziehen des NETZWERK-Kabels (NICHT des Stromkabels!) u.U. weiteren Schaden verhindern. Dies sollte nach Möglichkeit in Absprache mit dem IT-Forensiker geschehen.	☐	☐
✋ Sofern eine notwendige Sicherung der flüchtigen Daten ausgeschlossen werden kann, sollte das Gerät durch ziehen des Stromkabels am Gerät stillgelegt werden (achten Sie unbedingt darauf, dass keine USV mehr dazwischen angeschlossen ist, welche u.U. ein Herunterfahren des IT-Systems erzwingen und somit wertvolle Spuren vernichten kann).		
7. Spätestens jetzt sollten Sie einen IT-Forensiker Ihres Vertrauens mit der gerichtsfesten Sicherung der Daten auf den Datenträgern und deren anschließender Auswertung und Aufbereitung beauftragen.		

2.4 Checkliste zu Dokumentation der Beweissicherung

	ja	*nein*
1. Sollen einzelne Geräte eingesammelt werden, um diese dem IT-Forensiker zukommen zu lassen, oder weil dieser nicht sofort verfügbar ist und zunächst die betroffene Hardware in einem gegen unbefugten Zutritt gesicherten Raum verbracht werden soll?	☐	☐

Wenn Sie Frage 1 mit ja beantwortet haben, füllen Sie für jeden Gegenstand (auch Aservat genannt) einen sep. Beweiszettel [siehe Kopiervorlage in Anlage 1] möglichst vollständig aus. Dabei hat sich folgendes Vorgehen bewährt:

a. Anfertigung von Fotos zur Identifikation der Gegenstände (wichtig sind z.B. Merkmale wie Seriennummern, angeschlossene Kabel, Aufkleber, etc.) möglichst von allen Seiten.	☐	☐
b. Dokumentation aller anwesenden Personen (Ermittlungsteam, Zeugen, Verdächtige, etc.).	☐	☐
c. Durchführung einer verwechslungssicheren Kennzeichnung (z.B. mittels durchnummerierter Aufkleber), welche den Fotos und Beweiszetteln zugeordnet werden.	☐	☐
d. Sobald die Gegenstände das Haus verlassen (z.B. Übersendung oder Übergabe an den Ermittler) sollte ein Übergabeprotokoll [siehe Kopiervorlage in Anlage 1] ausgefüllt werden, welches im Original beim Herausgeber verbleibt.	☐	☐
e. Auf dem Übergabeprotokoll wird später auch die Rückgabe der Gegenstände dokumentiert.	☐	☐

2.5 Kopiervorlagen

» Beweiszettel mit Übergabeprotokoll siehe Anlage 1

» Weitere Kopiervorlage für Beweiszettel, Übergabeprotokoll sowie unsere Checklisten finden Sie auch als PDF-Datei im Internet:

➲ **www.audatis.de/consulting/it-forensik**

3 Glossar

Asservat	Bezeichnung für alle sichergestellten oder beschlagnahmten Gegenstände (von PC bis zum USB-Stick).
BYOD	Bring-Your-Own-Device ermöglicht die Einbringung und Nutzung privater Hardware (z.B. Smartphones) in die IT-Infrastruktur des Unternehmens.
Honeypot	Als Honigtopf wird meist eine technische Einrichtung bezeichnet, die einen Angreifer oder Eindringling anziehen soll (z.B. um weitere Informationen über diese zu sammeln).
Live-Analyse	Forensische Methoden zur Sicherung und Auswertung von flüchtigen Daten wie z.B. dem Inhalt des Arbeitsspeichers.
Pentesting	Der Penetrationstest wird eingesetzt um Schwachstellen in Netzwerken und Systemen zu entdecken. Dabei wird vorgegangen, als wäre man ein interner oder externer Angreifer.
Post-mortem-Analyse	Forensische Methoden zur Sicherung und Auswertung von persistenten Daten wie z.B. von Festplatten, ausgeschalteten Rechnern oder USB-Sticks.
RAID-Verbund	Mehrere Festplatten zusammen ergeben einen RAID-Verbund. Dabei können Sie in verschiedenen Arten interagieren und z.B. Daten redundant oder verteilt speichern. Je nach RAID-Version ist die Rekonstruktion von Daten schwieriger oder einfacher.
Störung	Als Störung wird Beeinflussung der Funktion eines IT-Systems bezeichnet, die nicht als Sicherheitsvorfall gilt (z.B. defekte Festplatte, ausgefallenes Netzwerk, fehlerhafte Software).
Sicherheitsvorfall	Als Sicherheitsvorfall (Security Incident) wird ein unerwünschtes Ereignis bezeichnet, welches die Einschränkung oder den Verlust der Vertraulichkeit, Verfügbarkeit oder Integrität von Daten oder Systemen nach sich ziehen kann. Sicherheitsvorfälle müssen schnell und effizient bearbeitet werden, um einen möglichen Schaden durch Ausspähung, Manipulation oder Zerstörung von Daten und Systemen zu vermeiden bzw. zu minimieren.
USV	Unterbrechungsfreie Stromversorgung (z.B. mittels Batterie), die kurzzeitige Stromausfälle und Spannungsschwankungen ausgleicht und im Notfall IT-System kontrolliert herunterfährt, um Datenverluste zu vermeiden.

4 Kontaktdaten

Für ein vertrauliches und kostenfreies Erstgespräch zur Abstimmung von möglichen Ermittlungen im Bereich der IT-Forensik stehen wir Ihnen und Ihren Mandanten gerne jederzeit zur Verfügung.

Sie erreichen uns von Montag bis Freitag zwischen 07:00 und 19:00 telefonisch oder jederzeit per E-Mail.

Unsere Telefonnummer für Ihre Fragen:
05221 / 854 96 90

Carsten Knoop, M.Sc.

Dipl. Wirtschaftsinformatiker
Sachverständiger für IT-Forensik

audatis® Consulting
Datenschutz und Informationssicherheit
Inh. Carsten Knoop

Hauptsitz / Ostwestfalen:

Wittekindstr. 3
32051 Herford

Fon: +49 (0) 5221 / 854 96 - 90
Fax: +49 (0) 5221 / 854 96 - 99

Büro Rhein-Main-Neckar:

Wehrstr. 30
69488 Birkenau

E-Mail: info@audatis.de
Web: www.audatis.de